3GPP TR 33.899 V1.1.0 (2017-03)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on the security aspects of the next generation system (Release 14)





The present document has been developed within the 3rd Generation Partnership Project (3GPP ™) and may be further elaborated for the purposes of 3GPP.
The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Report is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and Reports for implementation of the 3GPP ™ system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords
<keyword[, keyword]>

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© 2017, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners
GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword 30

Introduction 30

1 Scope 31

2 References 31

3 Definitions, symbols and abbreviations 35
3.1 Definitions 35
3.2 Symbols 37
3.3 Abbreviations 37

4 Security areas and high level security requirements 38
4.1 Security areas 38
4.2 High level security requirements 39

5 Key issues and solutions 40
5.1 Security area #1: Architectural aspects of Next Generation security 40
5.1.1 Introduction 40
5.1.2 Security assumptions 40
5.1.3 Key issues 40
5.1.3.1 Key issue #1.1: Overview of NextGen security architecture 40
5.1.3.1.1 Key issue details 40
5.1.3.1.2 Security threats 40
5.1.3.1.3 Potential security requirements 41
5.1.3.2 Key issue #1.2: Need for security anchor in NextGen network 41
5.1.3.2.1 Key issue details 41
5.1.3.2.2 Security threats 42
5.1.3.2.3 Potential security requirements 42
5.1.3.3 Key Issue #1.3: User plane integrity between UE and network 43
5.1.3.3.1 Key issue details 43
5.1.3.3.2 Security threats 43
5.1.3.3.3 Potential security requirements 43
5.1.3.4 Key Issue #1.4: User plane confidentiality between UE and network 44
5.1.3.4.1 Key issue details 44
5.1.3.4.2 Security threats 44
5.1.3.4.3 Potential security requirements 44
5.1.3.5 Key Issue #1.5 Integrity protection for the control plane between UE and network 44
5.1.3.5.1 Key issue details 44
5.1.3.5.2 Security threats 45
5.1.3.5.3 Potential security requirements 45
5.1.3.6 Key Issue #1.6 Confidentiality for the control plane between UE and network 45
5.1.3.6.1 Key issue details 45
5.1.3.6.2 Security threats 45
5.1.3.6.3 Potential security requirements 45
5.1.3.7 Key issue #1.7: Key hierarchy 46
5.1.3.7.1 Key issue details 46
5.1.3.7.2 Security threats 46
5.1.3.7.3 Potential security requirements 46
5.1.3.8 Key Issue #1.8: UEs with Asymmetric Keys 46
5.2.3.8.1 Key issue details 46
5.2.3.8.2 Security threats 47
5.2.3.8.3 Potential security requirements 47
5.1.3.9 Key issue #1.9: Security features for AN-CN Control Plane 48
5.1.3.9.1 Key issue details 48
5.1.3.9.2 Security threats 48
5.1.3.9.3 Potential security requirements 48
5.1.3.10 Key issue #1.10: Security features for AN-CN User Plane 48

5.1.3.10.1 Key issue details 48
5.1.3.10.2 Security threats 48
5.1.3.10.3 Potential security requirements 49
5.1.3.11 Key issue #1.11: Security features for CN-CN Control Plane 49
5.1.3.11.1 Key issue details 49
5.1.3.11.2 Security threats 49
5.1.3.11.3 Potential security requirements 49
5.1.3.12 Key issue #1.12: Security features for CN-CN User Plane 50
5.1.3.12.1 Key issue details 50
5.1.3.12.2 Security threats 50
5.1.3.12.3 Potential security requirements 50
5.1.3.13 Key Issue #1.13: Security Implications to Achieve Low Latency 50
5.1.3.13.1 Key issue details 50
5.1.3.13.2 Security threats 51
5.1.3.13.3 Potential security requirements 52
5.1.3.14 Key issue #1.14: Security for serving functions in a less secure location 52
5.1.3.14.1 Key issue details 52
5.1.3.14.2 Security threats 53
5.1.3.14.3 Potential security requirements 53
5.1.3.15 Key issue #1.15: Termination point of UP security 54
5.1.3.15.1 Key issue details 54
5.1.3.15.2 Security threats 55
5.1.3.15.3 Potential security requirements 55
5.1.3.16 Key issue #1.16: User plane protection granularity 55
5.1.3.16.1 Key issue details 55
5.1.3.16.2 Security threats 56
5.1.3.16.3 Potential security requirements 56
5.1.3.17 Key issue #1.17: On-demand security policy 56
5.1.3.17.1 Key issue details 56
5.1.3.17.2 Security threats 57
5.1.3.17.3 Potential security requirements 57
5.1.3.18 Key issue #1.18: Flexible security policies negotiation in control plane 57
5.1.3.18.1 Key issue details 57
5.11.3.18.2 Security threats 58
5.1.3.18.3 Potential security requirements 58
5.1.3.19 Key issue #1.19: Untrusted non-3GPP access 58
5.1.3.19.1 Key issue details 58
5.1.3.19.2 Security threats 58
5.1.3.19.3 Potential security requirements 58
5.1.3.20 Key issue #1.20: Trusted non-3GPP access 59
5.1.3.20.1 Key issue details 59
5.1.3.20.2 Security threats 59
5.1.3.20.3 Potential security requirements 59
5.1.3.21 Key issue #1.21: Dealing with signalling attacks 59
5.1.3.21.1 Key issue details 59
5.1.3.21.2 Security threats 60
5.1.3.21.3 Potential security requirements 60
5.1.3.y Key issue #1.y: <key issue name> 60
5.1.3.y.1 Key issue details 60
5.1.3.y.2 Security threats 60
5.1.3.y.3 Potential security requirements 60
5.1.4 Solutions 60
5.1.4.1 Solution #1.1: Radio interface user plane integrity protection 60
5.1.4.1.1 Introduction 60
5.1.4.1.2 Solution details 60
5.1.4.1.3 Evaluation 61
5.1.4.2 Solution #1.2: Periodic local authentication and packet count check 61
5.1.4.2.1 Introduction 61
5.1.4.2.2 Solution details 61
5.1.4.2.3 Evaluation 61
5.1.4.3 Solution #1.3: Radio interface user plane encryption 62
5.1.4.3.1 Introduction 62

5.1.4.3.2 Solution details 62
5.1.4.3.3 Evaluation 62
5.1.4.4 Solution #1.4: Key hierarchy 62
5.1.4.4.1 Introduction 62
5.1.4.4.2 Solution details 62
5.1.4.4.3 Evaluation 63
5.1.4.5 Solution #1.5: User plane security policy and key derivation 63
5.1.4.5.1 Introduction 63
5.1.4.5.2 Solution details 63
5.1.4.5.2.1 Introduction 63
5.1.4.5.2.2 Procedure 64
5.1.4.5.2 Evaluation 66
5.1.4.6 Solution #1.6: Architecture for NextGen that include a security anchor 66
5.1.4.6.1 Introduction 66
5.1.4.6.2 Solution details 66
5.1.4.6.2.1 Architecture 66
5.1.4.6.2.1.1 General 66
5.1.4.6.2.1.2 Alternative Roaming Architecture 68
5.1.4.6.2.1.3 Architecture for untrusted non-3GPP access in the roaming scenario 69
5.1.4.6.2.1.4 Procedure for home-terminated user plane session establishment for the roaming scenario 70
5.1.4.6.2.2 Key Hierarchy 72
5.1.4.6.2.3 Possible example procedures using the security anchor 73
5.1.4.6.2.3.1 General 73
5.1.4.6.2.3.2 Key derivation during the attach procedure 73
5.1.4.6.2.3.3 Key derivation during the NG2-based handover 74
5.1.4.6.2.3.4 Key derivation for the idle mode mobility 76
5.1.4.6.3 Evaluation 76
5.1.4.7 Solution #1.7: Serving functions all deployed in secure location 76
5.1.4.7.1 Introduction 76
5.1.4.7.2 Solution details 77
5.1.4.7.3 Evaluation 77
5.1.4.8 Solution #1.8: Key hierarchy for NextGen 77
5.1.4.8.2.2 Key Hierarchy 77
5.1.4.8.2.3 Key derivation 79
5.1.4.9 Solution #1.9: Key hierarchy and the related procedure 80
5.1.4.9.1 Introduction 80
5.1.4.9.2 Solution details 81
5.1.4.9.2.1 Architecture 81
5.1.4.9.2.2 Key hierarchy 82
5.1.4.9.2.3 Security procedure 83
5.1.4.9.3 Evaluation 84
5.1.4.10 Solution #1.10: UP protection for PDU session (re)establishment triggered by handover 84
5.1.4.10.1 Introduction 84
5.1.4.10.2 Solution details 86
5.1.4.10.3 Evalution 88
5.14.11 Solution #1.11 High level of Security Architecture 88
5.1.4.11.1 Introduction 88
5.1.4.11.2 Solution details 88
5.1.4.11.3 Evaluation 89
5.1.3.12 Solution #1.12: Low latency security technique to protect user plane 89
5.1.3.12.1 Introduction 89
5.1.3.12.2 Solution details 89
5.1.3.12.3 Evaluation 90
5.1.4.13 Solution #1.13: Security of NAS signallings before security activation 90
5.1.4.13.1 Introduction 90
5.1.4.13.2 Solution details 90
5.1.4.13.2.1 Protection of the uplink message 90
5.1.4.13.2.2 Protection of the downlink message 90
5.1.4.13.3 Evaluation 92
5.1.4.14 Solution #1.14: Single termination point for NAS security 92
5.1.4.14.1 Introduction 92

5.1.4.14.2 Solution details 92
5.1.4.14.3 Evaluation 92
5.1.4.15 Solution #1.15: AES as a fast stream cipher 93
5.1.4.15.1 Introduction 93
5.1.4.15.2 Solution details 93
5.1.4.15.3 Evaluation 93
5.1.4.16 Solution #1.16: Re-use of "Data efficient re-keying" 93
5.1.4.16.1 Introduction 93
5.1.4.16.2 Solution details 94
5.1.4.16.3 Evaluation 94
5.1.4.17 Solution #1.17: Delegated Subscriber Server 94
5.1.4.17.1 Introduction 94
5.1.4.17.2 Solution details 94
5.1.4.17.3 Evaluation 94
5.1.4.18 Solution #1.18: Combining Low Latency on User Plane with High Latency on Control Plane 95
5.1.4.18.1 Introduction 95
5.1.4.18.2 Solution details 95
5.1.4.18.3 Evaluation 95
5.1.4.19 Solution #1.19: Next Generation USIM 95
5.1.4.19.1 Introduction 95
5.1.4.19.2 Solution details 95
5.1.4.19.3 Evaluation 96
5.1.4.20 Solution 1.20: Flexible UP security termination point 96
5.1.4.20.1 Introduction 96
5.1.4.20.2 Solution details 96
5.1.4.20.3 Evaluation 96
5.1.4.21 Solution 1.21: Flexible UP security termination point 97
5.1.4.21.1 Introduction 97
5.1.4.21.2 Solution details 97
5.1.4.21.3 Evaluation 98
5.1.4.22 Solution #1.22: Terminating user plane security in the AN 98
5.1.4.22.1 Introduction 98
5.1.4.22.2 Solution details 99
5.1.4.22.3 Evaluation 99
5.1.4.23 Solution #1.23: Security for the AN-CN User Plane 100
5.1.4.23.1 Introduction 100
5.1.4.23.2 Solution details 100
5.1.4.23.3 Evaluation 101
5.1.4.24 Solution #1.24: Security for the AN-CN Control Plane 101
5.1.4.24.1 Introduction 101
5.1.4.24.2 Solution details 101
5.1.4.24.3 Evaluation 102
5.1.4.25 Solution #1.25: Protocol stack options for the user-plane security terminating at the UPF 102
5.1.4.25.1 Introduction 102
5.1.4.25.2 Solution details 102
5.1.4.25.3 Evaluation 104
5.1.4.26 Solution #1.26: Untrusted non-3GPP access 104
5.1.4.26.1 Introduction 104
5.1.4.26.2 Solution details 104
5.1.4.26.3 Evaluation 107
5.1.4.27 Solution #1.27: Authentication and Key Agreement procedure for untrusted non-3GPP Access 107
5.1.4.27.0 General 107
5.1.4.27.1 Solution Overview 107
5.1.4.27.2 Attach and UE Authentication Procedure via Untrusted non-3GPP Access 108
5.1.4.27.3 Evaluation 110
5.1.4.28. Solution #1.28: Authentication and Key agreement procedure for NextGen architecture with stand-alone non-3GPP access 110
5.1.4.28.1 Solution Overview 110
5.1.4.28.1.2 Attach Procedure with EPS-AKA for non-3GPP Access 111
5.1.4.28.3 Evaluation 113

5.1.4.29 Solution #1.29: A solution for KDF negotiation 113
5.1.4.29.1 Introduction 113
5.1.4.29.2 Solution details 114
5.1.4.29.2.0 General 114
5.1.4.29.2.1 gNB-KDF negotiation 114
5.1.4.29.2.2 AMF-KDF negotiation 115
5.1.4.29.2.3 SEAF-KDF negotiation 115
5.1.4.29.2.4 SMF-KDF negotiation 116
5.1.4.29.2.5 ARPF-KDF negotiation 116
5.1.4.29.3 Evaluation 117
5.1.4.30 Solution #1.30 Registration Procedure for NextGen network 119
5.1.4.30.1 Introduction 119
5.1.4.30.2 Solution details 119
5.1.4.30.3 Evaluation 120
5.1.4.31 Solution #1.31 Security mode command procedure for NextGen network 120
5.1.4.31.1 Introduction 120
5.1.4.31.2 Solution details 120
5.1.4.31.2.1 NAS security mode command procedure 120
5.1.4.31.2.2 AS security procedure 121
5.1.4.31.2.3 UP security mode command procedure 122
5.1.4.31.3 Evaluation 122
5.1.4.32 Solution #1.32 Security mode command procedure for NextGen network with NAS-SM 123
5.1.4.32.1 Introduction 123
5.1.4.32.2 Solution details 123
5.1.4.32.2.1 NAS security mode command procedure 123
5.1.4.32.2.2 AS security procedure 123
5.1.4.32.2.3 NAS-SM security mode command procedure 124
5.1.4.32.2.4 UP security mode command procedure 125
5.1.4.32.3 Evaluation 126
5.1.4.33 Solution #1.33: Consolidated Key hierarchy for NextGen 126
5.1.4.33.1 Introduction 126
5.1.4.33.2 Solution details 126
5.1.4.z.33.1 Architecture 126
5.1.4.33.2.2 Key Hierarchy 127
5.1.4.33.2.2.1 Consolidated Key Hierarchy Option 1 128
5.1.4.33.2.2.2 Consolidated Key Hierarchy Option 2 129
5.1.4.33.3 Evaluation 129
5.1.4.34 Solution #1.34: NextGen USIM 129
5.1.4.34.1 Introduction 129
5.1.4.34.2 Solution details 129
5.1.4.34.2.1 Overview 129
5.1.4.34.2.2 Extension of authentication command to cover new protocols 130
5.1.4.34.2.3 Addition of the ability to verify the user for UE applications and network applications 130
5.1.4.34.2.4 Addition of mechanisms to allow long term key refresh (such as Ki). 130
5.1.4.34.2.6 Addition of support for Asymmetric key cryptography. 131
5.1.4.34.3 Evaluation 131
5 1.4.35 Solution #1.35: Key management during AMF change 131
5.1.4.35.1 Introduction 131
5.1.4.35.2 Solution details 131
5.1.4.35.2.1 General 131
5.1.4.35.2.2 Key derivation 131
5.1.4.35.2.3 AMF change procedure 131
5.1.4.35.3 Evaluation 133
5 1.4.36 Solution #1.36: Security anchor function via primary AMFs 133
5.1.4.36.1 Introduction 133
5.1.4.36.2 Solution details 133
5.1.4.36.2.1 General 133
5.1.4.36.2.2 Role assignment 133
5.1.4.36.2.3 Security context handling during AMF change 133
5.1.4.36.2.3.1 Scenario #1: Re-authentication 133
5.1.4.36.2.3.2 Scenario #2: Key transfer 134

5.1.4.36.2.3.3 Scenario #3: Horizontal key derivation 135
5.1.4.36.2.3.4 Scenario #4: Vertical key derivation 135
5.1.4.36.3 Evaluation 135
5.1.4.38 Solution #1.38: Detection and response function for signalling attacks 137
5.1.4.38.1 Introduction 137
5.1.4.38.2 Solution details 137
5.1.4.38.3 Evaluation 138
5.1.4.39 Solution #1.39: Flexible UP Termination Point with LTE compatibility 138
5.1.4.39.1 Introduction 138
5.1.4.39.2 Solution details 139
5.1.4.39.2.1 Overview 139
5.1.4.39.2.2 Flexible UP Security Termination based on Option 3x 139
5.1.4.39.2.3 Flexible UP Security Termination based on Option 3a 139
5.1.4.39.3 Evaluation 139
5.1.4.z Solution #1.z: <solution name> 139
5.1.4.z.1 Introduction 139
5.1.4.z.2 Solution details 139
5.1.4.z.3 Evaluation 139
5.1.5 Conclusions 139
5.2 Security area #2: Authentication 140
5.2.1 Introduction 140
5.2.1.1 General 140
5.2.1.2 Authentication-related functions 141
5.2.2 Security assumptions 143
5.2.3 Key issues 144
5.2.3.1 Key Issue #2.1 Authentication framework 144
5.2.3.1.1 Key issue details 144
5.2.3.1.2 Security threats 145
5.2.3.1.3 Potential security requirements 145
5.2.3.2 Key Issue #2.2: Reducing the impact of secret key leakage 146
5.2.3.2.1 Key issue details 146
5.2.3.2.2 Security threats 146
5.2.3.2.3 Potential security requirements 147
5.2.3.3 Key issue #2.3: Authentication identifiers and credentials 147
5.2.3.3.1 Key issue details 147
5.2.3.3.2 Security threats 149
5.2.3.3.3 Potential security requirements 150
5.2.3.4 Key issue #2.4: Equipment identifier authentication 150
5.2.3.4.1 Key issue details 150
5.2.3.4.2 Security threats 151
5.2.3.4.3 Potential security requirements 152
5.2.3.5 Key issue #2.5: Non-AKA-based authentication 152
5.2.3.5.1 Key issue details 152
5.2.3.5.2 Security threats 153
5.2.3.5.3 Potential security requirements 153
5.2.3.6 Key Issue #2.6: Efficient in energy consuming and reduced signalling for resource constraint environment 153
5.2.3.6.1 Key issue details 153
5.2.3.6.2 Security threats 153
5.2.3.6.3 Potential security requirements 153
5.2.3.7 Key Issue #2.7: Reduced signalling overload for massive number of UEs activating at the same time 153
5.2.3.7.1 Key issue details 153
5.2.3.7.2 Security threats 154
5.2.3.7.3 Potential security requirements 154
5.2.3.8 Key Issue #2.8: Authentication of the user 154
5.2.3.8.1 Key issue details 154
5.2.3.8.2 Security threats 154
5.2.3.8.3 Potential security requirements 155
5.2.3.9 Key issue #2.9: Security for service provider connection 155
5.2.3.9.1 Key issue details 155
5.2.3.9.2 Security threats 156

5.2.3.9.3 Potential security requirements 156
5.2.3.10 Key issue #2.10: Secondary authentication for network slice access by 3rd party service 157
5.2.3.10.1 Key issue details 157
5.2.3.10.2 Security threats 158
5.2.3.10.3 Potential security requirements 158
5.2.3.11 Key issue #2.11: Increasing home control in roaming situations 158
5.2.3.11.1 Key issue details 158
5.2.3.11.2 Security threats 158
5.2.3.11.3 Potential security requirements 158
5.2.3.y Key issue #2.y: <key issue name> 159
5.2.3.y.1 Key issue details 159
5.2.3.y.2 Security threats 159
5.2.3.y.3 Potential security requirements 159
5.2.4 Solutions 159
5.2.4.1 Solution #2.1: Updating the long term secret key, in such a way that the new key is less exposed to potential attack than the original one was 159
5.2.4.1.1 Introduction 159
5.2.4.1.2 Solution details 159
5.2.4.1.3 Notes on statefulness at the HSS 160
5.2.4.1.4 Evaluation 161
5.2.4.2 Solution #2.2: Including a key exchange protocol into the derivation of the radio interface session keys 161
5.2.4.2.1 Introduction 161
5.2.4.2.2 Solution details 161
5.2.4.2.3 Evaluation 161
5.2.4.3 Solution #2.3: Device reporting on local user authentication 162
5.2.4.3.1 Introduction 162
5.2.4.3.2 Solution details 162
5.2.4.3.3 Evaluation 162
5.2.4.4 Solution #2.4: Authenticating a new user for a device using a known device 163
5.2.4.4.1 Introduction 163
5.2.4.4.2 Solution details 163
5.2.4.4.3 Evaluation 163
5.2.4.5 Solution #2.5: Timed attach for UEs 163
5.2.4.5.1 Introduction 163
5.2.4.5.2 Solution details 163
5.2.4.5.3 Evaluation 164
5.2.4.6 Solution #2.6: Binding a serving network public key into the derivation of the radio interface session keys 164
5.2.4.6.1 Introduction 164
5.2.4.6.2 Solution details 164
5.2.4.6.3 Evaluation 165
5.2.4.7 Solution #2.7: Authentication framework 167
5.2.4.7.1 Introduction 167
5.2.4.7.2 Solution details 167
5.2.4.7.2.1 Candidate authentication methods 167
5.2.4.7.2.2 Transport considerations 168
5.2.4.7.2.3 Efficiency considerations 169
5.2.4.7.2.4 General information flow 170
5.2.4.7.2.5 Alternatives for AKA-based authentication over 3GPP-defined access networks 171
5.2.4.7.3 Evaluation 172
5.2.4.8 Solution #2.8: Authentication Framework based on EAP 173
5.2.4.8.1 Introduction 173
5.2.4.8.2 Solution details 173
5.2.4.8.2.1 Authentication Entities and their location in the Next Generation System 173
5.2.4.8.2.1.1 Alternative 1: Authentication using direct interface between the UE and the SEAF 173
5.2.4.8.2.1.2 Alternative 2: Authentication using NG1 interface 176
5.2.4.8.3 Evaluation 179
5.2.4.9 Solution #2.9: EAP authentication framework 179
5.2.4.9.1 Introduction 179
5.2.4.9.2 Solution details 179

5.2.4.9.2.1 Introduction 179
5.2.4.9.2.3 Phase 2: Optional EAP method specific identity exchange 181
5.2.4.9.2.4 Phase 3: Rest of EAP method specific signalling 181
5.2.4.9.2.5 Phase 4: EAP Success/Failure and exchange of the ARSK 184
5.2.4.9.2.6 Fast re-authentication with ERP 184
5.2.4.9.3 Migration and interworking with LTE/eLTE 185
5.2.4.9.4 Optimization considerations: termination of EAP method in the VPLMN 186
5.2.4.9.5 Evaluation 188
5.2.4.10 Solution #2.10: Equipment Identifier Authentication using the Device Certificate 189
5.2.4.10.1 Introduction 189
5.2.4.10.2 Solution details 189
5.2.4.10.2.1 Introduction 189
5.2.4.10.2.2 Service Provider issued device certificate enrollment 191
5.2.4.10.2.3 Use of Equipment Identifier Authentication with EIR 192
5.2.4.10.3 Evaluation 192
5.2.4.11 Solution #2.11: Blocking the UE which repeats authentication in a short period 193
5.2.4.11.1 Introduction 193
5.2.4.11.2 Solution details 193
5.2.4.11.3 Evaluation 194
5.2.4.12 Solution #2.12: Mutual Authentication and Security Agreement 195
5.2.4.12.1 Introduction 195
5.2.4.12.2 Solution Details 195
5.2.4.12.2.1 NG Security Architecture 195
5.2.4.12.2.2 NG-MASA Main Security Aspects 195
5.2.4.12.2.3.1 Initial Authentication Request (IAR) 196
5.2.4.12.2.3.2 Initial Authentication Response (IAS) 196
5.2.4.12.2.3.3 Changes to S6a User Authentication and Data Request 197
5.2.4.12.2.4 Changes to AUSF/ARPF Functionality 197
5.2.4.12.2.4.1 Handling of Authentication and Data Request 197
5.2.4.12.2.4.2 Handling of Authentication and Data Response 198
5.2.4.12.2.4.3 Changes to SEAF Functionality 198
5.2.4.12.2.5 Initial Authentication Call Flow Details 199
5.2.4.12.3 MASA support 4G USIM 200
5.2.4.12.3.1 Initial Authentication Request (IAR) 201
5.2.4.12.3.2 Initial Authentication Response (IAS) 201
5.2.4.12.3.3 AUSF/ARPF Functionality 202
5.2.4.12.3.3.1 Handling of Authentication and Data Request 202
5.2.4.12.3.3.2 Handling of Authentication and Data Response 202
5.2.4.12.3.4 SEAF Functionality 202
5.2.4.12.3.5 4G USIM Initial Authentication Call Flow Details 203
5.2.4.12.4 MASA NG-UE Security Capabilities Negotiation 204
5.2.4.12.4.1 NG-UE Functionality 204
5.2.4.12.4.2 gNB-CP Functionality 205
5.2.4.12.4.3 SEAF Functionality 205
5.2.4.12.4.4 AUSF/ARPF Functionality 206
5.2.4.12.4.5 UP-GW Functionality 206
5.2.4.12.4.5.1 Initial Authentication Call Flow with NG-UE Security Capabilities Negotiation 206
5.2.4.12.5 Solution Evaluation 207
5.2.4.12.5.1 Evaluation#1 Summary 207
5.2.4.12.5.2 Detailed Evaluation#1 208
5.2.4.12.5.2.1 MASA Goals and Evaluation 208
5.2.4.12.5.3 Evaluation#2 212
5.2.4.13.1 Introduction 214
5.2.4.13.2 Solution details 214
5.2.4.13.3 Evalution 216
5.2.4.14 Solution #2.14: Solution for non-AKA Authentication 216
5.2.4.14.1 Introduction 216
5.2.4.14.2 Solution details 217
5.2.4.14.2.1 A Framework for Non-AKA Authentication 217
5.2.4.14.2.2 Generic Procedure Description for Non-AKA Authentication 218
5.2.4.14.2.3 Non-AKA Authentication Protocols based on EAP-TLS 219

5.4.2.14.2.4 Non-AKA Authentication Protocols based EAP-PSK and Identity-based Credentials ... 220
5.2.4.14.3 Evaluation ... 221
5.2.4.15 Solution #2.15: Aggregate Authentication for massive IoT ... 221
5.2.4.15.1 Introduction ... 221
5.2.4.15.2 Solution details ... 222
5.2.4.15.3 Evaluation ... 225
5.2.4.16 Solution #2.16: Mutual Authentication between Remote UE and Network over A Relay based on ID-based Credentials ... 225
5.2.4.16.1 Introduction ... 225
5.2.4.16.2 Solution details ... 225
5.2.4.16.3 Evaluation ... 227
5.2.4.17 Solution #2.17: Equipment identifier Authentication using the device certificate and IMEI binding ... 227
5.2.4.17.1 Introduction ... 227
5.2.4.17.2 Solution details ... 227
5.2.4.17.3 Evaluation ... 228
5.2.4.18 Solution #2.18: Equipment identifier Authentication using the device public key and IMEI binding ... 228
5.2.4.18.1 Introduction ... 228
5.2.4.18.2 Solution details ... 229
5.2.4.18.3 Evaluation ... 230
5.2.4.19 Solution #2.19: Alternative EAP architecture for 3GPP access ... 230
5.2.4.19.1 Introduction ... 230
5.2.4.19.2 Solution details ... 230
5.2.4.19.2.1 Protocol Stack ... 230
5.2.4.19.2.2 Authentication flows ... 230
5.2.4.20 Solution #2.20: void ... 232
5.2.4.21 Solution #2.21: Linking update location with authentication confirmation ... 232
5.2.4.21.1 Introduction ... 232
5.2.4.21.2 Solution details ... 232
5.2.4.21.3 Evaluation ... 233
5.2.4.22 Solution #2.22: EPS AKA with UE authentication confirmation ... 233
5.2.4.22.1 Introduction ... 233
5.2.4.22.2 Solution details ... 233
5.2.4.22.3 Evaluation ... 234
5.2.4.23 Solution #2.23: Equipment Identifier Authentication using Identity-based Authentication ... 236
5.2.4.23.1 Introduction ... 236
5.2.4.23.2 Solution details ... 236
5.2.4.23.3 Evaluation ... 237
5.2.4.24 Solution #2.24: Combining solutions 2.2 and 10.2 ... 237
5.2.4.24.1 Introduction ... 237
5.2.4.24.2 Solution details ... 237
5.2.4.24.3 Evaluation ... 237
5.2.4.25 Solution #2.25: Authentication Procedure for un-trusted non-3GPP access ... 237
5.2.4.25.1 Introduction ... 237
5.2.4.25.2 Solution details ... 237
5.2.4.25.3 Evaluation ... 239
5.2.4.26 Solution #2.26: EAP based secondary authentication by an external DN-AAA server ... 239
5.2.4.26.1 Introduction ... 239
5.2.4.26.2 Solution details ... 239
5.2.4.26.3 Evaluation ... 241
5.2.4.27 Solution #2.27: EAP-based solution for secondary authentication, authorization and UP protection ... 241
5.2.4.27.1 Introduction ... 241
5.2.4.27.2 Solution details ... 241
5.2.4.27.2.1 Overall procedure ... 241
5.2.4.27.2.3 Support of Network Slicing ... 242
5.2.4.28 Solution # 2.28: secondary authentication and authorization using SM NAS signalling ... 243
5.2.4.28.1 Introduction ... 243
5.2.4.28.2 Solution details ... 243
5.2.4.28.3 Evaluation ... 244

5.2.4.29 Solution #2.29: Equipment identifier authentication using EAP 244
5.2.4.29.1 Introduction 244
5.2.4.29.2 Solution details 244
5.2.4.29.3 Solution evaluation 246
5.2.4.30 Solution #2.30: EAP based secondary authentication by an external DN-AAA server 246
5.2.4.30.1 Introduction 246
5.2.4.30.2 Solution details 246
5.2.4.30.3 Evaluation 249
5.2.4.z Solution #2.z: <solution name> 249
5.2.4.z.1 Introduction 249
5.2.4.z.2 Solution details 249
5.2.4.z.3 Evaluation 249
5.2.5 Conclusions 249
5.3 Security area #3: Security context and key management 249
5.3.1 Introduction 249
5.3.2 Security assumptions 249
5.3.3 Key issues 249
5.3.3.1 Key Issue #3.1: Interception of radio interface keys sent between operator entities 249
5.3.3.1.1 Key issue details 249
5.3.3.1.2 Security threats 250
5.3.3.1.3 Potential security requirements 250
5.3.3.2 Key Issue #3.2: Refreshing keys 250
5.3.3.2.1 Key issue details 250
5.3.3.2.2 Security threats 250
5.3.3.2.3 Potential security requirements 250
5.3.3.3 Key issue #3.3: Principles of security negotiation 251
5.3.3.3.1 Key issue details 251
5.3.3.3.2 Security threats 251
5.3.3.3.3 Potential security requirements 251
5.3.3.4 Key Issue #3.4: Security context sharing 252
5.3.3.4.1 Key issue details 252
5.3.3.4.2 Security threats 252
5.3.3.4.3 Potential security requirements 252
5.3.3.5 Key issue #3.5: Unnecessary dependence of keys between security layers 252
5.3.3.5.1 Key issue details 252
5.3.3.5.2 Security threats 253
5.3.3.5.3 Potential security requirements 253
5.3.3.6 Key issue #3.6: Top-level key for access-network-specific keys 253
5.3.3.6.1 Key issue details 253
5.3.3.6.2 Security threats 253
5.3.3.6.3 Potential security requirements 253
5.3.3.7 Key issue #3.7: The storage of security context 253
5.3.3.7.1 Key issue details 253
5.3.3.7.2 Security threats 254
5.3.3.7.3 Potential security requirements 254
5.3.3.8 Key issue #3.8: Security context for small data mode 254
5.3.3.8.1 Key issue details 254
5.3.3.8.2 Security threats 254
5.3.3.8.3 Potential security requirements 254
5.3.3.9 Key issue #3.9: void 254
5.3.3.10 Key issue #3.10: void 254
5.3.3.11 Key issue #3.11: 5G security key and context identification 254
5.3.3.11.1 Key issue details 254
5.3.3.11.2 Security threats 255
5.3.3.11.3 Potential security requirements 255
5.3.3.y Key issue #3.y: <key issue name> 255
5.3.3.y.1 Key issue details 255
5.3.3.y.2 Security threats 255
5.3.3.y.3 Potential security requirements 255
5.3.4 Solutions 255
5.3.4.1 Solution #3.1: Including a key exchange protocol into the derivation of the radio interface session keys 255

5.3.4.1.1 Introduction 255
5.3.4.1.2 Solution details 255
5.3.4.1.3 Evaluation 258
5.3.4.2 Solution #3.2: UE can request a radio interface key refresh 259
5.3.4.2.1 Introduction 259
5.3.4.2.2 Solution details 259
5.3.4.2.3 Evaluation 260
5.3.4.3 Solution #3.3: Security Context Management for UE with Multiple Access Technologies 260
5.3.4.3.1 Introduction 260
5.3.4.3.2 Solution details 260
5.3.4.3.3 Evaluation 262
5.3.4.4 Solution #3.4: void 262
5.3.4.5 Solution #3.5: Trusted non-3GPP access 262
5.3.4.5.1 Introduction 262
5.3.4.5.2 Solution details 263
5.3.4.5.3 Evaluation 265
5.3.4.6 Solution #3.6: Next Generation Key Set Identifier 265
5.3.4.6.1 Introduction 265
5.3.4.6.2 Solution details 265
5.3.4.6.3 Evaluation 266
5.3.4.7 Solution #3.7: Algorithms Negotiation Procedure 266
5.3.4.7.1 Introduction 266
5.3.4.7.2 Solution details 266
5.3.4.7.3 Evaluation 268
5.3.4.8 Solution #3.8: Key negotiation of dual connectivity to deal with the leakage of secret key 268
5.3.4.8.1 Introduction 268
5.3.4.8.2 Solution details 268
5.3.4.8.3 Evaluation 269
5.3.4.9 Solution #3.9: Security Key Refresh Triggered by UE 269
5.3.4.9.1 Introduction 269
5.3.4.9.2 Solution details 269
5.3.4.9.3 Evaluation 273
5.3.4.10 Solution #3.10: void 274
5.3.4.11 Solution #3.11: Binding of keys to an authentication session with a serving network in NextGen systems 274
5.3.4.11.1 Introduction 274
5.3.4.11.2 Solution details 274
5.3.4.11.3 Evaluation 276
5.3.4.12 Solution #3.12: "Binding a serving network public key into the derivation of the radio interface session keys" 276
5.3.4.12.1 Introduction 276
5.3.4.12.2 Solution details 276
5.3.4.12.3 Evaluation 276
5.3.4.z Solution #3.z: <solution name> 277
5.3.4.z.1 Introduction 277
5.3.4.z.2 Solution details 277
5.3.4.z.3 Evaluation 277
5.3.5 Conclusions 277
5.4 Security area #4: RAN security 277
5.4.1 Introduction 277
5.4.2 Security assumptions 279
5.4.3 Key issues 279
5.4.3.1 Key Issue #4.1: AS security during RRC idle mode 279
5.4.3.1.1 Key issue details 279
5.4.3.1.1 Security threats 279
5.4.3.1.3 Potential security requirement 279
5.4.3.2.2 Security threats 280
5.4.3.2.3 Potential security requirements 280
5.4.3.3.1.0 General security aspects of dual connectivity 280
5.4.3.3.1.1 Security aspects for deployment scenario of option 3 281
5.4.3.4 Key issue #4.4: Security aspects of inactive mode mobility 282
5.4.3.4.1 Key issue details 282

5.4.3.4.2 Security threats 282
5.4.3.4.3 Potential security requirements 282
5.4.3.5 Key issue #4.5: Security aspects of RAN-WLAN aggregation/integration 282
5.4.3.5.1 Key issue details 282
5.4.3.5.2 Security threats 282
5.4.3.5.3 Potential security requirements 282
5.4.3.6 Key issue #4.6: User plane DoS attacks 282
5.4.3.6.1 Key issue details 282
5.4.3.6.2 Security threats 283
5.4.3.6.3 Potential security requirements 283
5.4.3.7 Key Issue #4.7 Key handling in RRC inactive state to RRC active state transition 283
5.4.3.7.1 Key issue details 283
5.4.3.7.2 Security threats 283
5.4.3.7.3 Potential security requirements 283
5.4.3.8 Key issue #4.8: void 283
5.4.3.9 Key issue #4.9: Security aspects of NG2 handover 283
5.4.3.9.1 Key issue details 283
5.4.3.9.2 Security threats 284
5.4.3.9.3 Potential security requirements 284
5.4.3.10 Key issue #4.10: Security aspects of sidehaul interfaces 285
5.4.3.10.1 Key issue details 285
5.4.3.10.2 Security threats 285
5.4.3.10.3 Potential security requirements 285
5.4.3.11 Key issue #4.11: Flexibility to retain or to change AS security keys 285
5.4.3.11.1 Key issue details 285
5.4.3.11.2 Security threats 286
5.4.3.11.3 Potential security requirements 286
5.4.3.12 Key issue #4.12: Changing AS security keys on-the-fly 286
5.4.3.12.1 Key issue details 286
5.4.3.12.2 Security threats 287
5.4.3.12.3 Potential security requirements 287
5.4.3.13 Key issue #4.13: Dealing with radio jamming 287
5.4.3.13.1 Key issue details 287
5.4.3.13.2 Security threats 287
5.4.3.13.3 Potential security requirements 287
5.4.3.14 Key issue #4.14: Privacy aspects of RAN level temporary identifiers 288
5.4.3.14.1 Key issue details 288
5.4.3.14.2 Security threats 288
5.4.3.14.3 Potential security requirements 288
5.4.3.15 Key issue #4.15: Security aspects of Xn handover 288
5.4.3.15.1 Key issue details 288
5.4.3.15.2 Security threats 290
5.4.3.15.3 Potential security requirements 290
5.4.3.16 Key issue #4.16: Security algorithm negotiation between UE and RAN 290
5.4.3.16.1 Key issue details 290
5.4.3.16.2 Security threats 291
5.4.3.16.3 Potential security requirements 291
5.4.3.17 Key issue #4.17: Supporting integrity protection of UP 291
5.4.3.17.1 Key issue details 291
5.4.3.17.2 Security threats 292
5.4.3.17.3 Potential security requirements 292
5.4.3.y Key issue #4.y: <key issue name> 292
5.4.3.y.1 Key issue details 292
5.4.3.y.2 Security threats 292
5.4.3.y.3 Potential security requirements 292
5.4.4 Solutions 292
5.4.4.1 Solution #4.1: Network signs selected signalling messages 292
5.4.4.1.1 Introduction 292
5.4.4.1.2 Solution details 292
5.4.4.1.2.1 Background 292
5.4.4.1.2.2 Provisioning and management of keys 292
5.4.4.1.2.3 Revocation 293

5.4.4.1.2.4 Signature algorithms and algorithm selection 294
5.4.4.1.2.5 UE actions 294
5.4.4.1.3 Evaluation 294
5.4.4.4 Solution #4.4: Fake gNB detection using UL traffic monitoring and System Query 300
5.4.4.4.1 Introduction 300
5.4.4.4.2 Solution details 300
5.4.4.4.3 Evaluation 301
5.4.4.5 Solution #4.5: Prevent User Plane DoS Attack over Air Interface for Small Data 302
5.4.4.5.1 Introduction 302
5.4.4.5.2 Solution details 302
5.4.4.5.3 Evaluation 303
5.4.4.6 Solution #4.6: Security mechanism for deployment scenario of option 3 304
5.4.4.6.1 Introduction 304
5.4.4.6.2 Solution details 304
5.4.4.6.3 Evaluation 305
5.4.4.7 Solution #4.7: Handover procedure for Intra NG (R)AN 305
5.4.4.7.1 Introduction 305
5.4.4.7.2 Solution details 306
5.4.4.7.3 Evaluation 306
5.4.4.8 Solution #4.8: Fake gNB Detection using Identity Based Signature 306
5.4.4.8.1 Overview 306
5.4.4.8.2 Solution Details 307
5.4.4.8.3 Evaluation 309
5.4.4.9 Solution #4.9: Security of Access Stratum (AS) keys on Xn handover 309
5.4.4.9.1 Introduction 309
5.4.4.9.2 Solution details 310
5.4.4.9.3 Evaluation 310
5.4.4.10 Solution #4.10: UE-assisted false base station detection 310
5.4.4.10.1 Introduction 310
5.4.4.10.2 Solution details 310
5.4.4.10.3 Evaluation 311
5.4.4.11 Solution #4.11: Security of sidehaul interfaces 312
5.4.4.11.1 Introduction 312
5.4.4.11.2 Solution details 312
5.4.4.11.3 Evaluation 312
5.4.4.12 Solution #4.12: Security Aspects of Option 3/3a/3x or EN-DC 312
5.4.4.12.1 Introduction 312
5.4.4.12.2 Solution details 312
5.4.4.12.3 Evaluation 315
5.4.4.13 Solution #4.13: Inputs to security algorithms at PDCP layer 315
5.4.4.13.1 Introduction 315
5.4.4.13.2 Solution details 315
5.4.4.13.3 Evaluation 316
5.4.4.14 Solution #4.14: Flexibile mechanism for AS key-change 316
5.4.4.14.1 Introduction 316
5.4.4.14.2 Solution details 316
5.4.4.14.3 Evaluation 318
5.4.4.15 Solution #4.15: Deriving ciphering and integrity keys in 5G 318
5.4.4.15.1 Introduction 318
5.4.4.15.2 Solution details 318
5.4.4.15.3 Evaluation 319
5.4.4.z Solution #4.z: <solution name> 319
5.4.4.z.1 Introduction 319
5.4.4.z.2 Solution details 319
5.4.4.z.3 Evaluation 319
5.4.5 Conclusions 319
5.4.5.1 AS security during RRC idle mode (Key issue #4.1) 319
5.4.5.2 Dual Connectivity architecture options 3/3a/3x (Non-Standalone NR with LTE anchor, EPC connected) 320
5.5 Security area #5: Security within NG-UE 320
5.5.1 Introduction 320
5.5.2 Security assumptions 320

5.5.3 Key issues 320
5.5.3.1 Key issue #5.1: Secure storage and processing of credentials and identities 320
5.5.3.1.1 Key issue details 320
5.5.3.1.2 Security threats 321
5.5.3.1.3 Potential security requirements 321
5.5.3.2 Key issue #5.2: Secure storage and processing of equipment identifier and credentials 322
5.5.3.2.1 Key issue details 322
5.5.3.2.2 Security threats 322
5.5.3.2.3 Potential security requirements 322
5.5.3.3 Key issue #5.3: NG UE supporting different use cases 322
5.5.3.3.1 Key issue details 322
5.5.3.3.2 Security threats 322
5.5.3.3.3 Potential security requirements 322
5.5.3.y Key issue #5.y: <key issue name> 322
5.5.3.y.1 Key issue details 322
5.5.3.y.2 Security threats 322
5.5.3.y.3 Potential security requirements 322
5.5.4 Solutions 322
5.5.4.1 Solution #5.1: Solution for Key Issue 5.1 322
5.5.4.1.1 Introduction 322
5.5.4.1.2 Solution details 323
5.5.4.1.3 Evaluation 323
5.5.4.z Solution #5.z: <solution name> 323
5.5.4.z.1 Introduction 323
5.5.4.z.2 Solution details 323
5.5.4.z.3 Evaluation 323
5.5.5 Conclusions 323
5.6 Security area #6: Authorization 323
5.6.1 Introduction 323
5.6.2 Security assumptions 323
5.6.3 Key issues 323
5.6.3.1 Key issue #6.1: UE authorization 323
5.6.3.1.1 Key issue details 323
5.6.3.1.2 Security threats 324
5.6.3.1.3 Potential security requirements 324
5.6.3.2 Key issue #6.2: Network authorization 324
5.6.3.2.1 Key issue details 324
5.6.3.2.2 Security threats 324
5.6.3.2.3 Potential security requirements 324
5.6.3.3 Key issue #6.3: Authorization decoupled from authentication 325
5.6.3.3.1 Key issue details 325
5.6.3.3.2 Security threats 325
5.6.3.3.3 Potential security requirements 325
5.6.3.y Key issue #6.y: <key issue name> 325
5.6.3.y.1 Key issue details 325
5.6.3.y.2 Security threats 325
5.6.3.y.3 Potential security requirements 325
5.6.4 Solutions 325
5.6.4.1 Solution #6.1: Network authorization by UE 325
5.6.4.1.1 Introduction 325
5.6.4.1.2 Solution details 326
5.6.4.1.3 Evaluation 326
5.6.4.2 Solution #6.2: Dynamic Authorization by Operator/MNO 326
5.6.4.2.1 Introduction 326
5.6.4.2.2 Solution details 326
5.6.4.2.3 Evaluation 327
5.6.4.3 Solution #6.3: Dynamic Authorization by Trusted 3-rd Party 328
5.6.4.3.1 Introduction 328
5.6.4.3.2 Solution details 328
5.6.4.3.3 Evaluation 330
5.6.4.4 Solution #6.4: EAP-based solution for secondary authentication and authorization 330
5.6.4.4.1 Introduction 330

5.6.4.4.2 Solution details 330
5.6.4.4.3 Evaluation 332
5.6.4.z Solution #6.z: <solution name> 332
5.6.4.z.1 Introduction 332
5.6.4.z.2 Solution details 332
5.6.4.z.3 Evaluation 332
5.6.5 Conclusions 332
5.7 Security area #7: Subscription privacy 332
5.7.1 Introduction 332
5.7.2 Security assumptions 333
5.7.3 Key issues 333
5.7.3.1 Key Issue #7.1: Refreshing of temporary subscription identifier 333
5.7.3.1.1 Key issue details 333
5.7.3.1.2 Security threats 334
5.7.3.1.3 Potential security requirements 335
5.7.3.2 Key issue #7.2: Concealing permanent or long-term subscription identifier 335
5.7.3.2.1 Key issue details 335
5.7.3.2.2 Security and privacy threats 337
5.7.3.2.3 Potential security requirements 337
5.7.3.3 Key issue #7.3: Concealing permanent or long-term equipment identifier 337
5.7.3.3.1 Key issue details 337
5.7.3.3.2 Security and privacy threats 338
5.7.3.3.3 Potential security requirements 338
5.7.3.4 Key issue #7.4: Using effective temporary or short-term subscription identifiers 338
5.7.3.4.1 Key issue details 338
5.7.3.4.2 Security and privacy threats 338
5.7.3.4.3 Potential security requirements 338
5.7.3.5 Key issue #7.5: Transmitting permanent identifiers in secure interface 338
5.7.3.5.1 Key issue details 338
5.7.3.5.2 Security threats 339
5.7.3.5.3 Potential security requirements 339
5.7.3.6 Key issue #7.6: Transmitting permanent subscription identifiers only when needed 339
5.7.3.6.1 Key issue details 339
5.7.3.6.2 Security threats 339
5.7.3.6.3 Potential security requirements 339
5.7.3.7 Key issue #7.7: Using effective temporary or short-term equipment identifiers 339
5.7.3.1.7 Key issue details 339
5.7.3.7.2 Security and privacy threats 340
5.7.3.7.3 Potential privacy requirements 340
5.7.3.8 Key issue #7.8: Privacy protection of network slice identifier 340
5.7.3.8.1 Key issue details 340
5.7.3.8.2 Security and privacy threats 340
5.7.3.8.3 Potential security requirements 340
5.7.3.9 Key issue #7.9: Need to protect entire Permanent Identifier. 340
5.7.3.9.1 Key issue details 340
5.7.3.9.2 Security threats 341
5.7.3.9.3 Potential security requirements 341
5.7.3.y Key issue #7.y: <key issue name> 342
5.7.3.y.1 Key issue details 342
5.7.3.y.2 Security threats 342
5.7.3.y.3 Potential security requirements 342
5.7.4 Solutions 342
5.7.4.1 Solution #7.1: UE can request an update of temporary identifier 342
5.7.4.1.1 Introduction 342
5.7.4.1.2 Solution details 342
5.7.4.1.3 Evaluation 342
5.7.4.2 Solution #7.2: UE encrypts permanent identifier sent to network 342
5.7.4.2.1 Introduction 342
5.7.4.2.2 Solution details 342
5.7.4.2.2.1 Background 342
5.7.4.2.2.2 Provisioning and management of keys 343
5.7.4.2.2.3 Revocation 343

5.7.4.2.2.4 Signature algorithms and algorithm selection 343
5.7.4.2.3 Evaluation 343
5.7.4.3 Solution #7.3: Concealing permanent or long-term subscriber identifier by using pseudonyms and public key encryption 343
5.7.4.3.1 Introduction 343
5.7.4.3.2 Solution details 344
5.7.4.3.2.1 General 344
5.7.4.3.2.2 Attach using encrypted IMSI ($IMSI_{Enc}$) 344
5.7.4.3.2.3 Attach using pseudo IMSI ($IMSI_{Pseudo}$) 345
5.7.4.3.2.4 Handling abnormal cases 346
5.7.4.3.2.4.1 Invalid $IMSI_{Pseudo}$ 346
5.7.4.3.2.4.2 Already assigned $IMSI_{Pseudo}$ 347
5.7.4.3.3 Evaluation 348
5.7.4.4 Solution #7.4: Privacy enhanced Mobile Subscription identifier (PMSI) 348
5.7.4.4.1 Introduction 348
5.7.4.4.2 Solution details 348
5.7.4.4.3 PMSI initialization 351
5.7.4.4.4 Evaluation 351
5.7.4.5 Solution #7.5: Effective generation of temporary or short-term identifiers using channel estimation 352
5.7.4.5.1 Introduction 352
5.7.4.5.2 Solution details 352
5.7.4.5.3 Evaluation 353
5.7.4.6 Solution #7.6: Parameters for Refreshing of temporary subscription identifier 353
5.7.4.6.1 Introduction 353
5.7.4.6.2 Solution details 354
5.7.4.6.3 Evaluation 354
5.7.4.7 Solution #7.7: Revealing permanent or long-term subscriber identifier to a serving PLMN 354
5.7.4.7.1 Introduction 354
5.7.4.7.2 Solution variants 354
5.7.4.7.2.1 Solution 7.7-A: Home PLMN authenticates UE 354
5.7.4.7.2.2 Solution 7.7-B: Serving PLMN authenticates UE 354
5.7.4.7.3 Evaluation 355
5.7.4.8 Solution #7.8: Opportunistic encryption for IMSI exchange 355
5.7.4.8.1 Introduction 355
5.7.4.8.2 Solution details 355
5.7.4.8.3 Evaluation 356
5.7.4.9 Solution #7.9 Adding the Diffie-Hellman key exchange process to the attach procedure 356
5.7.4.9.1 Introduction 356
5.7.4.9.2 Solution details 357
5.7.4.9.3 Evaluation 359
5.7.4.9.3.1 Security 359
5.7.4.9.3.2 Complexity 359
5.7.4.9.3.3 Compatibility 359
5.7.4.9.3.4 Efficiency 360
5.7.4.10 Solution #7.10: Applying DHIES to the attach procedure 360
5.7.4.10.1 Introduction 360
5.7.4.10.2 Solution details 360
5.7.4.10.3 Evaluation 362
5.7.4.10.3.1 Security 363
5.7.4.10.3.2 Complexity 363
5.7.4.10.3.3 Compatibility 363
5.7.4.10.3.4 Efficiency 364
5.7.4.11 Solution #7.11: Protect the Permanent or Long Term User Identity with Public Key Technologies 364
5.7.4.11.1 Introduction 364
5.7.4.11.2 Solution details 364
5.7.4.11.2.1 Protect the Permanent or Long Term Identifiers with a termination point at AN 364
5.7.4.11.2.2 Protect the Permanent or Long Term Identifiers with a termination point at Core Network 365
5.7.4.11.3 Evaluation 366

5.7.4.12 Solution #7.12: Mechanisms of Pseudo-IMSI for hiding long-term identifier 366
5.7.4.12.1 Introduction 366
5.7.4.12.2 Solution details 367
5.7.4.12.2.1 Introduction of Pseudo-IMSI (P-IMSI) by replacing MSIN-part by Mobile Station PseudoNym (MSPN) 367
5.7.4.12.2.2 NextGen signalling support for P-IMSI 367
5.7.4.12.2.3 Collision prevention 368
5.7.4.12.2.4 Retention of computed MSPN values 368
5.7.4.12.2.5 Description of the HSS process steps 368
5.7.4.12.2.6 Description of the USIM Process Steps 369
5.7.4.12.3 Evaluation 371
5.7.4.13 Solution #7.13: Refreshing CN short-term subscriber identifiers 371
5.7.4.13.1 Introduction 371
5.7.4.13.2 Solution details 371
5.7.4.13.2.1 General 371
5.7.4.13.2.2 Solution Variant-A 371
5.7.4.13.2.3 Solution Variant-B 372
5.7.4.13.3 Evaluation 373
5.7.4.14 Solution #7.14: Privacy protection of permanent or long-term subscription identifier using ABE 373
5.7.4.14.1 Introduction 373
5.7.4.14.2 Solution details 374
5.7.4.14.2.1 General 374
5.7.4.14.2.2 Option 1 374
5.7.4.14.2.3 Option 2 375
5.7.4.14.3 Evaluation 375
5.7.4.15 Solution #7.15: Encrypting IMSI based on Elliptic Curve Integrated Encryption Scheme (ECIES) 376
5.7.4.15.1 Introduction 376
5.7.4.15.2 Solution details 376
5.7.4.15.3 Evaluation 377
5.7.4.16 Solution #7.16: Mechanism for temporary identifier assignment 378
5.7.4.16.1 Introduction 378
5.7.4.16.2 Solution details 379
5.7.4.16.3 Evaluation 379
5.7.4.z Solution #7.z: <solution name> 380
5.7.4.z.1 Introduction 380
5.7.4.z.2 Solution details 380
5.7.4.z.3 Evaluation 380
5.7.5 Conclusions 380
5.8 Security area #8: Network slicing security 380
5.8.1 Introduction 380
5.8.2 Security assumptions 380
5.8.3 Key issues 381
5.8.3.1 Key Issue #8.1: Security isolation of network slices 381
5.8.3.1.1 Key issue details 381
5.8.3.1.2 Security threats 382
5.8.3.1.3 Potential security requirements. 382
5.8.3.2 Key Issue #8.2: Security mechanism differentiation for network slices 382
5.8.3.2.1 Key issue details 382
5.8.3.2.2 Security threats 382
5.8.3.2.3 Potential security requirements 383
5.8.3.3 Key Issue #8.3: Security on UEs' access to slices 383
5.8.3.3.1 Key issue details 383
5.8.3.3.2 Security threats 386
5.8.3.3.3 Potential security requirements 386
5.8.3.4 Key Issue #8.4: Security on sensitive network elements 386
5.8.3.4.1 Key issue details 386
5.8.3.4.2 Security threats 386
5.8.3.4.3 Potential security requirements 387
5.8.3.5 Key Issue #8.5: Security on management of slicing 387
5.8.3.5.1 Key issue details 387

5.8.3.5.2 Security threats 387
5.8.3.5.3 Potential security requirements 387
5.8.3.6 Key Issue #8.6: Security on interacting with third party 387
5.8.3.6.1 Key issue details 387
5.8.3.6.2 Security threats 387
5.8.3.6.3 Potential security requirements 387
5.8.3.7 Key Issue #8.7: Security of inter slice communications 387
5.8.3.7.1 Key issue details 387
5.8.3.7.2 Security threats 387
5.8.3.7.3 Security requirements 388
5.8.3.8 Key Issue #8.8: Virtualization security 388
5.8.3.8.1 Key issue details 388
5.8.3.8.2 Security threats 388
5.8.3.8.3 Security requirements 388
5.8.3.y Key issue #8.y: <key issue name> 388
5.8.3.y.1 Key issue details 388
5.8.3.y.2 Security threats 388
5.8.3.y.3 Potential security requirements 388
5.8.4 Solutions 388
5.8.4.1 Solution #8.1: Security isolation of network slices, Security mechanism differentiation 388
5.8.4.1.1 Introduction 388
5.8.4.1.2 Solution details 389
5.8.4.1.3 Evaluation 390
5.8.4.2 Solution #8.2: UE Authentication only by AUSF 390
5.8.4.2.1 Introduction 390
5.8.4.2.2 Solution details 390
5.8.4.3.3 Evaluation 392
5.8.4.3 Solution #8.3: UE Authentication by AUSF and NSI 392
5.8.4.3.1 Introduction 392
5.8.4.3.2 Solution details 392
5.8.4.4 Solution #8.4: UE Authentication by NSI 393
5.8.4.4.1 Introduction 393
5.8.4.4.2 Solution details 393
5.8.4.4.3 Evaluation 394
5.8.4.5 Solution #8.5: UE access network and slices 394
5.8.4.5.1 Introduction 394
5.8.4.5.2 Solution details 395
5.8.4.5.2.1 Attach procedure 396
5.8.4.5.2.2 Subsequent NG1 signalling with NAS SMC procedure (generic) 397
5.8.4.5.3 Evaluation 398
5.8.4.6 Solution#8.6: UE authentication and initial attach to a network slice using NSSAI 398
5.8.4.7 Solution #8.7: Security architecture for network slice 399
5.8.4.7.1 Introduction 399
5.8.4.7.2 Solution details 399
5.8.4.7.2.1 Architecture 399
5.8.4.7.2.2 Key Hierarchy 400
5.8.4.7.2.3 Procedure 401
5.8.4.7.3 Evaluation 403
5.8.4.8 Solution #8.8: UE access network and slices 403
5.8.4.8.1 Introduction 403
5.8.4.8.2 Solution overview 403
5.8.4.8.3 Non-roaming case 403
5.8.4.8.4 Roaming case 405
5.8.4.9 Solution #8.9: Security mechanism differentiation for network slices 405
5.8.4.9.1 Introduction 405
5.8.4.9.2 Security mechanism differentiation in authentication 405
5.8.4.9.4 Evaluation 407
5.8.4.10 Solution #8.10: Network authentication supporting network slices 407
5.8.4.10.1 Introduction 407
5.8.4.10.2 Solution details 408
5.8.4.10.3 Evaluation 409
5.8.4.11 Solution #8.11: Slice Authentication 409

5.8.4.11.1 Introduction 409
5.8.4.11.2 Solution details 409
5.8.4.11.3 Evaluation 410
5.8.4.12 Solution #8.12: PCO based authentication and authorization for Slice access 410
5.8.4.12.1 Introduction 410
5.8.4.12.2 Solution details 411
5.8.4.12.3 Evaluation 411
5.8.4.13 Solution #8.13: Slice-specific NAS keys 412
5.8.4.13.1 Introduction 412
5.8.4.13.2 Solution details 412
5.8.4.13.3 Evaluation 413
5.8.4.z Solution #8.z: <solution name> 413
5.8.4.z.1 Introduction 413
5.8.4.z.2 Solution details 413
5.8.4.z.3 Evaluation 413
5.8.5 Conclusions 413
5.9 Security area #9: Relay security 413
5.9.1 Introduction 413
5.9.2 Security assumptions 413
5.9.3 Key issues 414
5.9.3.1 Key Issue #9.1: Mutual authentication of remote UE and network over a relay 414
5.9.3.1.1 Key issue details 414
5.9.3.1.2 Security threats 414
5.9.3.1.3 Potential security requirements 414
5.9.3.2 Key Issue #9.2: Integrity and confidentiality protection of remote UEs 414
5.9.3.2.1 Key issue details 414
5.9.3.2.2 Security threats 414
5.9.3.2.3 Potential security requirements 414
5.9.3.3 Key Issue #9.3: Remote UE session continuity 414
5.9.3.3.1 Key issue details 414
5.9.3.3.2 Security threats 414
5.9.3.3.3 Potential security requirements 415
5.9.3.y Key issue #9.y: <key issue name> 415
5.9.3.y.1 Key issue details 415
5.9.3.y.2 Security threats 415
5.9.3.y.3 Potential security requirements 415
5.9.4 Solutions 415
5.9.4.z Solution #9.z: <solution name> 415
5.9.4.z.1 Introduction 415
5.9.4.z.2 Solution details 415
5.9.4.z.3 Evaluation 415
5.9.5 Conclusions 415
5.10 Security area #10: Network domain security 415
5.10.1 Introduction 415
5.10.2 Security assumptions 416
5.10.3 Key issues 416
5.10.3.1 Key Issue #10.1: Network and NE communication security 416
5.10.3.1.1 Key issue details 416
5.10.3.1.2 Security threats 417
5.10.3.1.3 Potential security requirements 417
5.10.3.2 Key issue #10.2: Interconnection Security 418
5.10.3.2.1 Key issue details 418
5.10.3.2.2 Security threats 418
5.10.3.2.3 Potential security requirements 419
5.10.3.y Key issue #10.y: <key issue name> 420
5.10.3.y.1 Key issue details 420
5.10.3.y.2 Security threats 420
5.10.3.y.3 Potential security requirements 420
5.10.4 Solutions 420
5.10.4.1 Solution #10.1: Circles of Trust 420
5.10.4.1.1 Introduction 420
5.10.4.1.2 Solution details 420

5.10.4.1.3 Evaluation 423
5.10.4.2 Solution #10.2: Public-key encryption of keys in authentication vectors 423
5.10.4.2.1 Introduction 423
5.10.4.2.2 Solution details 423
5.10.4.2.3 Evaluation 423
5.10.4.z Solution #10.z: <solution name> 424
5.10.4.z.1 Introduction 424
5.10.4.z.2 Solution details 424
5.10.4.z.3 Evaluation 424
5.10.5 Conclusions 424
5.11 Security area #11: Security visibility and configurability 424
5.11.1 Introduction 424
5.11.2 Security assumptions 424
5.11.3 Key issues 425
5.11.3.1 Key Issue #11.1: Service-dependent security requirements 425
5.11.3.1.1 Key issue details 425
5.11.3.1.2 Security threats 425
5.11.3.1.3 Potential security requirements 425
5.11.3.2 Key Issue #11.2: User awareness of security 425
5.11.3.2.1 Key issue details 425
5.11.3.2.2 Security threats 425
5.11.3.2.3 Potential security requirements 425
5.11.3.3 Key Issue #11.3: User control of security 426
5.11.3.3.1 Key issue details 426
5.11.3.3.3 Potential security requirements 426
5.11.3.4 Key Issue #11.4: On demand security framework 426
5.11.3.4.1 Key issue details 426
5.11.3.4.2 Security threats 427
5.11.3.4.3 Potential security requirements 427
5.11.3.y Key issue #11.y: <key issue name> 427
5.11.3.y.1 Key issue details 427
5.11.3.y.2 Security threats 427
5.11.3.y.3 Potential security requirements 427
5.11.4 Solutions 427
5.11.4.1 Solution #11.1: Device API allowing an application to state security requirements 427
5.11.4.1.1 Introduction 427
5.11.4.1.2 Solution details 428
5.11.4.1.3 Evaluation 428
5.11.4.2 Solution #11.2: Security visibility solution using security indication policy 428
5.11.4.2.1 Introduction 428
5.11.4.2.2 Solution details 428
5.11.4.2.3 Evaluation 429
5.11.4.3 Solution #11.3: Security configurability solution using security control policy 429
5.11.4.3.1 Introduction 429
5.11.4.3.2 Solution details 429
5.11.4.3.3 Evaluation 429
5.11.4.4 Solution #11.4: UE configuration of key and identifier refresh 430
5.11.4.4.1 Introduction 430
5.11.4.4.2 Solution details 430
5.11.4.4.3 Evaluation 431
5.11.4.z Solution #11.z: <solution name> 431
5.11.4.z.1 Introduction 431
5.11.4.z.2 Solution details 431
5.11.4.z.3 Evaluation 431
5.11.5 Conclusions 431
5.12 Security area #12: Credential provisioning 431
5.12.1 Introduction 431
5.12.2 Security assumptions 431
5.12.3 Key issues 431
5.12.3.1 Key issue #12.1: Credential provisioning 431
5.12.3.1.1 Key issue details 431
5.12.3.1.2 Security threats 432

5.12.3.1.3 Potential security requirements 432
5.12.3.2 Key Issue #12.2: Remote credential provisioning for IoT devices 432
5.12.3.2.1 Key issue details 432
5.12.3.2.2 Security threats 432
5.12.3.2.3 Potential security requirements 433
5.12.3.y Key issue #12.y: <key issue name> 433
5.12.3.y.1 Key issue details 433
5.12.3.y.2 Security threats 433
5.12.3.y.3 Potential security requirements 433
5.12.4 Solutions 433
5.12.4.1 Solution #12.1: Remote credential provisioning – Add Headless IoT device to existing user's MNO subscription 433
5.12.4. 1.1 Overview 433
5.12.4.1.2 Solution Details 433
5.12.4.1.3 Evaluation 435
5.12.4.2 Solution #12.2: Remote credential provisioning - for headed devices using captive portal technique 435
5.12.4.2.1 Overview 435
5.12.4.2.2 Solution Details. 435
5.12.4.2.3 Evaluation 437
5.12.4.3 Solution #12.3: Secure Mechanism to Achieve Remote Credential Provisioning for IoT devices 437
5.12.4.3.1 Introduction 437
5.12.4.3.2 Solution details 437
5.12.4.3.3 Evaluation 439
5.12.4.4 Solution #12.4 Authentication Procedure for credential provisioning 439
5.12.4.4.1 Introduction 439
5.12.4.4.2 Reference Architecture for connectivity for credential provisioning 440
5.12.4.4.3 Authentication procedure for credential provisioning 441
5.12.4.5.2.1 Credentials and identifiers used for network access for credentials provisioning 442
5.12.4.5.2.2 Network access for credentials provisioning 442
5.12.4.z Solution #12.z: <solution name> 443
5.12.4.z.1 Introduction 443
5.12.4.z.2 Solution details 444
5.12.4.z.3 Evaluation 444
5.12.5 Conclusions 444
5.13 Security area #13: Security for Interworking and Migration 444
5.13.1 Introduction 444
5.13.2 Security assumptions 445
5.13.3 Key issues 445
5.13.3.1 Key issue #13.1: Security for Handovers 445
5.13.3.1.1 Key issue details 445
5.13.3.1.2 Security threats 445
5.13.3.1.3 Potential security requirements 445
5.13.3.2 Key issue #13.2: Security for Idle Mode Mobility 445
5.13.3.2.1 Key issue details 445
5.13.3.2.2 Security threats 446
5.13.3.2.3 Potential security requirements 446
5.13.3.3 Key issue #13.3: Security aspects of migration 446
5.13.3.3.1 Key issue details 446
5.13.3.3.2 Security threats 446
5.13.3.3.3 Potential security requirements 446
5.13.3.4 Key issue #13.4: Bidding down to an older 3GPP generation or a non-3GPP access technology 446
5.13.3.4.1 Key issue details 446
5.13.3.4.2 Security threats 446
5.13.3.4.3 Potential security requirements 446
5.13.4 Solutions 447
5.13.4.1 Solution #13.1: 447
5.13.4.1.1 Introduction 447
5.13.4.1.2 Solution details 447
5.13.4.1.3 Evaluation 447

5.13.4.z Solution #13.z: <solution name> 447
5.13.4.z.1 Introduction 447
5.13.4.z.2 Solution details 447
5.13.4.z.3 Evaluation 447
5.13.5 Conclusions 447
5.14 Security area #14: Security aspects of small data 447
5.14.1 Introduction 447
5.14.2 Security Assumptions 447
5.14.4 Solutions 448
5.14.5 Key issues 448
5.14.3.1 Key Issue #14.1: Access security for small data session 448
5.14.3.1.1 Key issue details 448
5.14.3.1.2 Security threats 448
5.14.3.1.3 Potential security requirements 448
5.14.3.2 Key Issue #14.2: Security for data over the small data interface. 448
5.14.3.2.1 Key issue details 448
5.14.3.2.2 Security threats 448
5.14.3.2.3 Potential security requirements 449
5.14.3.3 Key Issue #14.3: Restricting small data resource utilization 449
5.14.3.3.1 Key issue details 449
5.14.3.3.2 Security threats 449
5.14.3.3.3 Potential security requirements 449
5.14.3.4 Key Issue #14.4: Small data context retention 449
5.14.3.4.1 Key issue details 449
5.14.3.4.2 Security threats 449
5.14.3.4.3 Potential security requirements 449
5.14.4 Solutions 449
5.14.4.z Solution #14.z: <solution name> 449
5.14.4.z.1 Introduction 449
5.14.4.z.2 Solution details 450
5.14.4.z.3 Evaluation 450
5.14.5 Conclusions 450
5.15 Security area #15: Broadcast/Multicast Security 450
5.15.1 Introduction 450
5.15.2 Security assumptions 450
5.15.3 Key issues 450
5.15.3.1 Key issue #15.1: Broadcast/Multicast capabilities 450
5.15.3.1.1 Key issue details 450
5.15.3.1.2 Security threats 450
5.15.3.1.3 Potential security requirements 450
5.15.3.2 Key issue #15.2: Usage of MBMS security 450
5.15.3.2.1 Key issue details 450
5.15.3.2.2 Security threats 451
5.15.3.2.3 Potential security requirements 451
5.15.4 Solutions 451
5.15.4.z Solution #15.z: <solution name> 451
5.15.4.z.1 Introduction 451
5.15.4.z.2 Solution details 451
5.15.4.z.3 Evaluation 451
5.15.5 Conclusions 451
5.16 Security area #16 Management security 451
5.16.2 Security assumptions 451
5.16.3 Key issues 452
5.16.3.1 Key issue # 16.1: management plane communication protection 452
5.16.3.1.1 Key issue details 452
5.16.3.1.2 Security threats 452
5.16.3.1.3 Potential security requirements 452
5.16.3.2 Key issue #16.2: network element deployment security 452
5.16.3.2.1 Key issue details 452
5.16.3.2.2 Security threats 452
5.16.3.2.3 Potential security requirements 453
5.16.3.3 Key issue #16.3: Network slice life-cycle security 453

5.16.3.3.1 Key issue details 453
5.16.3.3.2 Security threats 453
5.16.3.3.3 Potential security requirements 454
5.16.3.y Key issue #16.y: <key issue name> 454
5.16.3.y.1 Key issue details 454
5.16.3.y.2 Security threats 454
5.16.3.y.3 Potential security requirements 454
5.16.4 Solutions 454
5.16.4.z Solution #16.z: <solution name> 454
5.16.4.z.1 Introduction 454
5.16.4.z.2 Solution details 455
5.16.4.z.3 Evaluation 455
5.16.5 Conclusions 455
5.17 Security area #17: Cryptographic algorithms 455
5.17.1 Introduction 455
5.17.2 Security assumptions 455
5.17.3 Key issues 455
5.17.3.1 Key issue #17.1: Cryptographic algorithms for backward compatibility 455
5.17.3.1.1 Key issue details 455
5.17.3.1.2 Security threats 455
5.17.3.1.3 Potential security requirements 455
5.17.3.2 Key issue #17.2: Quantum safe cryptography 455
5.17.3.2.1 Key issue details 455
5.17.3.2.2 Security threats 456
5.17.3.2.3 Potential security requirements 456
5.17.3.y Key issue #17.y: <key issue name> 457
5.17.3.y.1 Key issue details 457
5.17.3.y.2 Security threats 457
5.17.3.y.3 Potential security requirements 457
5.17.4 Solutions 457
5.17.4.1 Solution #17.1: Incorporate a quantum safe algorithm from day one 457
5.17.4.1.1 Introduction 457
5.17.4.1.2 Solution details 457
5.17.4.1.3 Evaluation 457
5.17.4.2 Solution #17.2: Message flexibility 457
5.17.4.2.1 Introduction 457
5.17.4.2.2 Solution details 458
5.17.4.2.3 Evaluation 458
5.17.4.3 Solution #17.3: Updating algorithms to be used by home network and UE 458
5.17.4.3.1 Introduction 458
5.17.4.3.2 Solution details 458
5.17.4.3.3 Evaluation 458
5.17.4.4 Solution #17.4: Secure negotiation of algorithms to be used by home network and UE 459
5.17.4.4.1 Introduction 459
5.17.4.4.2 Solution details 459
5.17.4.4.3 Evaluation 459
5.17.4.5 Solution #17.5: Secure negotiation of algorithms to be used by serving network and UE 459
5.17.4.5.1 Introduction 459
5.17.4.5.2 Solution details 460
5.17.4.5.3 Evaluation 460
5.17.4.z Solution #x.z: <solution name> 460
5.17.4.z.1 Introduction 460
5.17.4.z.2 Solution details 460
5.17.4.z.3 Evaluation 460
5.17.5 Conclusions 460
5.x Security area #x: <security area name> 460
5.x.1 Introduction 460
5.x.2 Security assumptions 461
5.x.3 Key issues 461
5.x.3.y Key issue #x.y: <key issue name> 461
5.x.3.y.1 Key issue details 461
5.x.3.y.2 Security threats 461

5.x.3.y.3 Potential security requirements 461
5.x.4 Solutions 461
5.x.4.z Solution #x.z: <solution name> 461
5.x.4.z.1 Introduction 461
5.x.4.z.2 Solution details 461
5.x.4.z.3 Evaluation 461
5.x.5 Conclusions 461

6 Conclusions 461

Annex A: Focus areas, and rationales behind them 462

Annex B: Guiding principles 463

B.1 Introduction 463

B.2 Guiding principles 463
B.2.1 Usage of the wording 'security level' for a system: 463
B.2.1.1 Issue details 463
B.2.1.2 Recommendations 463
B.2.2 Comparison of 'security levels' between building blocks or slices 463
B.2.2.1 Issue details 463
B.2.2.2 Recommendation 463
B.2.3 Threats - functional requirements - security requirements 464
B.2.3.1 Issue details 464
B.2.3.2 Recommendation 464
B.2.4 Solutions and Evaluations 464
B.2.4.1 Solution Location 464
B.2.4.1 Solution Presentation 464

Annex C: Trust model study for network slicing 465

C.1 Introduction 465

C.2 Trust model 465

C.3 Trust establishment 466
C.3.1 Analysis 466
C.3.2 The infrastructure layer 466
C.3.3 The virtualization layer 466
C.3.4 The network function layer 466

C.4 Trust maintenance 466
C.4.1 Analysis 466
C.4.2 The Accesses 466
C.4.3 The Data flows 467
C.4.4 The network slices 467

Annex D: Prioritization of key issues 468

Annex E: Questions and Interim Agreements 475
E.1 Questions and Interim Agreements for security area #1 475
E.1.1 Questions and Interim Agreements for Key Issue #1.1 475
E.1.2 Questions and Interim Agreements for Key Issue #1.2 475
E.1.2.1 Need for a security anchor 475
E.1.2.1.1 Description of Question 475
E.1.2.1.2 Interim Agreement 475
E.1.2.2 Separation of security anchor from other entities 475
E.1.2.2.1 Description of Question 475
E.1.2.2.2 Interim Agreement 475
E.1.3 Questions and Interim Agreements for Key Issue #1.3 475
E.1.3.0 Questions in other clauses affecting this key issue 475
E.1.3.1 Support of User plane integrity between UE and network 475
E.1.3.1.1 Description of Question 475
E.1.3.1.2 Interim Agreement 475

E.1.3.2 How should use of the feature be negotiated between UE and network 476
E.1.3.2.1 Description of Question 476
E.1.3.2.2 Interim Agreement 476
E.1.4 Questions and Interim Agreements for Key Issue #1.4 476
E.1.4.0 Questions in other clauses affecting this key issue 476
E.1.4.1 Support of UP confidentiality protection in the UE and the Network 476
E.1.4.1.1 Description of Question 476
E.1.4.1.2 Interim Agreement 476
E.1.5 Questions and Interim Agreements for Key Issue #1.5 476
E.1.5.0 Questions in other clauses affecting this key issue 476
E.1.5.1 Shall CP integrity be mandatory to support / use by 5G UEs, 5G networks? 476
E.1.5.1.1 Description of Question 476
E.1.5.1.2 Interim Agreement 477
E.1.5.2 Shall integrity for all NAS messages terminate in a single point? 477
E.1.5.2.1 Description of Question 477
E.1.5.2.2 Interim Agreement 477
E.1.6 Questions and Interim Agreements for Key Issue #1.6 477
E.1.6.0 Questions in other clauses affecting this key issue 477
E.1.6.1 Shall CP confidentiality be mandatory to support / use by 5G UEs, 5G networks? 477
E.1.6.1.1 Description of Question 477
E.1.6.1.2 Interim Agreement 477
E.1.6.2 Shall confidentiality for all NAS messages terminate in a single point? 477
E.1.6.2.1 Description of Question 477
E.1.6.2.2 Interim Agreement 478
E.1.7 Questions and Interim Agreements for Key Issue #1.7 478
E.1.8 Questions and Interim Agreements for Key Issue #1.8 478
E.1.8.0 Questions in other clauses affecting this key issue 478
E.1.8.1 Private keys in the UE 478
E.1.8.1.1 Description of Question 478
E.1.8.1.2 Interim Agreement 478
E.1.8.2 Public network keys 478
E.1.8.2.1 Description of Question 478
E.1.8.2.2 Interim Agreement 478
E.1.9 Questions and Interim Agreements for Key Issue #1.9 478
E.1.9.0 Questions in other clauses affecting this key issue 478
E.1.9.1 Security features for the AN-CN control plane 478
E.1.9.1.1 Description of Question 478
E.1.9.1.2 Interim Agreement 478
E.1.10 Questions and Interim Agreements for Key Issue #1.10 479
E.1.10.0 Questions in other clauses affecting this key issue 479
E.1.10.1 Security features for the AN-CN user plane 479
E.1.10.1.1 Description of Question 479
E.1.10.1.2 Interim Agreement 479
E.1.11 Questions and Interim Agreements for Key Issue #1.11 479
E.1.11.0 Questions in other clauses affecting this key issue 479
E.1.11.1 Security features for the CN-CN control plane 479
E.1.11.1.1 Description of Question 479
E.1.11.1.2 Interim Agreement 479
E.1.12 Questions and Interim Agreements for Key Issue #1.12 479
E.1.12.0 Questions in other clauses affecting this key issue 479
E.1.12.1 Security features for the CN-CN user plane 479
E.1.12.1.1 Description of Question 479
E.1.12.1.2 Interim Agreement 479
E.1.13 Questions and Interim Agreements for Key Issue #1.13 480
E.1.13.0 Questions in other clauses affecting this key issue 480
E.1.13.1 Security Implications to Achieve Low Latency 480
E.1.13.1.1 Description of Question 480
E.1.13.1.2 Interim Agreement 480
E.1.14 Questions and Interim Agreements for Key Issue #1.14 480
E.1.14.0 Questions in other clauses affecting this key issue 480
E.1.14.1 Security for serving core network functions in a less secure location 480
E.1.14.1.1 Description of Question 480

E.1.14.1.2 Interim Agreement 480
E.1.15 Questions and Interim Agreements for Key Issue #1.15 480
E.1.15.0 Questions in other clauses affecting this key issue 480
E.1.15.1 Location of UP security termination point 480
E.1.15.1.1 Description of Question 480
E.1.15.1.2 Interim Agreement 481
E.1.15.2 Flexibility of UP security termination points 481
E.1.15.2.1 Description of Question 481
E.1.15.2.2 Interim Agreement 481
E.1.19 Questions and Interim Agreements for Key Issue #1.19 481
E.1.19.0 Questions in other clauses affecting this key issue 481
E.1.19.1 Untrusted non-3GPP access 481
E.1.19.1.1 Description of Question 481
E.1.19.1.2 Interim Agreement 481
E.1.20 Questions and Interim Agreements for Key Issue #1.20 481
E.1.20.0 Questions in other clauses affecting this key issue 481
E.1.20.1 Trusted non-3GPP access 481
E.1.20.1.1 Description of Question 481
E.1.20.1.2 Interim Agreement 481
E.2 Questions and Interim Agreements for security area #2 482
E.2.1 Questions and Agreements for Key Issue #2.1 Authentication Framework 482
E.2.1.0 Questions in other clauses affecting this key issue 482
E.2.1.1 Support for AKA and its variants for primary authentication 482
E.2.1.1.1 Description of Question 482
E.2.1.1.2 Interim Agreement 482
E.2.1.2 Support for EAP framework for primary authentication 483
E.2.1.2.1 Description of Question 483
E.2.1.2.2 Interim Agreement 483
E.2.1.3 The choice of EAP methods 483
E.2.1.3.1 Description of Question 483
E.2.1.3.2 Interim Agreement 483
E.2.1.4 Creating an anchor key through primary authentication 483
E.2.1.4.1 Description of Question 483
E.2.1.4.2 Interim Agreement 483
E.2.1.5 Support for secondary authentication 484
E.2.1.5.1 Description of Question 484
E.2.1.5.2 Interim Agreement 484
E.2.2 Questions and Agreements for Key Issue #2.2 reducing the impact of secret key leakage 484
E 2.2.0 Questions in other clauses affecting this key issue 484
E.2.2.1 Support to reduce the impact of secret key leakage 484
E.2.2.1.1 Description of Question 484
E.2.2.1.2 Interim Agreement 484
E.4 Questions and Interim Agreements for security area #4 484
E.4.1 Questions and Interim Agreements for Key Issue #4.1 484
E.4.1.1 Prevention of false base station attack during RRC idle mode 484
E.4.1.1.1 Description of question 484
E.4.1.1.2 Interim agreement 484
E.4.1.2 Detection of false base station attack during RRC idle mode 484
E.4.1.2.1 Description of question 484
E.4.1.2.2 Interim agreement 485
E.4.2 Questions and Interim Agreements for Key Issue #4.2 485
E.4.3 Questions and Interim Agreements for Key Issue #4.3 485
E.4.3.1 The inputs to the security algorithms for Option 3 485
E.4.3.1.1 Description of Question 485
E.4.3.1.2 Interim Agreement 485
E.4.4 Questions and Interim Agreements for Key Issue #4.4 485
E.4.5 Questions and Interim Agreements for Key Issue #4.5 485
E.4.6 Questions and Interim Agreements for Key Issue #4.6 485
E.4.7 Questions and Interim Agreements for Key Issue #4.7 485
E.4.8 Questions and Interim Agreements for Key Issue #4.8 485
E.4.9 Questions and Interim Agreements for Key Issue #4.9 485
E.4.10 Questions and interim agreements for key issue #4.10 485

E.4.10.1 Security of sidehaul (Xn and Xx) interfaces 485
E.4.10.1.1 Description of question 485
E.4.10.1.2 Interim agreement 485
E.4.11 Questions and interim agreements for key issue #4.11 485
E.4.11.1 Flexibility of retaining or changing AS security keys during HO 485
E.4.11.1.1 Description of question 485
E.4.11.1.2 Interim agreement 486
E.4.12 Questions and interim agreements for key issue #4.12 486
E.4.13 Questions and interim agreements for key issue #4.13 486
E.4.13.1 Prevention of radio jamming attack 486
E.4.13.1.1 Description of question 486
E.4.13.1.2 Interim agreement 486
E.4.13.2 Detection of radio jamming attack 486
E.4.13.2.1 Description of question 486
E.4.13.2.2 Interim agreement 486
E.4.14 Questions and interim agreements for key issue #4.14 486
E.4.14.1 Addressing privacy of RAN level temporary identifiers 486
E.4.14.1.1 Description of question 486
E.4.14.1.2 Interim agreement 486
E.5 Questions and Interim Agreements for security area #5 486
E.5.1 Questions and Interim Agreements for Key Issue #5.1 486
E.5.1.0 Questions in other clauses affecting this key issue 486
E.5.1.1 Storage of Credentials 486
E.5.1.1.1 Description of Question 486
E.5.1.1.2 Interim Agreement 487
E.17 Questions and Interim Agreements for security area #17 487
E.17.1 Questions and Interim Agreements for cryptographic algorithms 487
E.17.1.1 Choice for cryptographic algorithms 487
E.17.1.1.1 Description of Question 487
E.17.1.1.2 Interim Agreement 487
E.17.1.2 5G signalling supporting to carry 256-bit keys 487
E.17.1.2.1 Description of Question 487
E.17.1.2.2 Interim Agreement 487

Annex F: Comparison on non 3GPP access solutions 488

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

The 3GPP network operators are striving to accommodate continuously fast increasing data (i.e., user information transfer) traffic demand resulting from the support of existing services such as Internet access, voice, and multimedia communication. In addition, new services such as Internet of Things (IoT), cloud-based services, industrial control, autonomous driving, mission critical communications, etc., are emerging. Such services may require, for example, massive connectivity, extreme broadband, ultra-low latency, ultra-high reliability, and enhanced group communication. Those requirements differ dramatically from the ones that defined current network traffic and service models and pose great challenges for existing networks.

It is expected that network functions will run as software components on operators' telco-cloud systems rather than using dedicated hardware components. The architecture should therefore be as cloud-friendly as possible, to improve distribution of processing by separation of control from data forwarding.

For the agile introduction of new technology, one driver is to allow independent evolution of radio and the core network. Another driver is to facilitate architecture convergence between the 3GPP access and other access technologies (e.g. WLAN, Fixed Broadband Access).

There are already network architecture aspects investigated by other organizations, e.g., 4G Americas' Recommendations on 5G Requirements and Solutions [14], NGMN 5G White Paper [10], 5G Forum Korea's White Paper on 5G Vision Requirements and Enabling Technologies[15], and Chinese IMT-2020 (5G) Promotion Group 5G White Paper on Network Technology Architecture [16], FCC requirements on 5G [17] as well as white papers published by companies.

3GPP TR 22.864 [6] identifies use cases and service/operational requirements for next generation networks.

All the above create the need for studying the next generation 3GPP system architecture (including improvements and optimizations on the existing architecture) to achieve a simple, flexible, scalable, secure and extensible architecture with high overall efficiency for all types of communication services of significantly differing traffic characteristics and with high flexibility for deploying networks and network slices of different characteristics for serving various user and service needs adequately and efficiently.

1 Scope

In the scope of this TR are the threats, potential requirements and solutions for the security of next generation mobile networks.

The work will include:

- Collection, analysis and further investigation of potential security threats and requirements for the next generation systems, based on the service, architectural and radio related requirements for the next generation mobile networks.
- Investigation of the security architecture and access security.

The complete or partial conclusions of this study will form the basis for the normative work and/or for any further study.

The security threats and requirements, and the security architecture may additionally include standalone security topics. These topics may not be covered by the security work described above but they shall not be in conflict with service, architectural or radio related requirements for next generation mobile networks. It is part of the study to determine whether such topics need to be dealt with, and, if so, what they are.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 23.799: "Study on Architecture for Next Generation System".

[3] 3GPP TR 22.861: "Feasibility Study on New Services and Markets Technology Enablers for Massive Internet of Things".

[4] 3GPP TR 22.862: "Feasibility Study on New Services and Markets Technology Enablers - Critical Communications".

[5] 3GPP TR 33.849: "Study on subscriber privacy impact in 3GPP".

[6] 3GPP TR 22.864: "Feasibility Study on New Services and Markets Technology Enablers - Network Operation".

[7] 3GPP TR 22.891: "Study on New Services and Markets Technology Enablers".

[8] 3GPP TS 22.185: "Service requirements for V2X services".

[9] NGMN Alliance [Internet]. [cited 13 April 2016]. Available from: https://www.ngmn.org

[10] NGMN 5G White Paper V1.0 [Internet]. [cited 13 April 2016]. Available from: https://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2015/NGMN_5G_White_Paper_V1_0.pdf

[11] 5G Ensure Project [Internet]. [cited 30 March 2016]. Available from: http://www.5gensure.eu/

[12] 5G Ensure Deliverable D3.1 - 5G-PPP security enablers technical roadmap (early vision) [Internet]. [cited 30 March 2016]. Available from: http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D3.1-5G-PPPSecurityEnablersTechnicalRoadmap_early_vision.pdf

[13] 3GPP TR 22.863: "Feasibility Study on New Services and Markets Technology Enablers - Enhanced Mobile Broadband".

[14] "4G Americas' Recommendations on 5G Requirements and Solutions" [Internet]. [cited 26 July 2016]. Available from: http://www.4gamericas.org/files/2714/1471/2645/4G_Americas_Recommendations_on_5G_Requirements_and_Solutions_10_14_2014-FINALx.pdf

[15] "5G Forum Korea's White Paper on 5G Vision Requirements and Enabling Technologies" [Internet]. [cited 26 July 2016]. Available from: http://kani.or.kr/5g/whitepaper/5G%20Vision,%20Requirements,%20and%20Enabling%20Technologies.pdf

[16] "Chinese IMT-2020 (5G) Promotion Group 5G White Paper on Network Technology Architecture" [Internet]. [cited 26 July 2016]. Available from:http://www.imt-2020.cn/en/documents/download/3

[17] "FCC requirements on 5G" [Internet]. [cited 26 July 2016]. Available from: http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0714/FCC-16-89A1.pdf

[18] 3GPP TS 33.246: "Security of Multimedia Broadcast/Multicast Service (MBMS)".

[19] FIDO UAF Complete Specifications, version 1.0, December 2014, http://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208.zip

[20] Mobile Connect, https://developer.mobileconnect.io/about

[21] RFC 3748: "Extensible Authentication Protocol (EAP)".

[22] 3GPP TR 33.402: "Security aspects of non-3GPP accesses".

[23] IETF RFC 5216:"The EAP-TLS Authentication Protocol".

[24] 3GPP TR 33.821: "Rationale and track of security decisions in Long Term Evolved (LTE) RAN / 3GPP System Architecture Evolution (SAE)".

[25] IETF RFC 6696: "EAP Extensions for the EAP Re-authentication Protocol (ERP)".

[26] 3GPP TR 33.868: "Study on security aspects of Machine-Type Communications (MTC) and other mobile data applications communications enhancements".

[27] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[28] Tobias Engel. (December 2014). "SS7: Locate. Track. Manipulate", http://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf

[29] Sergey Puzankov and Dmitry Kurbatov, "How to Intercept a Conversation Held on the Other Side of the Planet".Positive Technologies, (May 2014), http://www.slideshare.net/phdays/phd4-pres-callinterception119

[30] Karsten Nohl (December 2014) "Mobile Self-Defense", https://events.ccc.de/congress/2014/Fahrplan/system/attachments/2493/original/Mobile_Self_Defense-Karsten_Nohl-31C3-v1.pdf

[31] 3GPP TS 33.401: "Security architecture".

[32] FIPS Publication 186-4 "Digital Signature Standard (DSS)", http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

[33] RFC 6507: "Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)".

[34] 3GPP TS 33.401: "System Architecture Evolution (SAE); Security architecture"

[35] 3GPP TS 33.402: "System Architecture Evolution (SAE); Security aspects of non-3GPP accesses"

[36] 3GPP TS 33.117: "Catalogue of General Security Assurance Requirements"

[37] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)"

[38] ETSI GS NFV-SEC 001: "NFV Security; Problem Statement"

[39] ETSI GS NFV-SEC 002: "NFV Security; Cataloguing security features in management software"

[40] ETSI GS NFV-SEC 003: "NFV Security; Security and Trust Guidance"

[41] NIST SP 800-125 A: "Security Recommendations for Hypervisor Deployment"

[42] Cloud Security Alliance (CSA): https://cloudsecurityalliance.org/

[43] 3GPP TS 33.210: "3G Security, Network Domain Security (NDS), IP Network Layer Security"

[44] GSMA RIFS: "Diameter Roaming Security - Proposed Permanent Reference Document" (editor Silke Holtmanns)

[45] Tobias Engel. (December 2008). "Locating Mobile Phones using Signaling System 7", http://berlin.ccc.de/~tobias/25c3-locating-mobile-phones.pdf.

[46] Siddharth Rao, Silke Holtmanns, Ian Oliver, Tuomas Aura (June 2015) "Unblocking Stolen Mobile Devices Usign SS7 – MAP Vulnerabilities", http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7345408

[47] RFC 6733: "Diameter Base Protocol",

[48] "AVP Level Security for Non-neighboring Diameter Nodes: Scenarios and Requirements": https://tools.ietf.org/html/draft-ietf-dime-e2e-sec-req-05

[49] GSMA RSP Technical Specification SGP.02, v3.1

[50] 3GPP TS 33.310: "Technical Specification Group Services and System Aspects; Network Domain Security (NDS); Authentication Framework (AF)".

[51] 3GPP TS 33.401: "Technical Specification Group Services and System Aspects; 3GPP System Architeture Evolution (SAE); Security architecture".

[52] SOG-IS: "Agreed cryptographic mechanims"

[53] NIST SP 800-131A R1: "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths"

[54] ETSI White Paper "Quantum Safe Cryptography and Security"; June 2015

[55] NISTIR SP 8105 (draft): "Report on Post-Quantum Cryptography"; February 2016

[56] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)"

[57] IETF Internet Draft, "The Transport Layer Security (TLS) Protocol Version 1.3", 2016, https://tools.ietf.org/html/draft-ietf-tls-tls13

[58] IETF RFC 5281:"Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)".

[59] IETF Internet Draft, "EAP Tunneled TLS Authentication Protocol Version 1 (EAP-TTLSv1)", 2016, https://tools.ietf.org/html/draft-funk-eap-ttls-v1-01

[60] IETF Internet Draft, "TLS Inner Application Extension (TLS/IA)", 2016, https://tools.ietf.org/html/draft-funk-tls-inner-application-extension-03.txt

[61] RFC 5448: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

[62] 3GPP TR 38.804: "Study on New Radio Access Technology; Radio Interface Protocol Aspects"

[63] M. Groves, "Sakai-Kasahara Key Encryption (SAKKE) ", RFC 6508, February 2012.

[64] Shaik A, Borgaonkar R, Asokan N, Niemi V, Seifert JP. Practical attacks against privacy and availability in 4G/LTE mobile communication systems. arXiv preprint arXiv:1510.07563. 2015 Oct 26. Available from: https://arxiv.org/pdf/1510.07563v2.pdf

[65] 3GPP TS 23.003: "Numbering, addressing and identification".

[66] Report on Pairing-based Cryptography in Volume 120 (2015) of Journal of Research of the National Institute of Standards and Technology "http://nvlpubs.nist.gov/nistpubs/jres/120/jres.120.002.pdf"

[67] V. Gayoso Martinez, L. Hernandez Encinas, and C. Sanchez Avila, "A survey of the elliptic curve integrated encryption scheme," Journal of Computer Science and Engineering, vol. 2, no. 2, 2010. Available at http://digital.csic.es/bitstream/10261/32671/1/V2-I2-P7-13.pdf

[68] Ecrypt II. ECRYPT II yearly report on algorithms and keysizes (2011-2012). Available at http://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf

[69] NIST Special Publication 800-38G, Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption (March 2016). Available at http://dx.doi.org/10.6028/NIST.SP.800-38G

[70] Standards for Efficient Cryptography Group (SECG), Elliptic Curve Cryptography, SEC 1, version 2, 2009. Available at http://www.secg.org/sec1-v2.pdf

[71] A.W. Dent. Proofs of security for ECIES. Chapter III of Advances in Elliptic Curve Cryptography, pp 41–46, Cambridge University Press, 2005.

[72] 3GPP TR 38.801: "Study on New Radio Access Technology; Radio Access Architecture and Interfaces ".

[73] 3GPP TS 33.102: "3G Security; Security architecture".

[74] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[75] ETSI TS 102 225: Smart Cards; Secured packet structure for UICC based applications (Release 12)

[76] ETSI TS 102 226: Smart Cards; Remote APDU structure for UICC based applications (Release 13)

[77] 3GPP TS 31.102: Technical Specification Group Core Network and Terminals; Characteristics of the USIM application (Release 14)

[78] ETSI TS 102 221: Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 13)

[79] ETSI TS 102 484: Smart Cards; Secure channel between a UICC and an end-point terminal (Release 11)

[80] 3GPP TS 22.261: "Service requirements for next generation new services and markets".

[81] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[82] RFC 4764: "The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method".

[83] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[84] Jover, R. P. (AT&T), Security Attacks Against the Availability of LTE Mobility Networks: Overview and Research Directions. 16th International Symposium on Wireless Personal Multimedia Communications (WPMC). 2013.

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

Example: text used to clarify abstract rules by applying them literally.

3GPP service layer user identifier: uniquely identifies a user within the 3GPP service layer. IMS is an example of a 3GPP defined service layer. Within the IMS, various identifiers are defined: IP Multimedia Public Identity (IMPU) identifies a user; IP Multimedia Private Identity (IMPI) uniquely identifies a subscription in the IMS and so on.

3GPP subscription credential: a subscription credential that has a 3GPP subscription identifier, and a key (i.e. an existing 3GPP key or alternative key).

3GPP subscription identifier: a subscription identifier that is routable to the home 3GPP network if the UE is roaming; an example of such an identifier is the IMSI.

NextGen USIM: The evolution of the current USIM for NextGen use.

Alternative 3GPP subscription credential: a 3GPP subscription credential that has a 3GPP subscription identifier and alternative key.

Alternative subscription credential: a subscription credential that has non-3GPP subscription identifier and an alternative key.

Anonymity: The condition when personally identifiable information (PII) is irreversibly altered in such a way that personal information can no longer be identified directly or indirectly.

Application service identifier: uniquely identifies an application service (operator or 3rd party owned) that is using 3GPP service layer (e.g. IMS) and transport layer (access layer) to deliver IP based services to the user. The application service identifier may be used by the operator and/or application service provider to control which applications are allowed to use service provider's network.

Application service user identifier: identifies a user within an application service(s) that's being delivered to the human user over the service provider's network. An IMPU is associated with this identifier to enable routing within the IMS. IMPU may be used as the Application service user identifier, for example, in scenarios where the application service is provided by the service provider.

Confidentiality: The property that data is not disclosed to system entities unless they have been authorized to know the data.

Equipment Identifier: The identifier that uniquely characterises an equipment (consisting of at least hardware and, possibly, associated software) used to access the 3GPP system (e.g. IMEI and MAC address).

Existing 3GPP subscription credential: a 3GPP subscription credential that has 3GPP subscription identifier and an existing 3GPP key.

Human user identifier: identifies a human user who is associated with one or more 3GPP subscriptions in a 3GPP network, and is using services offered by the service provider over a 3GPP network.

Identifier (ID): The data object that definitively represents a specific identity of an entity, distinguishing that identity from all others.

Identity: The collective aspect of a set of attribute values (i.e., a set of characteristics) by which a user is recognizable or known.

Inside attack: The attack that is initiated by an authorized or legitimate user of the system, e.g. an employee or third-party personnel.

Non-3GPP subscription credential: a subscription credential that has a non-3GPP subscription identifier and a key (i.e. alternative key).

Non-3GPP subscription identifier: a subscription identifier that is not routable to the home 3GPP network, and cannot be used for roaming; example of such identifier could be e.g. "sensor12345@factory.example.com"

Editor's note: Word "non-3GPP" should be replaced by another word because the "non-3GPP" credentials and "non-3GPP" identifiers are being described in 3GPP specifications.

Outside attack: The attack that is initiated by an unauthorized or illegitimate user of the system.

Personally identifiable information (PII): Any information that (a) can be used to identify a subscription to whom such information relates, or (b) is or might be directly or indirectly linked to a subscription.

Privacy: The right to the protection to any information that (a) can be used to identify a subscription to whom such information relates, or (b) is or might be directly or indirectly linked to a subscription.

Privacy impact assessment: Overall process of privacy risk identification, risk analysis and risk evaluation with regard to the processing of personally identifiable information (PII).

Privacy principles: Set of shared values governing the privacy protection of personally identifiable information (PII) when processed in information and communication technology systems.

Privacy requirements: set of requirements to take into account when a 3GPP node is processing personally identifiable information (PII).

Processing of personally identifiable information (PII): Any operation or set of operations performed upon personally identifiable information (PII), including but not limited to: collection, transmission, storage, modification, anonymization, disclosure, erasure.

Pseudonymity: The condition when the processing of personally identifiable information (PII) is such the data can no longer be attributed to a specific subscription without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable subscription.

Revocation Server Fuction (RSF): RSF stores the revocated certificates or Identity-based Identifiers and Public Verfication Tokens (PVT). RSF receives request from other function entities for checking whether a given certificate or Identity-based Identifiers and PVT are in the revocation list and replies a validation results.

Security anchor: It is a signalling entity that resides in a physically protected location. Its functions at least include: authentication function, deriving AN- and CN-specific keys by using a key that is never forwarded to exposed locations, and secure storage of security context.

Editor's note: Authentication function and derivation of keys may reside in different functional entities.

Subscriber: A Subscriber is an entity (associated with one or more users) that is engaged in a Subscription with a service provider, cf. 3GPP TR 21.905 [1].

Subscription: A Subscription describes the commercial relationship between the subscriber and the service provider, cf. 3GPP TR 21.905 [1].

Subscription credential: a pair of values consisting of a key and an identifier that serves to identify a subscription and that is to be used as a basis for authentication and key agreement.

Subscription Identifier: The identifier that uniquely identifies a subscription in the 3GPP system. The identifier is used to access networks based on 3GPP specifications.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply.
An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

AES Advanced Encryption Standard
AKA Authentication and Key Agreement
AMF Access and Mobility Management Function
AMF Authentication Management Field;
(NOTE: The AMF acronym is used in two meanings in this document; which of those is intended in a specific place should be clear from the context.)AN Access Network
AUTN Authentication token
CK Cipher Key
CP Control Plane
CriC Critical Communications
C-RNTI Cell RNTI as used in TS 36.331
DoS Denial of Service
EAP Extensible Authentication Protocol
eKSI Key Set Identifier in E-UTRAN
ERP EAP Re-authentication Protocol
EPS Evolved Packet System
FQDN Fully Qualified Domain Name
IK Integrity Key
IMEI International Mobile Station Equipment Identity
IMSI International Mobile Subscriber Identity
KDF Key Derivation Function
KSI Key Set Identifier
LSB Least Significant Bit
ME Mobile Equipment
MSC Mobile Switching Center
MSIN Mobile Station Identification Number
MTC Machine Type Communication
NAS Non Access Stratum
NCC Next hop Chaining Counter
NEF Network Exposure Function
NF Network Function
NG NextGen
NG UE NextGen User Equipment
NGC NextGen Core
NRF Network Repository Function
NSI Network Slice Instance
NST Network Slice Template
OCSP Online Certificate Status Protocol
OTA Over-The-Air (update of UICCs)
PCC Policy and Charging Control
PCF Policy Control Function

PCRF	Policy and Charging Rules Function
PDCP	Packet Data Convergence Protocol
PGW	Packet Gateway
PLMN	Public Land Mobile Network
PRNG	Pseudo Random Number Generator
PSK	Pre-shared Key
QoE	Quality of Experience
RRC	Radio Resource Control
SCG	Secondary Cell Group
SeNB	Secondary eNB
SGW	Serving Gateway
SIM	Subscriber Identity Module
SMF	Session Management Function
SN	Serving Network
SQN	Sequence Number
SRB	Source Route Bridge
SRVCC	Single Radio Voice Call Continuity
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
UP	User Plane
UPF	User Plane Function
USIM	Universal Subscriber Identity Module
XRES	Expected Response

4 Security areas and high level security requirements

4.1 Security areas

This document includes the following security areas:

1) Security architecture deals with architectural aspects of the security for NextGen system.

2) Authentication deals with authentication framework, identifiers, and credentials, authentication methods.

3) Security context and key management deals with security aspects related to management of security context and security keys.

4) RAN security deals with the security for Next Generation radio interface and radio access network.

5) Security within NG-UE deals with the security of sensitive data handled within the NG-UE.

6) Authorization deals with both, authorization of the UE to access the network and authorization of the network to serve the UE.

7) Subscription privacy deals with various aspects related to the protection of subscribers' personal information, e.g. identifiers, location, data, etc.

8) Network slicing security covers security aspects related to the network slicing concept such as service access, network function sharing and isolation.

9) Relay security deals with security of the NextGen connectivity over relays.

10) Network domain security deals with security of the signalling protocols in the network domain such as authentication, integrity, and availability.

11) Security visibility and configurability deals with presentation of security information to a user of a UE, and management of security configuration by a user or a UE.

12) Credential provisioning deals with security aspects of provisioning 3GPP credential(s) on equipment that will access the NextGen system.

13) Interworking and migration deals with security aspects related to the interworking and migration scenarios between radio technologies and possible core network concepts.

14) Small data deals with massive number of IoT UEs that usually send small amounts of data sporadically and also moves around.

15) Broadcast/Multicast security deals with security for broadcast services that will be used in verticals, for example MCPTT, Critical Communication, V2X, and massive MTC.

16) Management Security deals with security related to management plane and deployment scenarios.

17) Cryptographic algorithms deal with cryptographic algorithms to be used for security mechanisms and protocols within Next Generation System.

4.2 High level security requirements

3GPP specifications shall provide mechanisms to verify the integrity of 3GPP radio messages to a common point in the visited network. These mechanisms shall allow the detection of unauthorised radio messages, detection of "false base stations" and verification of an authorised network. The mechanisms shall be extensible so that suitable security can be maintained of the life of the NextGen implementations. The mechanisms defined should cater for the high speed communications envisioning in NextGen and for battery efficient low volume data.

The security mechanisms defined in NextGen shall be able to be configured to comply with local lawful interception laws and regulations.

The security mechanisms defined in NextGen shall be able to be configured to confidentially protect voice, data and signalling.

The security mechanisms defined in NextGen shall be able to be configured to protect subscriber's privacy.

The security mechanisms defined in NextGen shall be able to be configured to provide authorisation services for users, devices and networks both at a bearer level and at a services level.

The security mechanisms defined in NextGen shall be able to be configured to provide authorisation, integrity protection and confidentiality between network elements and between networks.

The security mechanisms defined in NextGen shall be able to be configured to provide authorisation, integrity protection and confidentiality for new NextGen services.

As NextGen networks may be active upto and beyond 2030 and as the ability to attack security mechanisms increases over time, the security mechanisms specified for NextGen shall be extensible to new algorithms and procedures that will be defined during the lifetime of the specifications, where appropriate.

The control plane shall be protected against denial of service attacks from UEs. Mechanisms should be specified which limit the effect which signaling attacks may cause to the network. Signaling caused by UEs should not be able to degrade the network performance for other end users and the network itself, this is especially the case for NextGen where the amount of signaling may increase.

UEs shall be protected against denial of service attacks from network. Mechanisms should be specified which limit the effect which signaling attacks may cause to UEs. Signaling caused by the network should not be able to degrade the network performance for end users, this is especially the case for NextGen where the amount of signaling may increase.

UEs and NextGen network should be protected against denial of service attack from external networks, e.g. the internet, and from other UEs. Impact to network and end user signalling or data processing due to external attacks should be minimized. Signaling and data processing caused by external network traffic should not degrade the network performance for end users and the network itself, as well as the UE performance, e.g. the power consumption.

Editor's note: Clarification is needed for the terms used in this clause: service, network service, NextGen services and UE.

5 Key issues and solutions

5.1 Security area #1: Architectural aspects of Next Generation security

5.1.1 Introduction

This security area covers architectural aspects of the security for NextGen systems. It also covers the security features to be provided on the protected reference points identified in the security area #1 on architectural aspects of the security for NextGen systems. For each feature, it is stated for both security endpoints whether it is optional or mandatory to support or use. In all cases, it is assumed that a feature, if optional to use, is applied in the same way in uplink and downlink. If a feature is optional to use then its use is determined during the security negotation procedure.

The present security area is structured such that there is one key issue for each reference point.

NOTE: This security area also covers the security features to be provided on the backhaul link and core network interfaces, as opposed to clause 5 of TS 33.401.

Editor's Note: The referenece architecture for authentication framework in solution #12.1 of TR 23.799 is taken as a starting point for the reference points here.

Editor's Note: The security procedures realizing the security features described here are addressed in separate security areas.

5.1.2 Security assumptions

tba

5.1.3 Key issues

5.1.3.1 Key issue #1.1: Overview of NextGen security architecture

Editor’s note: This key issue can be added as a separate clause of the TR.

5.1.3.1.1 Key issue details

The present key issue covers

- a figure describing the NextGen security architecture, abstracted so as to contain only the elements that are deemed relevant for security. It is expected that this abstracted architecture may be refined as the work progresses.
- a list of entities performing security functions
- a list of reference points that need to be protected

Editor's Note: Figure and lists tba

5.1.3.1.2 Security threats

tba

5.1.3.1.3 Potential security requirements

tba

5.1.3.2 Key issue #1.2: Need for security anchor in NextGen network

5.1.3.2.1 Key issue details

Summary:

Is a security anchor in the Core Network beneficial for Next Generation? If so, can it be realized in an access-agnostic way?

Details:

A major advantage of the EPS security architecture over that of UMTS and GSM CS is that the MME provides a security anchor in the Core Network (CN). KASME is an intermediate key stored in the MME that is never transferred to the Access Network (AN). All AN-related keys are derived (directly or indirectly) from KASME without the need for re-authentication.

This key issue deals with the question whether it is necessary or advantageous to have a security functional entity in Next Generation that exhibits properties similar to that of the MME, i.e. it is a signalling entity that resides in a physically protected location and maintains a key that is never forwarded to exposed locations and is used to derive AN-specific keys. We call this entity "security anchor".

In the current evolved packet core (EPC) system, the mobility management entity (MME) is an entity that is responsible for mobility management (MM) and session management (SM) for Ues. In addition, the MME is performs authentication and key agreement (AKA) with a UE based on an authentication vector(s) provided by the UE's home network (i.e., HSS). In other words, the MME is the security anchor in the serving network.

The security anchor functionality of the MME assumes that the MME is deployed in a physically secure location, thereby being sufficiently isolated and protected from external entities. However, locating the AKA functionality in the MME may prohibit flexible deployment of network functions in the NextGen networks. For example, MM and SM functionalities may need to be moved towards the network edge (i.e., closer to RAN or collocated with RAN) to reduce signalling latency or to reduce management overhead at a single MME (i.e., for scalability). As another example, MM functionality and SM functionality may be located in different network entities.

To support various deployment models/scenarios of network functions, it is desired to decouple AKA functionality from other functionalities and maintain the authentication function in the security anchor deep inside the network independently of deployment scenarios. This enables flexible MM and SM function placement without impacting security. Furthermore, introduction of a seperate security anchor helps reduce security configuration complexity between network entities/functions.

It should be clear from the functional specification and not depend on particular deployments whether the security anchor resides in a physically protected location or not.

NOTE: For EPS, the assumption was made that CN nodes always reside in physically protected locations while AN nodes may reside in exposed locations. The term "physically protected" is not meant to imply tamper-resistance or similar concepts.

In case the need for a security anchor is agreed then it needs to be decided further whether the security anchor can be realized efficiently in a (completely) access-agnostic way or needs to be access-dependent (at least to some degree).

Editor's Note: The current text in TR 23.799: "Supporting a security context hierarchy to introduce flexibility in deriving the required security context, while maintaining access-dependent aspects in the access networks" could be misunderstood as not allowing a security anchor performing access-specific functions in the core network. However, this should be open for further study.

The following provides more background information:

Potential security benefits of the security anchor (motivated by observations from EPS) include:

- Forward security (In EPS, a fresh key is sent from MME to target eNB in handovers, meant to provide increased security in case of chained handovers)
- Provisioning of fresh key after idle-active transition without the need for re-authentication (as opposed to UMTS); there is no need to keep keys in exposed node during idle mode. (But will there still be an idle mode in Next Generation?)
- Termination of security for UE-CN signalling in security anchor can thwart some persistent DoS attacks (e.g. paging attack, 2013). (But will there still be NAS signalling in Next Generation?)
- A connectionless mode is under discussion in SA2 where user plane security terminates in the CN. Such a mode could possibly benefit from a security anchor in the CN.

It is ffs whether these security benefits are also desired in Next Generation, and, if so, how they can be realized.

The following questions should be studied for this key issue, motivated by observations from EPS:

- Is the provisioning of new AN keys by the security anchor tied to AN mobility events?
  - In EPS, initial NAS messages or Path Switch messages are triggers for key generation in the MME.
  - Efficiency is achieved in EPS through piggy-backing keys on mobility messages
- How is fresh input to key derivation synchronized between UE and security anchor?
  - Examples of fresh inputs from EPS include: NAS uplink COUNT, previous NH key
  - Synchronization is efficiently provided in EPS as part of mobility signalling (e.g. inclusion of 3-bit NCC in HO Command)
- How is a replay of keys prevented?
  - In EPS, the UE and the MME are in control of the fresh input
- How is inter-RAT mobility (NextGen-LTE, NextGen-other) supported? Which NextGen entity would interface with LTE CN or WLAN network for handover or idle mode mobility (providing key derivation and key transfer)?
  - In EPS, the MME provides mapped keys
- How is multiple-RAT connection (NextGen-LTE, NextGen-other) supported (for single UE)? Which NextGen entity would interface with LTE CN or WLAN network for security context setup (providing key derivation and key transfer)?
  - In EPS, the MME (or AAA in case of non-3GPP access) are in the control of security setup

5.1.3.2.2 Security threats

In Next Generation, mobility and session management functions may be located closer to the network edge, where those function are more exposed to attacks. In such deploymenet scenario, if an authentication and key management function is managed by an MME, compromising a single MME can break the security of a whole system if the MME is the security anchor in the serving network. Put another way, when the MME is the security anchor in a serving network, a compromise of an MME means that the compromise can affect other MmEs (a UEs data is still decryptable by an attacker even after the UE has moved to a different MME).

5.1.3.2.3 Potential security requirements

- The authentication functionality should be kept in a physically secure location in the network even if the MM and SM functionalities are located closer to the RAN or collocated with the RAN.

5.1.3.3 Key Issue #1.3: User plane integrity between UE and network

5.1.3.3.1 Key issue details

Legacy GSM/GPRS security provides no explicit integrity protection of either user plane data or control plane data. User plane data is (in most countries) encrypted, but this still provides very limited protection against a Man-In-The-Middle attacker changing that data en route, because encryption is linear (a stream cipher) and any checksums are also linear. UMTS and LTE include cryptographic integrity protection of most of the signalling messages, but not for user plane data. For the IoT-tailored GPRS ('Enhanced-Coverage GSM', 3GPP Release-13), however, user plane integrity protection was added, partly due to different security threats for user plane data for IoT compared for the human usage for which GSM-LTE were mainly tailored.

If data integrity is needed, it may be enforced at the transport or application layer (typically also with additional encryption). In this case the security endpoints will align with the service endpoints – typically either a server on the internet or (for phone calls, messages etc) another device. Adding another layer of integrity on the radio interface serves little purpose as far as protecting the traffic is concerned (although it may serve a purpose for overall system security assurance).

However, there may be cases in which transport or application security conflict with performance constraints (latency, battery life), and bearer level integrity provides a useful compromise (as considered in 3GPP TR 33.863 [13], for instance).

There is also a risk of a session as a whole being hijacked, and used to insert quantities of rogue data into a mobile connection (either to increase subscriber bills, or to waste resources carrying the data to the service end-point, where it will be rejected anyway).

The use of Message Authentication Codes is only appropriate for packets that should be received 100% correctly (after any error correction). Bit errors are common in cellular transmissions. Some user plane traffic is still valuable when received with a few bit errors, and should not be rejected just because one or two bits are wrong; voice and video codecs tend to be error tolerant, for instance, or else there may be error correction at a higher layer.

Descriptions on the security termination point, granularity and security policy could be referred to the Key issue #1.3: User plane confidentiality part.

5.1.3.3.2 Security threats

User plane security could be compromised if an attacker can influence the selection of the security termination point.

Next generation network will include middle nodes in open environments e.g. heterogeneous access, NFV, thus the termination point of the current UP-traffic protection is less secure.

In cases where end to end (transport or application layer) security protocols are ruled out by performance constraints, user plane traffic could be forged or modified by an attacker.

An attacker could inject rogue data into an established traffic channel, raising the subscriber's bill (or simply wasting network or device resources).

5.1.3.3.3 Potential security requirements

- Integrity protection is optional to support for UE and mandatory to support for network endpoint; even when both UE and network support it, it is still optional to use. At least two alternative and substantially different algorithms should be supported.
- The selection of the feature and the algorithms, according to the capabilities supported by the UE, shall be under network control.
- A mechanism should be available to detect (substantial) unauthorised insertion of rogue data onto an established traffic channel.
- The selection of the different security termination points shall be under network control.

5.1.3.4 Key Issue #1.4: User plane confidentiality between UE and network

5.1.3.4.1 Key issue details

As for user plane integrity, where confidentiality of user traffic is needed, it will usually be applied at the transport or application layer anyway. Just encrypting over the radio interface is not enough, because most services terminate either at an internet server (so need to be protected over the internet leg too) or at another device (often transiting the internet in between). Moreover, most of the same services may alternatively run over WiFi, which may be poorly protected, so again transport or application layer security will be applied to services that need it.

However, the overhead of radio interface encryption is low. It does not extend packets (unlike integrity protection), if stream ciphers are used; and, again if stream ciphers are used, it does not lead to bit error propagation. And there is some residual value in radio interface encryption, since it provides an additional layer of protection over what is one of the more exposed legs of its journey.

5.1.3.4.2 Security threats

User traffic that is not encrypted or encrypted with weak algorithm at the transport or application layer would be somewhat more exposed to interception if it is not encrypted over the radio interface.

5.1.3.4.3 Potential security requirements

- Confidentiality protection is mandatory to support for both UE and network endpoint and optional to use. At least two alternative and substantially different algorithms should be supported in both devices and networks.
- The selection of the feature and the algorithms, according to the capabilities supported by the UE, shall be under network control.
- The 5G system shall support that the UE can signal that the UE does not require UP confidentiality protection.

NOTE: Confidentiality protection is recommended to be used.

- The selection of the different security termination points shall be under network control.

NOTE: In all of the above, regulatory requirements need to be taken into account.

5.1.3.5 Key Issue #1.5 Integrity protection for the control plane between UE and network

5.1.3.5.1 Key issue details

The present key issue covers integrity protection for signalling between the UE and appropriate endpoints in the network.

In LTE, signalling is integrated protected between UE and AN, and between UE and the CN. This is the basic principle to follow in the NextGen network.

NOTE: In EPS, the only form of user plane traffic protected between UE and core network is the Rel-13 feature "data via MME", which, however, could also be seen as part of the UE-CN control plane.

Futhermore, some NAS signalling messages have to be exchanged between the UE and the MME before NAS security activation. For example, the very first attach request is sent before NAS security activation. Some downlink reject NAS messages have also be sent before NAS security activation because e.g., MME cannot get AVs from the HSS and consequently cannot activate NAS security.

For uplink NAS signalling messages sent before security activation (e.g., attach request), attackers can modify the capability information carried in these messages, which may prohibit use of some functions. This is a "bidding-down" attack or "DoS" attack to the UE.

For downlink NAS signalling messages before security activation (e.g., attach reject or TAU reject), attackers can forge reject NAS signalling messages with special error code which can lead UE into a "no-service" state. This is a DoS attack to the UE.

Countermeasures in LTE for above threats can be found in TS 24.301 [56] and TS 33.401 [31].

It is desirable that above attacks can be countered in next generation system. Current countermeasures in LTE need to be reviewed to see if they address all of the threats identified in the current clause of the current document. And new countermeasures may need to be introduced in next generation system.

5.1.3.5.2 Security threats

Without integrity protection, the signallings between UE and network can be modified, injected and replayed by the attacker, which can lead to some severe attacks such as UE impersonation, false network.

An attacker sends a paging message to get the UE to transition to active unnecessarily.

NAS signallings exchanged before security activation can cause e.g., DoS attacks to the UE.

5.1.3.5.3 Potential security requirements

- Integrity protection is mandatory to support and mandatory to use for both UE and CN endpoint, except for emergency calls.
- Integrity protection is mandatory to support and mandatory to use for both UE and AN endpoint, except for emergency calls.
- The Next Generation System shall support mechanisms to mitigate the risk caused by NAS signalling messages exchanged before NAS security activation.

Editor's note: Protection against spoofed paging message need to be considered. The balance between protecting paging messages and the risk of making the UE unreachable need to be taken into account.

5.1.3.6 Key Issue #1.6 Confidentiality for the control plane between UE and network

5.1.3.6.1 Key issue details

The present key issue covers confidentiality for signalling between the UE and appropriate endpoints in the network.

In LTE, signalling is confidentiality protected between UE and AN, and between UE and the CN for security. This is the basic principle to follow in the NextGen network.

NOTE: In EPS, the only form of user plane traffic protected between UE and core network is the Rel-13 feature "data via MME", which, however, could also be seen as part of the UE-CN control plane.

5.1.3.6.2 Security threats

Without confidentiality protection, the signallings between UE and network can be eavesdropped by the attacker, which can lead to some severe attacks such as tracing UE.

5.1.3.6.3 Potential security requirements

- Confidentiality protection is mandatory to support for both UE and CN endpoint and is recommended to be used.
- Confidentiality protection is mandatory to support for both UE and AN endpoint and is recommended to be used.

NOTE: Confidentiality protection is subject to local regulations

Editor's note: Protection from eavesdropping the content of messages that may be sent before security has been fully established needs to be considered.

5.1.3.7 Key issue #1.7: Key hierarchy

5.1.3.7.1 Key issue details

Key hierarchy is required to provision confidentiality and integrity requirements presented in other key issues.

5.1.3.7.2 Security threats

Using a flat key hierarchy, there is a greater attack surface for attackers due to multiple key agreements and the timing of these agreements. Additionally, there are opportunities to attack the keys when re-synchronization is required. Furthermore, using a hierarchy with common keys among network slices could cause other security problems, e.g., leakage of the information on the keys on one slice could affect other network slices.

5.1.3.7.3 Potential security requirements

- Keys for confidentiality and integrity of control plane shall be provided
- Keys for confidentiality and integrity of user plane shall be provided
- Keys to support network slicing shall be provided
- Keys to support new radio (NR) shall be provided
- Keys to support non-3GPP RAT (Radio Access Technology) access shall be provided, such as the keys for ePDG in LTE.
- Keys to support backward compatibility with SAE/LTE shall be provided

Security for different communications mentioned above shall be isolated.

5.1.3.8 Key Issue #1.8: UEs with Asymmetric Keys

5.2.3.8.1 Key issue details

Requirements across several key issues suggest that NextGen UEs will require asymmetric keys, or at least would strongly benefit from having such keys. In particular:

- Equipment identifier authentication (Key Issue #2.4), would be difficult to do with symmetric keys. A symmetric key solution would require either binding a given equipment to a specific operator (so that only said operator can then authenticate it), or else would require that a non-operator party (most likely the equipment manufacturer) has to keep a copy of the equipment symmetric key and run the equivalent of an AuC.
- User authentication requirements are stated in 3GPP TR 22.861: "Enhanced authentication mechanism shall enable an operator to provide efficient means to authenticate a user and a device (e.g., using biometric information)." Instead of operators storing large quantities of biometric data, it would be more secure for the user to authenticate locally to the device (using a fingerprint etc.) and then for the device to report this fact securely to the operator. However trusting such a report in part requires the device to be suitably trusted.
- Non-AKA-based authentication (Key Issue #2.5) suggests that UEs will authenticate to non-3GPP access networks, or perhaps to NextGen factory networks, using public key methods like EAP-TLS.
- Remote credential provisioning for IoT devices (Key Issue #12.2), includes the requirement from TR 22.861 that "The 3GPP system shall support a secure mechanism to remotely provision a device that has not been pre-provisioned, with its 3GPP subscription credentials." This may include i) Allowing limited temporary access to a mobile network for a device which does not yet have a 3GPP subscription. But doing that suggests that some form of secure device authentication is needed for subscription-less

devices, or otherwise spoof devices may attempt to repeatedly join the network to request subscriptions and waste resources. ii) Ensuring that the destination point for the provisioning of subscription credentials is trustworthy enough to receive these credentials. This calls for authentication of the device or of a secure component embedded within the device (e.g. the existing GSMA eUICC solution relies on an elliptic curve keypair to authenticate the eUICC to multiple operators).

Further key issues suggest that NextGen UEs will need to verify asymmetric keys used by network components:

- AS security during RRC idle mode" (Key Issue #4.1) includes the following potential security requirement: Next generation system should provide a means to ensure a UE in idle state is able to determine the authenticity of a cell. The main goal is to prevent denial of service attacks from false networks. It is very difficult to imagine that a UE without a security context yet established could do this by symmetric key means. But if the UE could recognize the public key signatures from genuine networks, this requirement could be met.

- Key issue #7.1 "Subscription identifier privacy" discusses the leakage of permanent subscription identifiers, such as IMSI, on the radio interface. The ideal would, of course, be to ensure that permanent identifiers are never sent in clear over the radio interface, but are instead encrypted to legitimate network nodes. Again, it is very difficult to imagine doing this by symmetric key means before establishing a security context. But if the UE could recognize the encryption public keys of genuine networks, this requirement could be met.

If there are several areas where public key authentication is needed, then the architectural implications should be considered early on, rather than being introduced on a piecemeal basis. For example:

1. It will be very messy and complex if UEs have to get multiple key pairs/and or certificates from different sources, by different mechanisms, using different crypto-technologies, and perhaps stored in different parts of the equipment, in order to support each use case separately.

2. Some of the use cases could be architected using an operator-run database of public keys; but others appear to call for a public key certificate. This then raises the question of whether the device manufacturer has to arrange for a certificate in all cases (quite an overhead, especially for ultra-low-cost IoT devices), or whether it is better for an operator to generate one as and where it is needed, or whether a third party PKI becomes needed.

3. The operational consequences of using asymmetric keys vs symmetric needs to be taken into account when evaluating proposed solutions.

5.2.3.8.2 Security threats

A UE with multiple asymmetric key pairs (or multiple components hosting keypairs) may present a larger attack surface than one containing a unified keypair (or a unified component for such keypairs). Security of the device may be reduced to that of the weakest key, weakest key-provisioning method or weakest component.

If a UE has multiple different keys, an attacker may try to force the wrong key to be used (e.g. a signing key may be used for decryption, or may be used to sign a spoof protocol handshake). Or on the verification side, an attacker may try to force the wrong public key to be used, to verify a spoofed signature or certificate.

The cost of provisioning multiple key-pairs and/or certificates may force security compromises which would not be needed under a more unified solution (such as generating a single master equipment key within a single secure component).

Public key technology may force operators to rely on so-called trusted third parties without having any real control over the security offered by such parties.

Over-use of a single UE key-pair may harm user privacy (allowing a user's actions to be linked and tracked across multiple domains and services).

Public key cryptography may be vulnerable to advances in quantum computing over the lifetime of the NG system.

5.2.3.8.3 Potential security requirements

Where asymmetric keys are identified as being required as part of a solution:

- The UE shall support a component for generating, storing and using asymmetric keys which meets the security needs of all use cases calling for such keys.
- It shall be possible for operators to use UE keypairs for various means without necessarily trusting third parties. It shall be possible for operators to deploy keypairs for network components (to be verified by UEs) without necessarily using trusted third parties.
- UEs and network components shall be able to support at least one form of quantum-safe public key cryptography. This might be done by upgrading/patching over the lifetime of the UE / NG network.

5.1.3.9 Key issue #1.9: Security features for AN-CN Control Plane

5.1.3.9.1 Key issue details

The present key issue covers authentication, confidentiality and integrity for control plane traffic between appropriate entities in the access network and core network, respectively.

In LTE, interfaces betweenAN and CN are protected for signalling transfering. This is the basic principle to follow in the NextGen network.

NOTE: This corresponds to backhaul link control plane security in EPS, cf. TS 33.401, clause 11.

5.1.3.9.2 Security threats

The attacker can obtain lots of information during intial attach procedure by eavesdropping when there is no confidentiality protection between these nodes.

If Integrity is not used, the attacker can modify the signalling, especially during initial attach procedure. If the attacker modifies the XRES in user authentication response, a DoS attack to the user is successful.

If no authentication has been performed before signalling exchange between AN NEs and CN NEs, these nodes will potentially suffer spoofing attack from both sides and Man-in-the-Middle attack, especially in the environment of virtualization/NFV.

5.1.3.9.3 Potential security requirements

The Control Plane between AN-CN shall support mutual authentication.

The Control Plane between AN-CN shall be confidentiality protected.

The Control Plane between AN-CN shall be integrity protected.

NOTE: Confidentiality protection is subject to national regulations

5.1.3.10 Key issue #1.10: Security features for AN-CN User Plane

5.1.3.10.1 Key issue details

The present key issue covers authentication, confidentiality and integrity for user plane traffic between appropriate entities in the access network and core network, respectively.

In LTE, the interfaces betweenAN and CN are protected for the security of user messages. This is the basic principle to be used in the NextGen network.

NOTE: This corresponds to backhaul link control plane security in EPS, cf. TS 33.401, clause 12.

5.1.3.10.2 Security threats

If there is no confidentiality in AN-CN, an attacker can easily obtain the user's privacy information.

The NextGen Core network will not mandate to use user plane integrity protection between UE and CN. This leave holes for an attacker impersonating an entity to send information to the UE or to the CN which cannot verify where the message from.

If no authentication has been performed before data transfer between AN NEs and CN NEs, these nodes will potentially suffer spoofing attack from both sides and Man-in-the-Middle attack, especially in the environment of virtualization/NFV.

5.1.3.10.3 Potential security requirements

The User Plane interface between AN-CN shall support mutual authentication.

The User Plane between AN-CN shall be confidentiality protected.

The User Plane between AN-CN shall be integrity protected.

NOTE: Confidentiality protection is subject to national regulations

5.1.3.11 Key issue #1.11: Security features for CN-CN Control Plane

5.1.3.11.1 Key issue details

The present key issue covers authentication, confidentiality and integrity for control plane traffic between appropriate Network Functions in the core network.

Service based architecture is introduced in Next Generation. Security for service based architecture need to be considered. Current NDS/IP mechanisms needs to be reviewed and possibly enhanced for service based architecture.

NOTE1: This corresponds to network domain security in EPS, cf. TS 33.210 and TS 33.310.

NOTE2: This key issue is included in the security area "Architecture" so as to obtain a complete overview of the interfaces that need to be protected in this security area. Further details and solutions can be found in security area 10 "Network Domain Security".

5.1.3.11.2 Security threats

The security context may be transferred from one CN node to another CN node in point to point architecture or service based architecture. The attacker can easily obtain it when there is no confidentiality protection between these CN nodes. Without integrity protection, the security context can be modified to make the UE and the CN use different keys.

If no authentication has been performed before signalling exchange between CN NEs in point to point architecture or service based architecture, these nodes will potentially suffer spoofing attack from both sides and Man-in-the-Middle attack, especially in the virtualization/NFV environment and the scenario when the NEs are deployed at the edge of network.

If no authorization has been performed in service based architecture, a requester NF can potentially obtain information and request NF service which are not allowed for it, e.g. the AMF may obtain SMF related subscriber data from UDM or SMF directly, or SMF NF requests "Update UE Location" service from UDM to update UE location.

5.1.3.11.3 Potential security requirements

CN-CN control plane shall support mutual authentication.

CN-CN control plane traffic shall be confidentiality protected.

CN-CN control plane traffic shall be integrity protected.

NF service access shall be authorized in service based architecture.

NOTE: Confidentiality protection is subject to national regulations

5.1.3.12 Key issue #1.12: Security features for CN-CN User Plane

5.1.3.12.1 Key issue details

The present key issue covers authentication, confidentiality and integrity for user plane traffic between appropriate entities in the core network.

Editor's Note: This key issue has been added for completeness so that an explicit decision can be made. There is no equivalent in EPS as network domain security in TS 33.210 is explicitly limited to control plane traffic. It is ffs whether 3GPP should specify the equivalent of network domain security for user plane traffic in 5G. If so then further details and solutions can be found in security area 10 "Network Domain Security".

5.1.3.12.2 Security threats

If no authentication has been performed before data transfer between CN NEs, these nodes will potentially suffer spoofing attack from both sides and Man-in-the-Middle attack, especially in the virtualization/NFV environment and the scenario when the NEs are deployed at the edge of network.

5.1.3.12.3 Potential security requirements

CN-CN user plane shall support mutual authentication.

5.1.3.13 Key Issue #1.13: Security Implications to Achieve Low Latency

5.1.3.13.1 Key issue details

The following requirements are stated in [4], among others related to latency of Next Gen communications:

- [PR 5.1.3-001] The 3GPP system shall support cycle times of [1 ms to 2 ms]. Within the cycle time, both uplink and downlink transactions must be executed. Additional margin is needed for the sensor/actuator to process the request.
- [PR 5.2.3-001] The 3GPP system shall support very low latency (~1 ms).
- [PR 5.2.3-010] The 3GPP system shall support low end-to-end latency ranging from 1 ms up to 10 ms even in the high mobility scenario.
- [PR 5.3.3-001] The 3GPP system shall support 1 ms one-way delay between mobile devices and devices in the nearby Internet.
- [PR 5.3.3-002] The 3GPP System shall support very low one-way latency on the radio layer [1 ms].
- [PR 5.3.3-005] The 3GPP System shall minimize the delay (e.g. that caused by signalling, incl. for security) that is required prior to user data transmission.

The natural reading of these requirements is that they apply to user plane traffic; however it is not immediately clear what the implications would be for control plane latency (e.g. signalling to transition from idle mode to active mode, to run AKA and establish a security context). Certainly it could be argued from [PR 5.3.3-005] that the intention is to achieve ultra-low control plane latency as well, although a precise target is not given.

However, both low user-plane and low control-plane latency requirements have serious security implications:

a) User Plane

In conventional cellular networks, billable traffic is routed into the core network (e.g. SGSN, PD-GW). During roaming, it is usually routed into the cores of both the visited and home network. This allows both networks to keep track of how much data is being consumed (and of what billable types etc.) and so helps prevent billing errors, or deliberate fraud.

By contrast, to achieve very low latencies, significant data will need to be routed directly between the UE and the network edge, without passing through the core network (and without touching the home network at all in a roaming scenario). In particular, the visited network must rely on edge components to tell it what charging

records to send to the home network, and the home network must also rely entirely on these components, despite having almost no control over how they are set up/secured. Since the edges of networks are more vulnerable to attack than the cores, this creates a significant risk both of billing errors (and disputed bills with the subscriber), and of deliberate billing fraud.

A further concern is that operators are required to provide LEA Support including Lawful interception (LI) and Retained Data (RD) capabilities for traffic carried on their networks; typically this functionality is supported at nodes within the core network. However, traffic carried from the UE to an application at the network edge is currently designed to avoid the core, and hence would avoid the usual intercept points.

Moreover, in the context of mobile edge computing, placing multiple additional LI points around the network edge raises security risks:

- there will be many more LI points than in traditional deployments
- and also edge nodes are likely to be more exposed to attack than core nodes.

Finally, even basic crypto-operations become a challenge with <1 ms round trip time. If say 10% of that latency is consumed by the crypto, this requires at most 25 micro-seconds for each send and receive operation, or at most 12.5 micro-seconds for each crypto operation;

b) Control Plane

Overly aggressive latency targets for the control plane (e.g. <10ms or <1ms latency) may compromise system security, or else entail a completely new security architecture, without actually being justified by the envisaged use cases.

3GPP security mechanisms include authentication and key agreement, with periodic re-authentication (which requires round trips to the home network), signalling to the core network to manage security associations and session key updates, secure handovers between cells, and basic cryptographic operations of encryption and decryption, creation and verification of MACs etc.

Authentication to the home network becomes extremely difficult within a round trip of <10 ms (for speed of light reasons, the home network can be at most 1500 km away), and core network signalling is very challenging within a round trip of <1 ms (core network nodes can be at most 150 km away). It is important to note that currently we don't have any business use case or service requirement for such low latency needs regarding the authentication or control plane between the UE and the core network

There is not always a clear motivation for the ultra-low latency targets which would give rise to these security issues. Latencies of 50ms seem to be acceptable for use cases with human interaction (nerve signals cannot transmit faster than this through the human body, so human reaction times are always measured in 10s of ms). Or for cases like automated driving, 10ms of latency corresponds to less than 25 cm of motion at typical speeds. Air bags deploy in 15 to 30 msec.

5.1.3.13.2 Security threats

Fraudulent users and/or applications may disrupt accurate billing or create false billing records. Under-billing is an obvious risk (where the end user or edge application tries to use more data, or more valuable classes of data, than they will be billed for), but so is over-billing (if a hosted edge application has a revenue-share model, or pay-per-click model, it may try to inflate the amount of data billed for). Inter-operator roaming fraud may also be an issue.

LI capabilities which are distributed to a large number of edge components may be hijacked and abused to spy on user traffic. LI targets may evade interception (by disrupting the LI function) or learn that they are being targeted (by observing a change in behaviour/performance).

Traffic which cannot be fully encrypted (because the latency target does not permit this) may be read by an attacker from the radio interface, or elsewhere, leading to loss of user confidentiality. Traffic which cannot be integrity protected (because the latency target does not permit this) may be altered by an attacker.

A subscription which cannot be authenticated at the home network may incur billable events that are never paid for or inject malicious traffic into a visited network without accountability/traceability. Replication of home network functionality (e.g. HSS) closer to the UE risks exposure of long-term secret keys.

5.1.3.13.3 Potential security requirements

It shall be possible for visited networks and home networks to verify billing records supplied by potentially vulnerable components. when a lower level of security is used.

Editor's Note: Further research is needed to address LI issues. Liaisons have been already exchanged between ETSI MEC and ETSI TC LI.

For some services, it shall be possible to encrypt the user-plane with a very fast stream cipher. If, based on the operator's decision, security of user plane data is dropped entirely for some ultra-low latency services, the operator shall still be able to achieve some assurances on types and quantity of data carried via control plane signalling.

It shall be possible to adequately authenticate subscriptions even if there is very low control-plane latency, without exposing sensitive assets (such as a long term authentication secret key) at the network edge.

To support some critical services, such as remote surgery and industrial control, it shall be possible to provide integrity protection and replay protection for user plane even if very low latency is requested.

To support the services which require the transport of high volume user data with confidentiality and very low latency simultaneously, e.g., tactile internet, and considering network elements been deployed in virtualized environment, the cipher algorithms introduced into next generation system should support high computation efficiency.

5.1.3.14 Key issue #1.14: Security for serving functions in a less secure location

5.1.3.14.1 Key issue details

In a NextGen system, the serving functions in the core network may be virtualized. Some serving functions, such as SM, even MM, may be deployed close to AN, which may not be as secure as the core network location.

The following two deployment modes are identified:

- Mode A: all serving functions are deployed in a secure location.

  In this mode, a serving function (e.g. vSF-x in figure 5.1.3.14.1-1) can be deployed to handle UE-CN secure signalling (e.g. NAS in LTE), while the signalling latency between the NG UE and other vSFs needs to be considered as all UE-CN signalling shall pass through the vSF.

- Mode B: some serving functions are deployed in a less secure location.

  In this mode the serving fuctions are located typically close to the AN and as there are many AN locations this is typically less secure. If UE-CN secure signalling can only be terminated at one vSF (e.g. vSF-y in figure 5.1.3.14.1-2), then the signalling and data need to be verifiable and protected for privacy between the NG UE and the vSF as well as between the vSF and the rest of the core network. This will make the signalling security inefficient. As the secure tunnel between vSFs that across unsecured domain may be hacked, and the vSF itself may also be hacked, so there is a risk that subscription sensitive information (e.g. IMSI) may be eavesdropped even if it is sent in the secure tunnel. Hence, no subscription sensitive information should be send to a vSF that is in a less secure location.

NOTE1: There may be a vSF in the middle of UE-CN security signalling path, e.g. serving function for slice selection.

It is recommended that mode A is the only case used for Next Generation, however, it is FFS whether both deployment modes need to be considered. If mode B needs to be considered, then security requirements need to be specified for mode B.

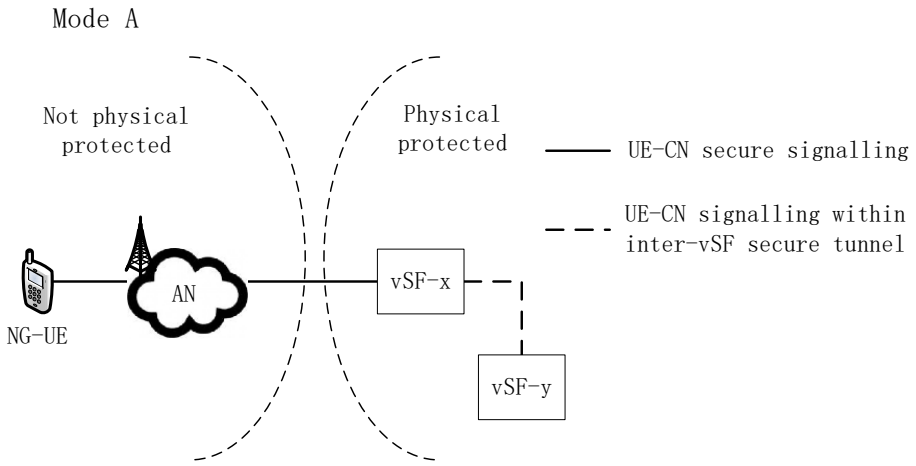


Figure 5.1.3.14.1-1 Mode A

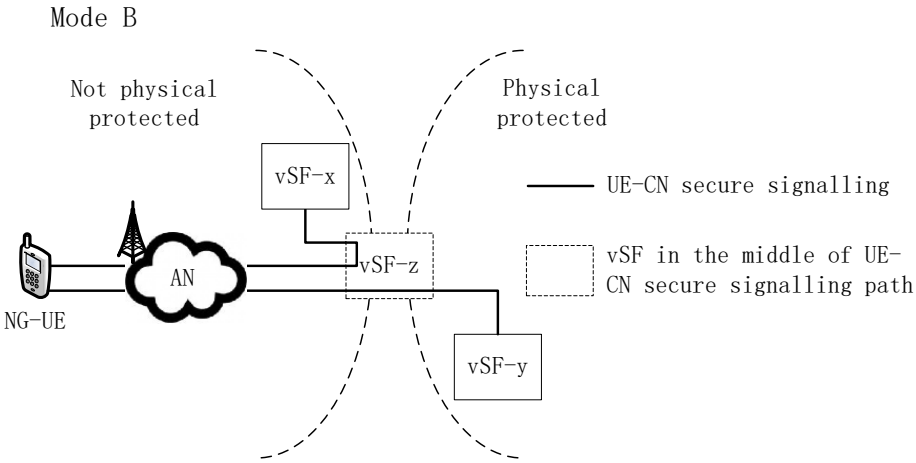


Figure 5.1.3.14.1-2 Mode B

NOTE2: An AN can be in secure location as well as in less secure location, depends on deployment.

Editor's note: Terminology of vSF need to be defined. For model B, new requirement maybe needed to let the vSFs to report its location status, so the network can use policy to control the security mechanism for the vSFs.

5.1.3.14.2 Security threats

There's no special security threat can be identified for mode A.

For mode B, if subscription sensitive information (e.g. IMSI) is delivered to the vSF that is in a less secure location, then exposure of the subscription sensitive information to hacker may occur. As the vSF may be accessed, storage of the vSF maybe hacked, so, UE related information is not secure, if the information can be tracked, e.g. by temporary ID, then user related information may be retrieved. If the vSF is able to handle UE-CN security signalling, and the keys for handling UE-CN secure signalling in the vSF can deduce keys for handling UE-CN secure signalling in the other vSF, then the attacker can also eavesdrop information that is transferred between the NG UE and the other vSF.

5.1.3.14.3 Potential security requirements

If the vSF is in a less secure location:

- Subscription sensitive information should not be delivered to the vSF.

- Any UE related information should be assigned to pseudonymity in the vSF, and any temporary ID related to the UE shoud be changed frequently.

If the vSF handles UE-CN signalling then:

- It should be possible that the vSF can handle UE-CN secure signalling (i.e. perform integrity and confidentiality process per UE) if needed.

- The keys for handling UE-CN secure signalling in the vSF should not be able to deduce keys in any other vSF, which handles UE-CN secure signalling too.

5.1.3.15 Key issue #1.15: Termination point of UP security

5.1.3.15.1 Key issue details

In Next Generation network different termination points for User Plane traffic should be supported, (i.e. the gateway where the User Plane is terminated may be located, for example, in the CN rather than in the AN, depending on the scenario). Therefore, it also needs to be studied whether the user plane integrity protection and confidentiality protection mechanism may be located in different places in order to provide appropriate security for all scenarios.

From security point of view, it is better if the user plane protection terminates deeper in the network rather than closer to the edge of the network. This was the reason why termination point was moved from the base station to the radio network controller when GSM was replaced by 3G. For LTE the termination point was moved back to the base station but this was done because of other reasons than security. In addition, this is an advantage that does not require the NG-UE to continuously negotiates new UP security protection keys whenever moving from one gNB to another.

From TR 23.799, it appears that there will be multiple UP gateways located in different places depending on the service scenarios and requirements. Therefore, UP user plane security protection architecture could be implemented by locating the user plane security termination point in these different locations.

Two concerns on user plane protection from heterogeneous access and IT-Driven network architecture are listed as following:

- Heterogeneous access. The heterogeneous access networks in NextGen may include 3GPP and non-3GPP accesses, and the number of the access points (e.g. base stations, APs etc) could be quite large. Furthermore, there could be many independent parties that control parts of the heterogeneous access network. All this increases the risk of having a vulnerable and/or compromised node in the network. As a mitigation for this increased risk, user plane protection between UE and User Plane Gateway could reduce the security complexity caused by multiple access technologies and massive number of potentially vulnerable access nodes.

NOTE: According to TR23.799, the IPsec tunnel for untrusted non-3GPP access terminates at N3WIF.

- IT-Driven Network Architecture. The next generation system is expected to support deployments in virtualized environments. So the network nodes would be virtualized, and that could lead to re-evaluation of security attacks based on the NFV (Network Function Virtualization). Therefore, UP protection between UE and User Plane Gateway for the user plane would imply minimizing the security impact from the network virtualization to UP data security. If we assume that the UP protection is terminated somewhere in the network then at least one node in the network would be a terminating point. (Possibly there are several termination points if hop-by-hop protection is applied.) It is possible that all nodes in the network are virtualized, including the UP Gateway itself. Then the UP protection termination point is affected by the virtualization but still number of virtualized nodes that have an impact on the UP protection is limited to its minimal value, i.e. to a single node.

Editor's Note: The LI of UP security termination point in home network is ffs.

5.1.3.15.2 Security threats

5.1.3.15.3 Potential security requirements

- Flexible UP-traffic protection shall be capable to support the flexible UP-traffic termination for different services with different security termination points.

Editor's Note: The following requirement needs more explanation, e.g. it is not clear if there will be a UP gateway in RAN and what is its relation to gNB.

- UP-traffic protection termination point should be the same point where the UP-traffic itself is terminated. Typically, this point would be the UP gateway, which can be located in CN or AN.
- Flexible UP-traffic protection shall support the scenario where different network slices can use different UP-traffic protection mechanisms.
- Flexible UP-traffic protection shall support the scenario where heterogeneous access technologies can use different UP-traffic protection mechanisms.
- LTE RAN nodes deployments can be exposed to attacks which compromise the confidentiality, authenticity and the integrity of the UP.
- Even if IPSec is implemented in the backhaul, access security is hop-by-hop. Depending on scenarios, security becomes dependent on also strong hardening of gNB.
- It cannot be assumed that a customer uses an over-the-top security solution to guarantee the confidentiality, authenticity and integrity of UP.
- The solution to be designed should allow the MNO to flexibly terminate the UP security in a physically secure location (defined by the MNO, based on deployment scenario) ;

5.1.3.16 Key issue #1.16: User plane protection granularity

5.1.3.16.1 Key issue details

This key issue is investigating the aspects of User plane protection granularity. The following analysis is given to compare different security protection granularities for UP security protection.

The definition of slice and session and the concept of flow are referred to SA2 TR23.799.

Table 5.1.3.16.1-1

Granularity	Pros.	Cons.
Per-Slice	- Simple and slice specific, guarantee the slice isolation from the security point of view	- Can't distinguish UEs, it's almost impossible that all the UEs use the same security policy referring the same key and algorithms. - Protections for all eMBB services of UE are the same. - Packet routing schema should be re-designed. Protection has to be made on the whole packet. - User plane integrity is good for some services (added security) but bad for others (too many rejected packets)
Per-Session	- One IP or non-IP traffic connectivity for one UE, having the explicit end users, UP security protection could be applied reasonable efficiently - Distinguish UEs, and distinguish different session of one UE - For one UE may have only a few sessions, the security cost could be suitable - Routing is fine. Protection can be made on the payload	- If there are multiple services simultaneously in same session, then user plane integrity may be good for some and bad for others. - If Anti Replay protection of IPsec and QoS are active at the same time, they may conflict. It's an implementation issue, and several solutions already exist
Per-Flow	- More specific security protection for different services - Routing is fine. Protection can be made on the payload.	- Relying on the session implement procedures - Difficult to implement for there would be numerous flows for one UE - High complexity on management - If Anti Replay protection of IPsec and QoS are active at the same time, they may conflict. It's an implementation issue, and several solutions already exist

In order to provide security protection selections, UP security protection should identify proper granularities (e.g. per-slice, per-session, per-flow).

5.1.3.16.2 Security threats

5.1.3.16.3 Potential security requirements

- UP-traffic protection granularity should support the per-session mechanism

Editor Note: The definition of session and flow in this context need to be clarified, e.g. how do they map to SA2 and RAN definitions.

5.1.3.17 Key issue #1.17: On-demand security policy

5.1.3.17.1 Key issue details

In UP security architecture, there would be a number of types of security requirements required by the service, UE, or network, which should be considered together for deciding on the security policy.

Considering the security policies are various for different service and end user, thus, it would be necessary to negotiate the security policies for the UP regarding each protection.

The following provides more potential security benefits of security policy negotiation:

- For eMBB scenario, traditionally, the network side takes the decision for both NAS and AS security mode procedures which cover the cryptographic algorithms will be used for the security context in EPS.

After the security mode procedure, all the service data of the UE will be protected by the same security policy in LTE. However, in future eMBB network, the situation would be a little complex for taking the service into account with specific service security requirements which are independent from MNO's security, to its own service, so a dedicate security requirement may be provided by the service server, and with the traditional UE's supported security capabilities and other security features from the network elements. Hence, the final security policy should be negotiated based on these provided security requirements from all the possible elements (but with the network having the final decision).

- To meet the stringent requirements of Critical communications, such as, higher reliability, higher availability, higher accuracy positioning, the specific security requirements should also be taken into account which could cover longer key and stronger security algorithm or shorter key update cycle. However, there would be a tradeoff between the network performance and the security cost.

- For IoT, excerpts from 6.1 TR 22.891: "[PR.6.1-001] The 3GPP system should support end-to-end integrity protection and confidentiality for data transmitted to/from a device, when the device is in indirect 3GPP connection mode." show that the UP security should be designed to meet the IoT service requirements. Some of the IoT devices are expected to be simple sensor kind of devices, in addition, the number would be large, thus, the security policy should be specific to support these devices' capabilities and limited communication requirements (e.g., smart meter), such as, shorter key length, fast authentication mechanism and so on.

5.1.3.17.2 Security threats

5.1.3.17.3 Potential security requirements

In order to support UP security protection mechanism between UE and UP Gateway for the user plane in the next generation system, UP-traffic protection mechanism should support the security policy negotiated from security requirements. Upon the security policy negotiation, the network (access network entity and core network entity) (i.e., SM, Policy Control) could have the final decision on which security policy including explicit security features and algorithms will be used. The network could negotiate the security policy through an independent procedure or pigged back in the other service procedures. It should be preferred that the next generation network can enable the network to have the flexibility to choose security mechanism according to different services requirements.

5.1.3.18 Key issue #1.18: Flexible security policies negotiation in control plane

5.1.3.18.1 Key issue details

It is difficult to update the algorithms, and the update method is practically to replace the network element, which can be cost-prohibitive in many cases. On the other hand, NextGen has a long expected lifetime, and new cryptography algorithm may be needed in the period of NextGen. So, in the NextGen network, the cryptographic algorithms in network element should not be unchangeable.Furthermore, as noted in key issue #1.17, the UP's security policies including cryptographic algorithms, key length, etc, are flexible according to the security requirements of UE and service. However, the key issue focuses on the security policy negotiation in CP, whichcaters for the evolution requirement of 3GPP. It is obvious that cryptographic algorithm is part of security policy negotiation in CP. Negotiation mechanism for cryptographic algorithms can facilitate the introduction of new algorithms in 5G lifetime.

NOTE: Updating crypto algorithms of UE is out of scope..

It is expected that algorithms used in NG include cipher algorithm, integrity algorithm and KDF. However, in LTE, cipher/integrity algorithm is negotiated in SMC procedure, and NG could apply the similar procedure. However, KDF is implemented stably, and there is no negotiation procedure for it. Furthermore, new KDF may also be needed during the lifetime of NextGen. Depending on use cases and services there may be more than one KDFs, so the use of KDF also requires a negotiation procedure.

As mentioned above, in the NextGen network, the security policies of control plane can be flexible in a negotiation method. For example, the participants of security process may negotiate security policies respectively before the process starts, or they could send their supported security policies to a controller, and the security policy will be negotiated under control of the controller.

5.11.3.18.2 Security threats

KDF used between UE and NEs may be attacked to lose key separation feature. Broken cryptographic algorithms may be difficult to update in the network element, and the only way to maintain security is to replace the network element with broken cryptographic algorithms, which may be cost-prohibitive in many cases.

5.1.3.18.3 Potential security requirements

The following provides design principals of security policy negotiation in control plane:

- The cryptographic algorithms implemented in network element should be extensible. The update of algorithm should be supported.
- The security policy such as cryptographic algorithm, key length, should be negotiated by participants of control plane.
- The selection of the security policy shall be under network control.

5.1.3.19 Key issue #1.19: Untrusted non-3GPP access

5.1.3.19.1 Key issue details

NG systems will support access via non-3GPP access technologies such as WiFi, fixed broadband, eHRPD, and others. Particular access networks may be considered trusted from the point of view of the core network, or untrusted. As a working hypothesis, the distinction between trusted and untrusted is assumed to be the same as for 4G, cf. TSs 23.402 and 33.402.

When an access network is considered untrusted then an additional layer of security on top of whatever security is provided in the access network is required. This additional layer needs to extend between the UE and an entity considered trusted by the core network. In 4G, this entity is the ePDG, and the additional layer of security is realized by IPsec.

Untrusted non-3GPP access needs considerations including aspects of architecture, authentication, and security context management. In particular, it needs to be explained how it fits in the unified authentication framework.

5.1.3.19.2 Security threats

When an access network is considered untrusted then there is no guarantee that the access network offers sufficient protection against eavesdropping on or unauthorized modification of messages, nor against theft of service or impersonation.

Editor's Note: rewording of threats section is required.

5.1.3.19.3 Potential security requirements

- When an access network is considered untrusted then an additional layer of security on top of whatever security is provided in the access network is required.
- The additional layer of security needs to extend between the UE and an entity considered trusted by the core network.

Editor's Note: it is ffs whether this entity needs to be trusted by the serving network or home network or both.

- The additional layer of security needs to provide protection against eavesdropping, unauthorized modification of messages, theft of service and impersonation.

5.1.3.20 Key issue #1.20: Trusted non-3GPP access

5.1.3.20.1 Key issue details

NG systems will support access via non-3GPP access technologies such as WiFi, fixed broadband, eHRPD, and others. Particular access networks may be considered trusted from the point of view of the core network, or untrusted. As a working hypothesis, the distinction between trusted and untrusted is assumed to be the same as for 4G, cf. TSs 23.402 and 33.402.

When an access network is considered trusted then the NG core deems the security mechanisms provided by the accesss network adequate, and no additional layer of security on top of access network security is required. However, UE authentication would still be the responsiblity of the NG core, and the NG core would also have to provide the related keys to the access network to enable access network security. This may include additional keys for protecting signalling protocols specific to trusted access, like e.g. the WLCP in 4G.

It is recognized that detailed specifications for trusted access networks in 4G are currently only available for Trusted WLAN (TWAN), cf. TS 23.402, clause 16, and TS 33.402, clause 7.2.3. The key issue should therefore explore the security aspects of the NG equivalent of TWAN as well as the need for similar specifications for other access network types.

Trusted non-3GPP access needs considerations including aspects of architecture, authentication, and security context management. In particular, it needs to be explained how it fits in the unified authentication framework.

5.1.3.20.2 Security threats

Even if the security mechanisms provided by the accesss network are deemed adequate, the access network cannot guarantee in itself protection against the following threats:

- UE impersonation
- Access network /serving network impersonation
- Eavesdropping on or modification of 3GPP-specific signalling

5.1.3.20.3 Potential security requirements

- Mutual authentication of access network /serving network.
- Protection against eavesdropping on and modification of 3GPP-specific signalling.

5.1.3.21 Key issue #1.21: Dealing with signalling attacks

5.1.3.21.1 Key issue details

A NextGen core network is likely to serve many different access networks, including a NextGen RAN, 5-n G (1<n<3) access networks, and perhaps even fixed access networks. A denial of service on the core network has therefore a larger impact than a denial of service on the access network and will impact a much larger geographical area than an attack on the Access Networks or earlier generation networks.

In [84], the attacks with highest impact are those that affect the core network and involve either bearer setup and release, attacking the S-GW in LTE or registration and deregistration, attacking the HSS or MME. These attacks correspond to the signalling attacks mentioned in the high level requirements 4.2.

The following key issues in this TR deal with some of these attacks, namely:

- KI #2.7: activation of many UEs at the same time for mIoT devices
- KI #8.1: slice isolation in order to prevent resource over consumption of one particular slice
- KI #8.3: UEs attaching to slices without authorization causing a denial of service.

All of these key issues deal with a specific type of signalling attack, rather than specifying the generic feature that a signalling attack should be detected and then dealt with. This key issue is to fill the gap that the others do

not fill by stating that the NextGen network should be able to detect a signalling attack, identify the offending UE and then provide measures to contain the attack or the UE.

5.1.3.21.2 Security threats

- Uncontrolled and uncontained signalling attacks can lead to a denial of service for many users;
- Existing congestion control mechanisms are undiscriminatory and will cause denial or degration of service for many users, even those not participating in a deliberate denial of service attack

5.1.3.21.3 Potential security requirements

- The NextGen network should be able to detect and identify UEs that cause a denial of service attack. Unauthenticated UEs may not be identified (in a reliable way);
- The NextGen system should be able to minimize the effects of a signalling attack by signalling the UEs participating in such an attack.

5.1.3.y Key issue #1.y: <key issue name>

5.1.3.y.1 Key issue details

5.1.3.y.2 Security threats

5.1.3.y.3 Potential security requirements

5.1.4 Solutions

5.1.4.1 Solution #1.1: Radio interface user plane integrity protection

5.1.4.1.1 Introduction

This solution addresses key issue #1.3.

5.1.4.1.2 Solution details

User plane integrity protection is mandatory to support in the network while optional in the UE, with at least two alternative and substantially different algorithms mandatory to support in network entities and UEs supporting user plane integrity protection. Both 128-bit and 256-bit integrity protection keys should be accommodated.

The NG-UE states, in signalling that is secure from bidding down attacks, which algorithms it supports and optionally, whether or not it desires user plane integrity / confidentiality protection. One way to achieve this is to include this information in the (unprotected) Attach Request message, and then repeating them later in an integrity protected message.

Algorithms allow either 32-bit or 64-bit MACs to be produced, and the device can optionally indicate which it prefers.

The serving network decides whether or not user plane integrity protection is possible (for example do both ends support it and have at least one algorithm in common); if it is possible, then the network decides whether or not it should be used, and with which algorithm and which MAC length. This also is indicated to the UE in an integrity protected signalling message.

A possible variation would be to have the decision made separately for uplink and downlink. If this variant is adopted, then the UE should be able to indicate separately for uplink and downlink whether it desires user plane integrity protection.

5.1.4.1.3 Evaluation

This solution allows user plane integrity to be used if and when it is believed to have value. The network can choose to switch on user plane integrity protection either because the device desires it or because the network itself values it (e.g. as a fraud protection measure).

The network can decide not to apply user plane integrity protection.

The solution addresses key issue #1.3. It allows strong user plane integrity protection to be applied where it makes sense to do so.

5.1.4.2 Solution #1.2: Periodic local authentication and packet count check

5.1.4.2.1 Introduction

This solution addresses some aspects of key issue #1.3, namely the threat of an attacker inserting significant quantities of rogue data into an established traffic channel.

5.1.4.2.2 Solution details

The solution is the same as the "Signalling procedure for periodic local authentication" (3GPP TS 33.102, clause 6.4.7, and 3GPP TS 33.401, clause 7.5), adapted as necessary to fit the Next Generation architecture.

Potential adaptations could be to help detect replacement of packets (not just addition or deletion of packets). For example: the signaling procedure could report on number of bits transmitted/received for various traffic types (not just a simple count of packets); or it could report a digest of all data transmitted/received within a window requested by the network; or it could report a digest of packets that were transmitted/received with robust error correction (this would prevent random bit errors causing a failed digest). A further set of adaptations could be to allow a similar report to run between the UE and the home network.

The appropriate polling/reporting frequency might vary; for instance, a UE sending occasional small readings might be polled (or report) less frequently than another UE that consumes data much faster.

Editor's note: The detailed solution to fit the Next Generation architecture is ffs.

5.1.4.2.3 Evaluation

This solution allows the network to detect if there is a significant difference between the number of packets that the UE has sent and received, and the number of packets that the network has received and sent respectively. In particular it allows the network to detect if more packets have been received than were genuinely sent – which is the most obvious indicator of abuse.

It thus addresses the threat of an attacker inserting quantities of rogue data on an established traffic channel. It does not, though, provide precise integrity protection of data, but some of the suggested adaptations could make it very difficult for an attacker to modify data transmitted/received while still avoiding detection.This solution can address part of Key Issue #1.13: Security Implications to Achieve Low Latency, in particular the risk of attacks on vulnerable network edges. The mechanism can be used to request a UE report on data transmitted/received, which can then be compared with the report from the network edge. Allowing the report to run between the UE and home network would provide assurance to the home network of billing integrity in vulnerable roaming scenarios.

Types of fraud which involve both a compromised network edge and a compromised UE could still evade detection, but such frauds may be difficult to execute.

Integrity protection of the user plane is another method to prevent these attacks.

Editor's Note: It is FFS how the HN could use the UE reports to the HN on number of packets sent, as comparing these reports with charging records sent by the VN, possibly some time later, may be complex.

5.1.4.3 Solution #1.3: Radio interface user plane encryption

5.1.4.3.1 Introduction

This solution addresses key issue #1.4.

5.1.4.3.2 Solution details

User encryption is mandatory to support in UE and network, with at least two alternative and substantially different algorithms mandatory to support. Both 128-bit and 256-bit encryption keys should be accommodated.

The NG-UE states in signalling that is secure from bidding down which algorithms it supports, and, optionally, whether or not it desires user plane integrity / confidentiality protection. One way to achieve this is to include this information in the (unprotected) Attach Request message, and then repeating them later in an integrity protected message.

The visited network decides whether or not to apply encryption, and which algorithm to use. This is indicated to the UE in an integrity protected signalling message.

The encryption should always be applied where regulations permit.

5.1.4.3.3 Evaluation

The solution straightforwardly addresses key issue #1.4.

5.1.4.4 Solution #1.4: Key hierarchy

5.1.4.4.1 Introduction

This solution addresses key issues of "#1 Architectural aspects of NextGen security" and "#8 Network slicing security".

5.1.4.4.2 Solution details

Figure 5.1.4.4.2-1 shows the proposed key hierarchy. We assume that (1) there is one common C-plane in the core network, (2) there is no slicing in radio access network thus the radio access technology keys as shown in the figure and (3) separate keys are required for each network slice.

In this key hierarchy, there is one long term "K" and the key is used only to derive "Kng" used as a master key to provide subsequent keys.

For security between a UE and core network, keys for C-plane "Kcp" and for U-plane in network slice A "Kns_a_up" are derived using the master key "Kng" and the identity information of the keys and the network slice. Other keys for integrity and confidentiality of C-plane (Kcp_i, Kcp_c) signalling and U-plane (Kns_a_up_i, Kns_a_up_c) messages are derived from Kcp and Kns_a_up, respectively. Although keys for C-plane are derived once and commonly used among multiple network slices, keys for U-plane are derived for each network slice. Security isolation between C-plane and U-plane is realized, because different keys are provided for C-plane and U-plane. Per slice based keys for C-plane can be derived. Per session based keys of U-Plane such as Kns_a_up_i_ses1 and Kn_a_up_c_ses1 can be derived subsequently from Kns_a_up, if security isolation per session is required.

For AS security, a key "Krat" used for the communication between a UE and RAT (Radio Access Technology) or between a UE and the gateway used for non-3GPP RAT accessing scenario is derived using the master key "Kng" and identity information on the RAT. Keys for C-plane "Krat_cp" and for U-plane "Krat _up" are derived using the master key "Kng" and the identity information of the keys. Other keys for integrity and confidentiality of C-plane (Krat_cp_i, Krat_cp_c) signalling and U-plane (Krat_up_i, Krat_up_c) messages are derived from Krat_cp and Krat_up, respectively. This key hierarchy also supports other RAT than 3GPP using "Krat_other" or "Knon-3GPP_other", and could derive legacy 3GPP-RAT keys such as E-UTRAN using "K3GPP_rat". Knon-3GPP_rat" is meant for existing non-3GPP radio networks. Legacy 3GPP-RAT keys, such as E-UTRAN, can be derived using "K3GPP_rat

Editor's Note : Definition of each key in detail including how it is derived and where it is stored, is FFS.

Editor's Note: It is FFS to consider how to realize security isolation among network slices for single C-plane in core network.

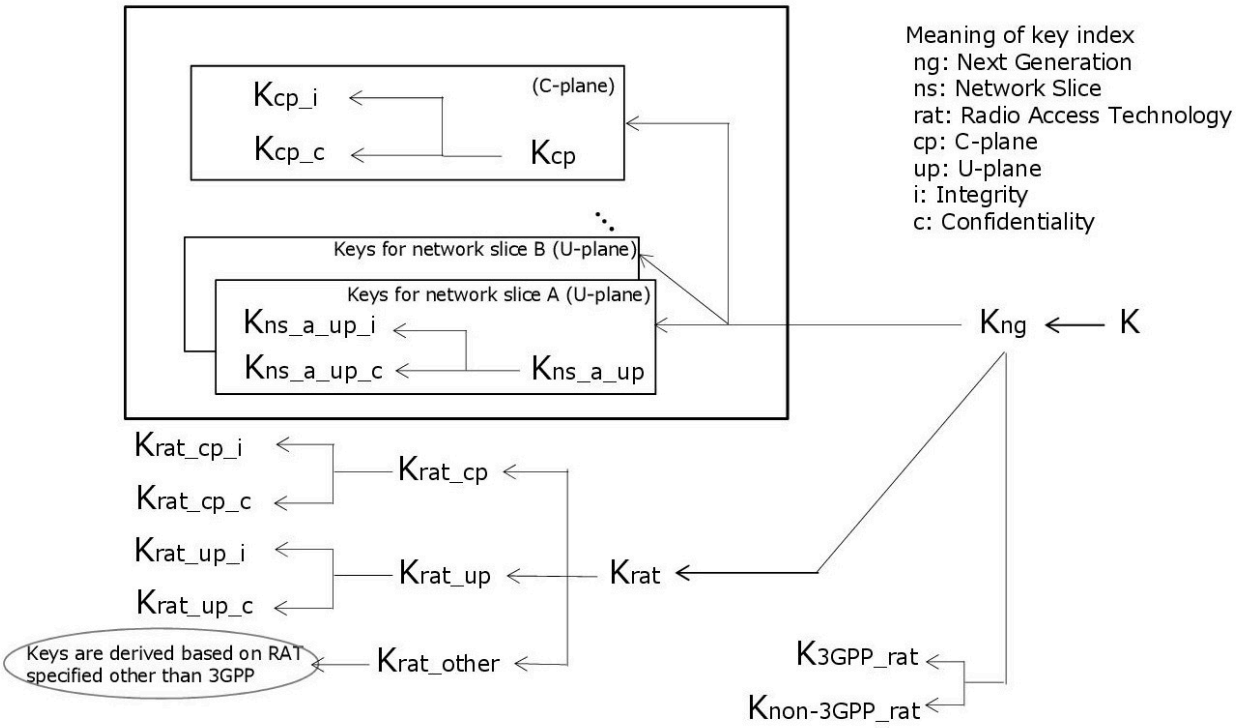


Figure.5.1.4.4.2-1: Key hierarchy

5.1.4.4.3 Evaluation

FFS

5.1.4.5 Solution #1.5: User plane security policy and key derivation

5.1.4.5.1 Introduction

This solution addresses Key Issue #1.3 and Key Issue#1.4. The terminologies are referred to TR23.799 solution #4.3 and solution #12.1.

5.1.4.5.2 Solution details

5.1.4.5.2.1 Introduction

In this document, it is assumed that security policy control function is mainly for executing the security policy determination and that Session Management Function is service specific, mainly for controlling the establishment of the UE's session, also, the UP-GW is user plane gateway serving the session. The definition of security policy control function (SPCF) is referred to clause 5.2.1.2.

UP-traffic protection granularity should support the per-session mechanism. The solution proposes to put the security termination point at User Plane Gateway. And the user plane is protected on per-session granularity with a security policy determined from security requirements. From the security point of view, there would be many types of security requirement required by the service, UE, or network, which should be considered together for the security policy. For example:

- Security Requirement A: UE's service requirement

- Security Requirement B: default security requirements pre-configured for the UE in HSS
- Security Requirement C: security capabilities from the gateway side
- Security Requirement D: security capabilities from Application Server
- Security Requirement E: security capabilities supported by the UE equipment

The UP security policies are determined from the above requirements, the security policy could apply for security protection for granularity of UP session. The security policy could include e.g.:

- Confidentiality protection algorithm, such as AES, Snow 3G, Zuc, Null.
- Integrity protection algorithm, such as AES, Snow 3G, Zuc, Null.
- Key length etc.

The security policy could be decided by the security policy control function or other elements. The security policy is applied to UP security protection, i.e. UP confidentiality protection and UP integrity protection between UE and UP GW.

The high level description is that: firstly, UE send the request to the network including the security requirement A. After retrieving the requirements, the security policy control determines the final security policy. Next, based on the security policy, the CN generates and distributes the protection key $K_{session1\text{-}enc}$, $K_{session1\text{-}int}$ for confidentiality protection and integrity protection of the session.

5.1.4.5.2.2 Procedure

The following figure gives one solution to about how to implement the UP security protection. In this solution, the security policy decision is completed based on the session setup procedure which could be either session established with attach procedure or a dedicate session setup procedure after UE already attached to the network. The security policy is determined from security requirement A and requirement C.

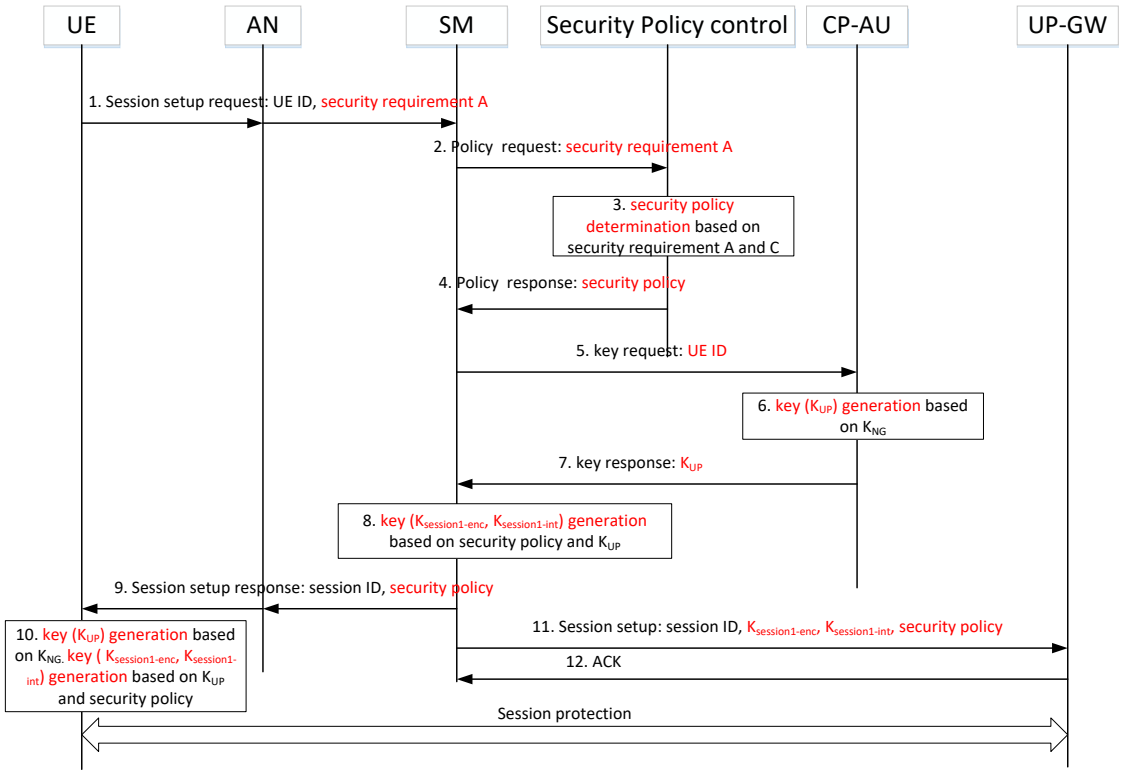


Figure 5.1.4.5.2.2-1: User Plane security policy and key derivation at per-session granularity

NOTE: Where is location of SM may have impact.

1. UE initiates a session setup request. UE provides security requirement A, which would be the service specific that UE wants to use. UE ID may also be included. This step may be combined with the attach procedure in case the session is established with the attach procedure (EPS-like session establishment). It is assumed that this message is carried via an access function. It is assumed that this message should be protected by control plane security.

2. Upon receiving UE ID and security requirement A, SM generates the session ID, and sends policy request to security policy control, including security requirement A.

3. Security policy control function determines the final security policy of the session based on the security requirement A and security requirement C, where the security requirement C could be the security capabilities of the UP-GW.

4. Security policy control function sends policy response back to SM with the security policy.

5. SM function sends the key request message to the CP-AU with the UE ID.

6. Firstly CP-AU retrieves the K_{NG} via UE ID, where K_{NG} is the shared key (similar as Kasme in LTE) derived after the mutual authentication between UE and core network. Then, CP-AU generates the UP protection key K_{UP} Using K_{NG}.

   Note that K_{UP} could also be generated after mutual authentication between UE and CP-AU. In this case, after receiving UE ID, CP-AU retrieves the K_{UP} with the UE ID.

7. CP-AU sends K_{UP} back to the SM.

8. After receiving the UP protection key K_{UP}, SM generates the session protection key (i.e. $K_{session1\text{-}enc}$, $K_{session1\text{-}int}$) using session ID and K_{UP}, according to the security policy. The security policy can be an explicit input to the Key Derivation Function.

   The key derivation function for $K_{session1\text{-}enc}$, $K_{session1\text{-}int}$ is as follows:

   $K_{session1\text{-}enc}$=KDF(K_{UP}, session ID, confidentiality protection algorithm identity),

   $K_{session1\text{-}int}$=KDF(K_{UP}, session ID, integrity protection algorithm identity).

   Confidentiality protection algorithm identity and integrity protection algorithm identity are included in the security policy.

   The key generation operation should follow the security policy requirements. For instance, if the security policy only requires the confidentiality protection, SM (UE) just generates the confidentiality protection key $K_{session1\text{-}enc}$ for this session protection.

9. Then, SM sends the session ID and security policy to UE. It is assumed that this message should be protected by control plane security.

10. After receiving the security policy, UE firstly generates the user plane protection K_{UP} with the same derivation function as CP-AU, then generates the session protection key (i.e. $K_{session1\text{-}enc}$, $K_{session1\text{-}int}$) using session ID and K_{UP}, according to the security policy, where K_{NG} is the shared key (similar as Kasme in LTE) derived after the mutual authentication between UE and core network. The security policy can be an explicit input to the Key Derivation Function.

    Note that K_{UP} could also be generated after mutual authentication between UE and CP-AU. In this case, UE retrieves the K_{UP} after receiving the session ID and security policy.

11. SM sends the session setup message to UP gateway (UP-GW) in order to setup the session, including session ID, $K_{session1\text{-}enc}$, $K_{session1\text{-}int}$ and the security policy.

12. UP-GW sends ACK back to SM.

Thus, UE and UP-GW share confidentiality protection key $K_{session1\text{-}enc}$, integrity protection key $K_{session1\text{-}int}$ and the security policy for them. Therefore, UP security protection would be deployed for the above session between UE and UP-GW.

5.1.4.5.2 Evaluation

Tba

5.1.4.6 Solution #1.6: Architecture for NextGen that include a security anchor

5.1.4.6.1 Introduction

This solution addresses Key Issue #1.2.

The solution addresses the issue of being able to separate the authentication functions in the CN from the Mobility Management (MM) and Session Management (SM) functions. It provides the ability to refresh the keys used to protect signalling and data between the NG-UE and the network without a fresh full authentication, e.g. keys are refreshed at MME-equivalent change which prevents any attacks leaking over from one MME-equivalent to another. This ensures that it is possible to store the keys resulting from an authentication in a very secure location even if MM and SM functions are placed nearer the edge of the network in not so secure a location. In particular, if fresh keys are used for each change of CN-MM, then this restricts security compromises to leak from one CN-MM to another.

The solution describes a key hierarchy and how that key hierarchy could be used in possible attach, idle mode mobility and handovers.

The solution makes no assumption on the actual authentication method used to authenticate the UE or on the storage of credentials in the UE as these are subject to their own key issues in different security areas.

5.1.4.6.2 Solution details

5.1.4.6.2.1 Architecture

5.1.4.6.2.1.1 General

This solution describes how a security anchor could fit into the NextGen architecture, which allows separation of authentication role of the CN from the MM and SM functionality. The description of the architecture assumes that MM and SM are deployed separately and co-locates the SM with the UP entities. This split follows on from the desire to provide keys separately for the MM and the protection of the UP that terminates above the RAN and also separate the network access authentication from any secondary authentication (see Key Issue #2.10) which relates to one user bearer. Another aim of the proposed architecture is for an authentication run to result in a key being left in the HPLMN. This key may be used for either fast re-authentications or providing a key that could be used for user plane security that terminates in the home network when the UE is roaming (which necessitates the use of H_{SEAF} while roaming).

The entities in the architecture are as follows:

ARPF

AUSF

SEAF

CN-MM: the core network node that terminate the NAS Mobility Management (MM) signalling

CN-SM/UP: the core network node(s) that terminate the SM and perform the signalling for UP and carrying the UP.

Service provider controls the credentials for the secondary authentication as described in Key Issue #2.10 and any keys resulting from this authentication are only used to protect the UP for the particular bearers.

Figure 5.1.4.6.2.1-1 shows the authentication architecture for non-roaming case, figure 5.1.4.6.2.1-2 shows the authentication for the roaming case figure 5.1.4.6.2.1-3 shows the authentication architecture for a non-roaming case where there a secondary authentication with a service provider to authenticate the use of a bearer.

NOTE 2: The provided figures are not intended to illustrate all uses cases. In the latter figure, the case of using keys from the secondary authentication to provide keys to protect the bearer from the UE to the core network is described. This is not preclude the use of keys from the secondary authentication to provide keys for UE to RAN protection. It is FSS if the secondary authentication could also use a SEAF.

The dashed connections show where it is expected that data will be protected between the UE and network, whereas the other connections show where the keys are carried. The following comment/observations apply:

Interfaces: The CN-MM to SEAF, CN-SM/UP to SEAF, SEAF and SEAF interfaces are very similar as they all are used to in effect request keys from the higher layer node and also carry various authentication related information elements (these IEs would depend on the chosen authentication method(s)).

Split between 'MM' and 'SM' keying: The architecture propose to derive the keys for the CN-SM/UP from the key at the SEAF rather than from the key at the CN-MM, as there are cases where the CN-SM/UP that requires a key is not in the same network as a the CN-MM serving the NG-UE.

Inclusion of an H-SEAF in roaming cases: As can be seen from the roaming use case, there is a possibility that a key will be need from the home network and having the H-SEAF avoids the need for an additional authentication run.

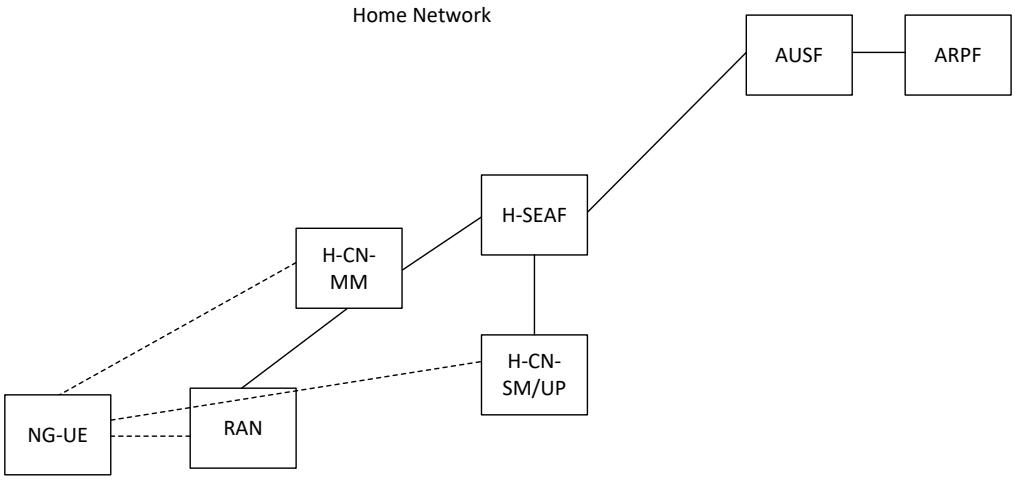


Figure 5.1.4.6.2.1-1: Architecture for authentication framework in non-roaming scenario

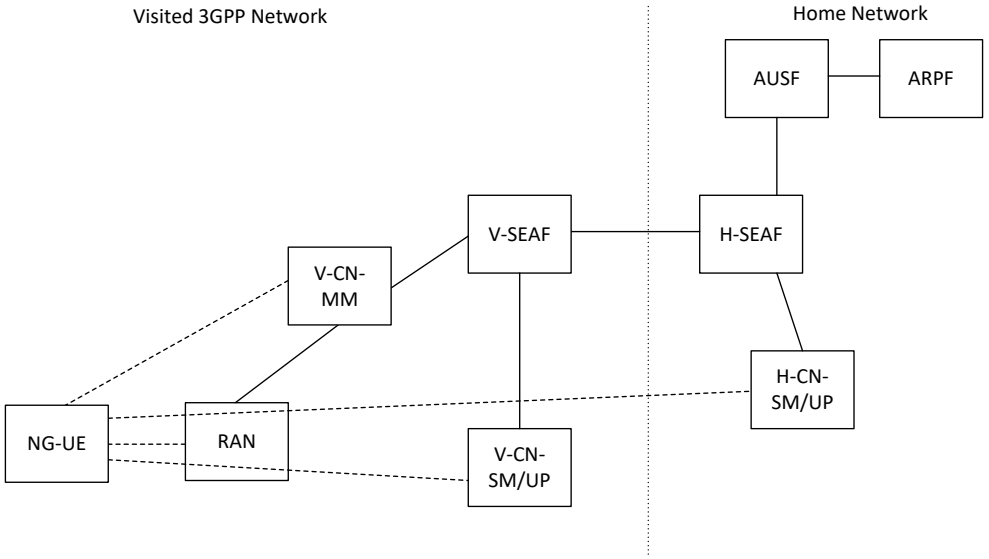


Figure 5.1.4.6.2.1-2: Architecture for authentication framework in roaming scenario

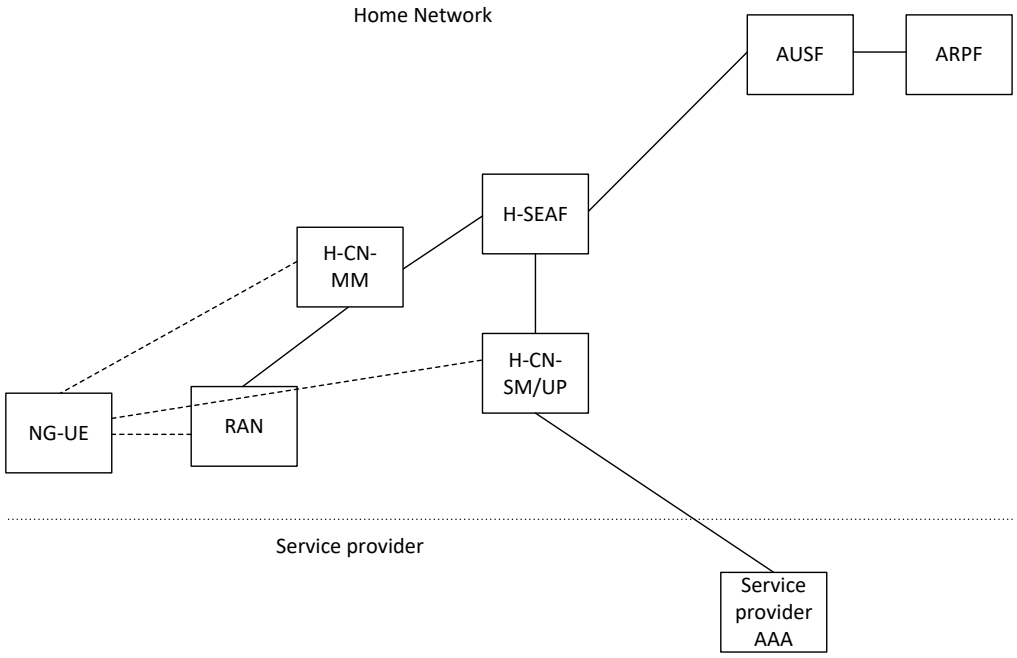


Figure 5.1.4.6.2.1-3: Architecture for authentication framework in non-roaming scenario with secondary authentication with a service provider

Editor's note: The expectation is that the H-CN-SM/UP to Service provider AAA interface will play a role similar to SGi.

This functional split requires a new key hierarchy and corresponding security and key derivation procedure.

5.1.4.6.2.1.2 Alternative Roaming Architecture

The architecture described in the previous has the feature that in the roaming use case (see figure 5.1.4.6.2.1-2) an authentication run can leave a key in the home network that means that additional keys that are not bound to the visited network can be derived without requiring a fresh authentication. The H-SEAF (a SEAF in the home network) is the network element that is proposed to hold this key. The reason for using the SEAF is that a SEAF needs to be stateful after an authentication run as it will hold the key that results from the authentication run.

The alternative possibility would be to use the AUSF to hold such a key. If there is a need for the key at the H-SEAF, then the H-SEAF needs to request the key from the AUSF. This has the disadvantage that the AUSF has now become stateful between authentication runs, i.e. it needs to store a key, in addition to the SEAF which is already stateful. Figure 5.1.4.6.2.1.2-1 provides the architecture for the roaming case when a key is held in the AUSF. The difference between this figure and figure 5.1.4.6.2.1-2 is that the interface between the V-SEAF and H-SEAF become an interface between the V-SEAF and the AUSF.

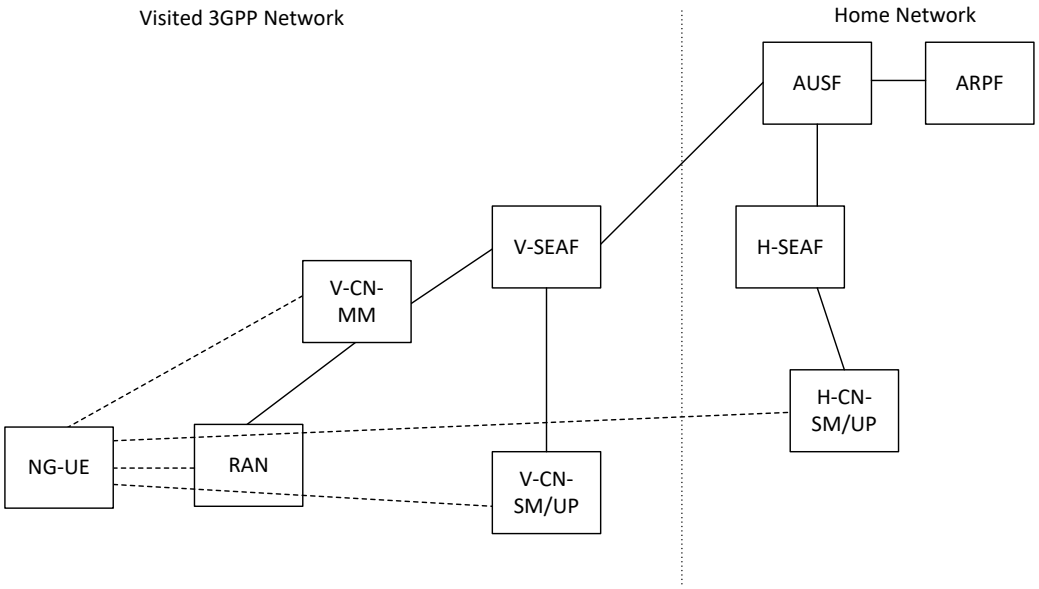


Figure 5.1.4.6.2.1.2-1: Alternative architecture for authentication framework in roaming scenario with AUSF holding a key after the authentication run

5.1.4.6.2.1.3 Architecture for untrusted non-3GPP access in the roaming scenario

When the NG-UE is roaming, it may connect to the NGC through an untrusted non-3GPP access network. In this case, it is assumed that there is no NG-PDG in the visited network and the NG-UE connects to an NG-PDG in the home network. In the NextGen system, untrusted non-3GPP access is made through a NG-PDG, where the NG-UE establishes an IPsec tunnel with the NG-PDG.

If the NG-UE has previously registered to the NGC, then the NG-UE will have been authenticated and this authentication results in a security context (i.e., $K_{H\text{-}SEAF}$) being established in the H-SEAF. The NG-UE establishes an IPsec tunnel with the NG-PDG in the HPLMN based on the security context established at the H-SEAF. If the NG-UE has not been registered to the NGC, the NG-UE performs an authentication (e.g., EAP authentication) through the NG-PDG.

Editor's Note: It is FFS whether the H-SEAF obtains the $K_{H\text{-}SEAF}$ during the authentication run or upon request by the H-CN-CP.

Editor's Note: The NG-PDG needs to be aligned with SA2 terminology.

Editor's note: The terminology used in between different subclauses of this solution needs aligning.

NOTE 1: When the NG-UE connects to the NG-PDG before registering to the VPLMN, the NG-UE may performs a full authentication with the AUSF if there is no valid anchor key.

NOTE 2: When the NG-UE attempts to connect to NG-PDG, the NG-UE does not need to perform fresh authentication if the NG-UE has already successfully authenticated and registered to the NGC.

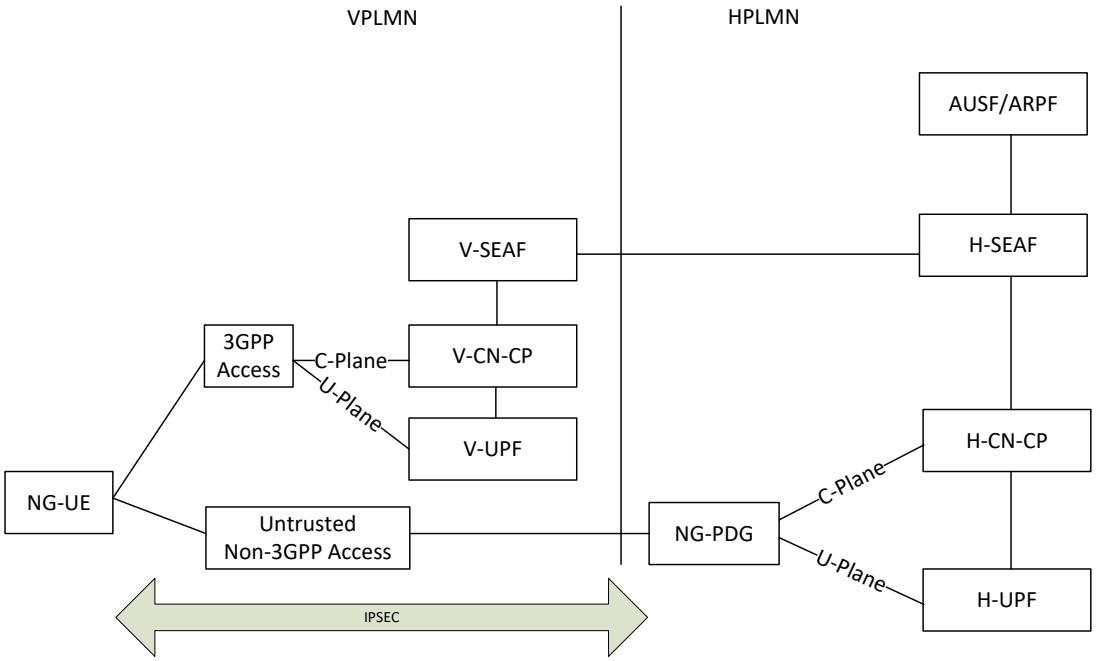


Figure 5.1.4.6.2.1.3-1 Architecture for non-3GPP access in the romaing scenario

5.1.4.6.2.1.4 Procedure for home-terminated user plane session establishment for the roaming scenario

Figure 5.1.4.6.2.1.4-1 show a flow for establishing security between the NG-UE and a Home UP-GW when the UE is roaming. If no key is kept in the HPLMN from the authentication that happens in step 5 (either the AUSF or the H-SEAF), then it will be necessary to run an additional authentication at step 17.

Editor's note: Feasibility of Home UP-GW termination of the user plane security need to be considered in coordination with SA2 and RAN2.

Details of how to protect the user plane between the UE and UP-GW are provided in solution 1.25.

NOTE 1: Does not support LI in VPLMN in the case of the user plane confidentiality protection terminating in the HPLMN.

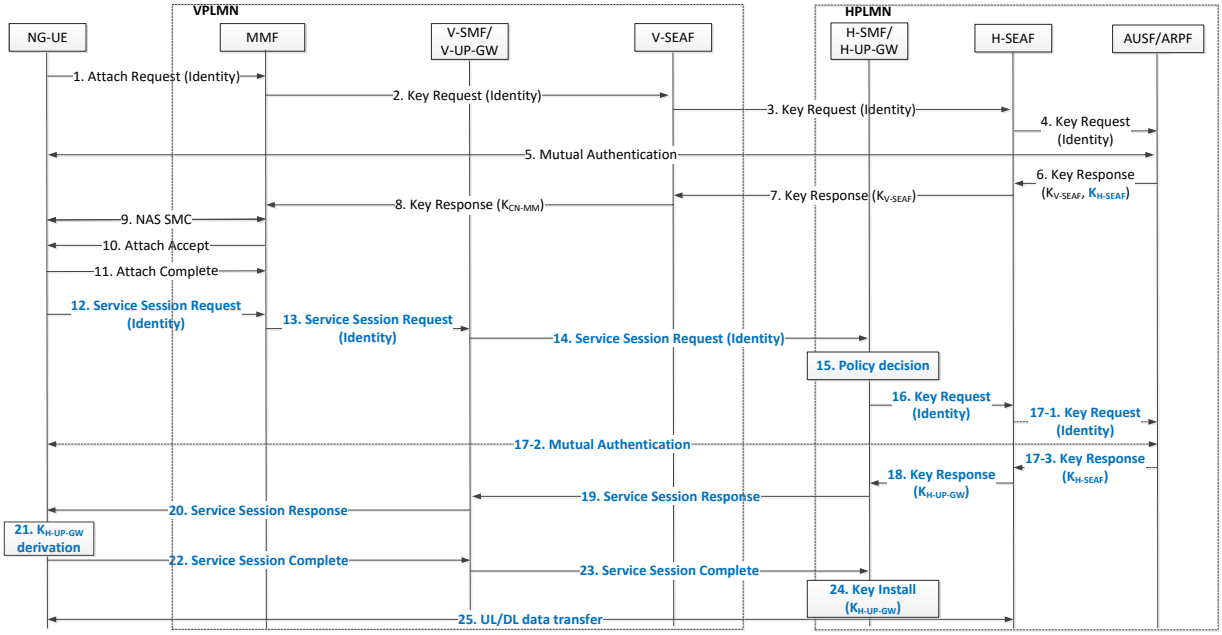


Figure 5.1.4.6.2.1.4-1 authentiation and home terminated user plane session establishment for the roaming scenario

NOTE 2: Figure 5.1.4.6.2.1.4-1 shows MM procedures followed by separate SM procedures. This does not preclude this procedures being trigger simultaneously.

1 – 11. The NG-UE performs an attach procedure to the NextGen network. At the successful completion of the mutual authentication (at step 5), the AUSF provides the H-SEAF with K_{H-SEAF} and the V-SEAF with K_{V-SEAF}, from which subsequent keys are derived (e.g., NAS keys, AS keys, UP-GW keys).

NOTE 3: An alternative would to hold a key in the AUSF. With this alternative step 6 would only contain the K_{V-SEAF} and steps 16 and 18 would become mandatory.

12. The NG-UE sends a service session request messge to the NextGen network to establish a service session in which the user plane (and the user plane security) terminates at the HPLMN. The request includes the UE identity that is associated with K_{H-SEAF} in the H-SEAF and an indication of security termination at H-UP-GW. The identity may include a NAI that can be used by the NextGen network to route the request to the SMF in the HPLMN (i.e., H-SMF).

NOTE 4: The UE security capability is provided in the service session request message.

13. The MMF, upon receipt of the service session request from the NG-UE, determines the V-SMF which interfaces with the H-SMF in the HPLMN and forwards the service session request to the V-SMF.

14. The V-SMF forwards the service session request to the H-SMF.

15. The H-SMF determines whether the NG-UE is allowed to create a home terminated service session based on the NG-UE subscription profile.

16. The H-SMF sends a key request for the home terminated user plane security protection (i.e., $K_{H-UP-GW}$) to the H-SEAF.

17-1 – 17.3. The H-SEAF, upon the receipt of the key request, checks whether it has a valid security context (K_{H-SEAF}) for the NG-UE. If the H-SEAF does not have a valid K_{H-SEAF}, the H-SEAF sends a key request to the AUSF. If the H-SEAF determines that a fresh authentication is required (e.g., due to the key expiry), the H-SEAF triggers the authentication by sending a key request with an indication of fresh authentication to the AUSF. The AUSF sends a K_{H-SEAF} to the H-SEAF.

NOTE 5: if the H-SEAF already has a valid K_{H-SEAF} obtained during the prior authentication, the steps 16 to 18are skipped.

Editor's note: It is expected that the authentication in step 17.2 is carried between the NG-UE and H-SM/UP-GW in NAS SM signalling via the MMF and between the H-SM/UP-GW and AUSF via the H-SEAF. The full details are FFS.

18. The H-SEAF derives a $K_{H\text{-}UP\text{-}GW}$ from the $K_{H\text{-}SEAF}$ and sends the $K_{H\text{-}UP\text{-}GW}$ to the H-SMF in the key response message.

Editor's Note: Whether SM message protection is necessary in addition to NAS protection and how to protect SM messages are FFS.

19. The H-SMF sends the service session response message to the V-SMF to grant the service session creation.

20. The V-SMF forwards the service session response message to the NG-UE via the MMF.

21. The NG-UE derives $K_{H\text{-}UP\text{-}GW}$ from $K_{H\text{-}SEAF}$ and starts protecting the user plane traffic for the service session based on the service session response from the H-SMF.

22. The NG-UE sends the service session complete message to the V-SMF to acknowledge the receipt of the response message. 23. The V-SMF forwords the service session complete message to H-SMF.

24. The H-SMF install the $K_{H\text{-}UP\text{-}GW}$ at the H-UP-GW.

25. UL/DL data transfer for the home terminated PDU session is protected using $K_{H\text{-}UP\text{-}GW}$.

5.1.4.6.2.2 Key Hierarchy

A key hierarchy for the NextGen system is shown in Figure 5.1.4.6.2.2-1. In general, the key hierarchy is similar to that of LTE with the following differences:

introduction of an additional layer of key hierarchy that allows a key resulting from the authentication to be held in a secure location (in effect this is splitting the K_{ASME} into K_{SEAF} and $K_{CN\text{-}MM}$);

ability to generate keys for termination of the UP security at a user plane gateway that is in the core network (see Key Issue # 1.4);

The details of performing the second are out of scope for this solution.

The description of each key in the key hierarchy is as follows.

- K: the subscription credential that is held in the UE and AAA

- K_{SEAF}: anchor key for the authentication session from which subsequent keys (e.g., CN control plane keys and AN keys) are derived.

NOTE: The derivation of K_{SEAF} is authentication method specific.

- $K_{CN\text{-}MM}$: control plane key bound to a CN-MM. The CN-MM further derives NAS encryption and integrity protection keys from $K_{CN\text{-}MM}$. $K_{CN\text{-}MM}$ may also be used to derive the AN level keys as shown in the below hierarchy.

NOTE: Regardless of whether $K_{CN\text{-}MM}$ is used to derive the AN keys or not, having $K_{CN\text{-}MM}$ is useful as it makes the CN-MM future proof in terms of requiring a new key material in a later release.

Editor's note: If $K_{CN\text{-}MM}$ is not used to derive the AN keys, then justification for the inclusion of $K_{CN\text{-}MM}$ in the key hierarchy is FFS.

- KAN/NH: The key provided to the AN (play the same role as KeNB/NH in LTE). AN further derives RRC encryption and integrity protection keys and UP encryption and integrity protection keys from KAN.

Editor's Note: whether KAN needs to be derived directly by SEAF is FFS. Even if the SEAF directly derives KAN and provides it to the AN, SEAF may derive an intermediate keys (e.g., $K_{CN\text{-}MM}$) in order to respect the key hierarchy. In this case, the parameter(s) used for KCP-CN derivation should be informed to the UE so that the UE derives the same key. This may be considered as a collocated SEAF with the CN-MM.

Editor's Note: whether a new NH derivation is necessary is FFS, i.e. whether there is a need for handovers using a vertical key derivation like in LTE.

- $K_{CN-SM/UP}$: user plane key for an UP-GW when the user plane security terminates at the UP-GW

Editor's Note: whether the user plane security terminates at an AN or an UP-GW is determined by the CN based on subscription information and service type and configured at the UE and the UP-GW.

The details on each key derivation (e.g., key derivation algorithm, input parameters) are FFS.

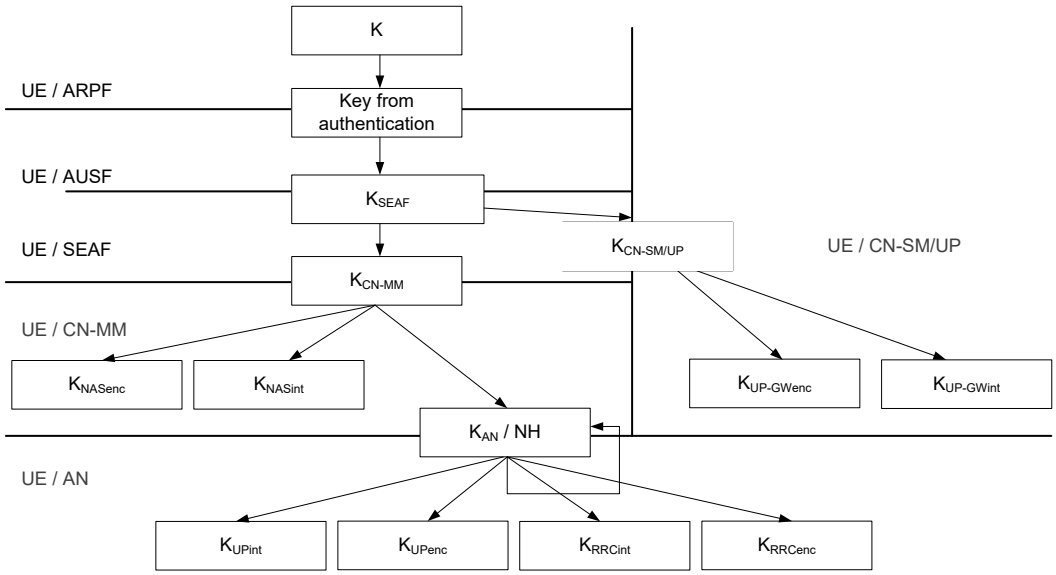


Figure 5.1.4.6.2.2-1: Key hierarchy of the NextGen system

Editor's Note: It is FFS whether the both sets of UP security keys will be needed simultaneously.

The above key hierarchy applies when the UE is in its home network. When the UE is roaming, the key hierarchy applies for the serving network (remembering that the ARPF and AUSF are in the home network in this proposed architecture). In addition (for the roaming case), there is a K_{SEAF} for the home network which can be used to calculate the $K_{CN-SM/UP}$ keys for use in the home network.

5.1.4.6.2.3 Possible example procedures using the security anchor

5.1.4.6.2.3.1 General

The following subclause contains some possible procedures involving the security anchor. The procedures are based on LTE procedures and are provided to show how a security anchor may be used.

Editor's note: The procedures are only examples and may need to be updated to keep aligned with any SA2 decisions

5.1.4.6.2.3.2 Key derivation during the attach procedure

Figure 5.1.4.6.2.3.2-1 shows the security procedure and corresponding key delivery during the UE attach procedure.

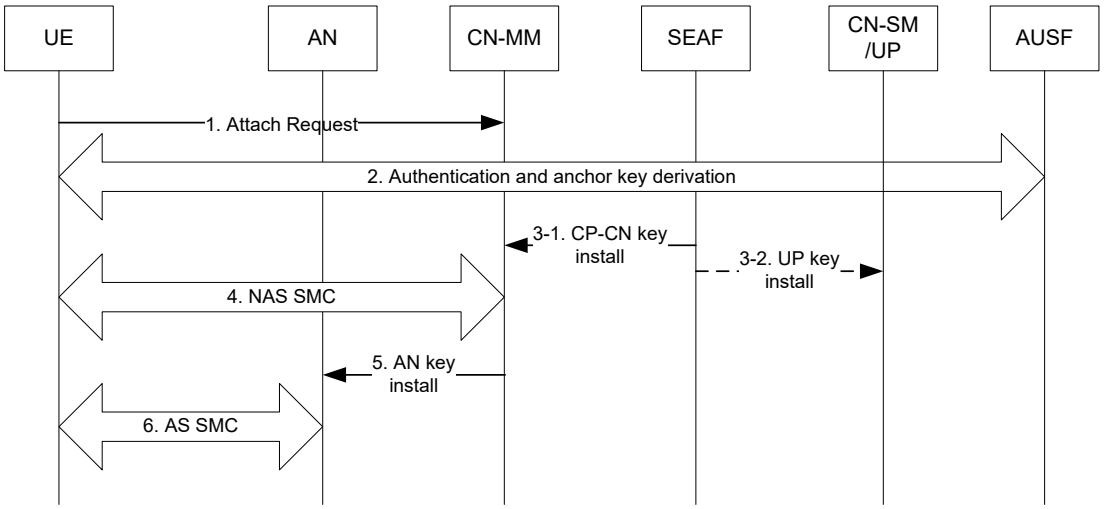


Figure 5.1.4.6.2.3.2-1: Security procedure during the attach

1. The UE sends an attach request to the network. The attach request is routed to the CN-MM based on a certain network function selection rule (e.g., CN-MM selection at AN).

2. The CN-MM triggers the authentication procedure. A successful authentication information results in an authentication session root key (i.e., K_{SEAF}) being available at the UE and sent to the SEAF. The exact details of the flows here depend on the authentication method being used.

3. The SEAF derives a key for the CN-MM that is managing the UE (i.e., K_{CN-MM}) and sends the key to the CN-MM. Additionally, the CN-MM derives a key for the CN-SM/UP selected for the UE (i.e., KUP-GW) and sends it to the CN-SM/UP.

Editor's Note: A CN-SM/UP selection procedure should be defined by SA2.

4. The CN-MM establishes a NAS security context for the UE by performing a NAS security mode command procedure with the UE.

5. The CN-MM derives a key for the AN serving the UE (KAN) and sends it to the AN.

6. The AN establishes an AS security context for the UE by performing an AS security mode command procedure with the UE.

5.1.4.6.2.3.3 Key derivation during the NG2-based handover

The figure 5.1.4.6.2.3.3-1 describes the security procedure during the NG2-based handover, i.e., handover involving CN-MM relocation. The handover procedure is described based on that of LTE (i.e., S1-based HO). The difference from the S1-based HO in LTE is that when the Target CN-MM receives a Forward Relocation Request message from the Source CN-MM, it obtains a fresh key from the SEAF, thereby deriving the AN key for the Target AN.

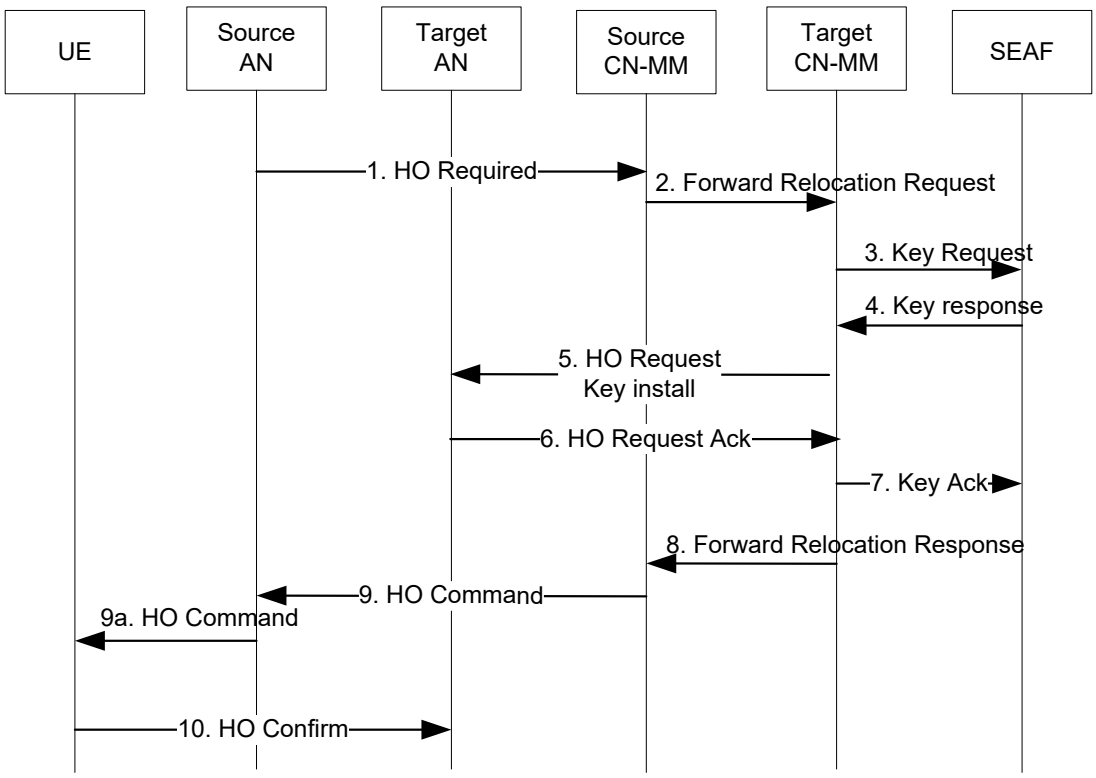


Figure 5.1.4.z.2.3.3-1: Security procedure during NG2-based handover

1. The source AN sends a Handover Required message to the source CN-MM.

2. The source CN-MM sends a Forward Relocation Request to the target CN-MM.

Editors' note: It is FFS whether handovers that support a change of SEAF will be needed.

3. The target CN-MM request a key to the SEAF. If the target CN-MM has a cached key for the UE, it removes the cached key.

4. The SEAF derives a fresh key for the target CN-MM and sends it to the target CN-MM.

5. The target CN-MM derives a key for the target AN and sends it to the target AN along with the handover request message.

6. The target AN sends the handover request acknowledgement message to the target CN-MM. By having the AN key, the target AN is ready to receive a protected RRC message from the UE. In case the target AN rejects the handover request, it shall discard the key received from the target CN-MM in step 5.

7. The target CN-MM sends a key acknowledgement message to the SEAF to indicate that the key derived for the target CN-MM is in use.

NOTE: This key acknowledgement may be optional. Whether the key ack is necessary may be determined based on the parameters used for key derivation.

8. The target CN-MM sends a forward relocation request to the source CN-MM.

9. The source CN-MM sends a handover command to the source AN. The handover command contains the information on the target CN-MM and target AN with which the UE can derive the corresponding keys.

10. The UE derives the key for the target CN-MM and based on which, derives the key for the target AN. The UE further derives the subsequent keys (RRCenc, RRCint) to protect RRC messages and user plane traffic. The UE sends a handover confirmation message to the target AN after protecting the message using the derived keys.

5.1.4.6.2.3.4 Key derivation for the idle mode mobility

The figure 5.1.4.6.2.3.4-1 describes the security procedure during the idle mode mobility, i.e., tracking area update procedure. The tracking area update procedure is described based on that of LTE. The difference from the LTE TAU is that the TAU request is verified by the old CN-MM and acknowledged to the new CN-MM because the old CN-MM does not share the security context with the new CN-MM in the presence of SEAF.

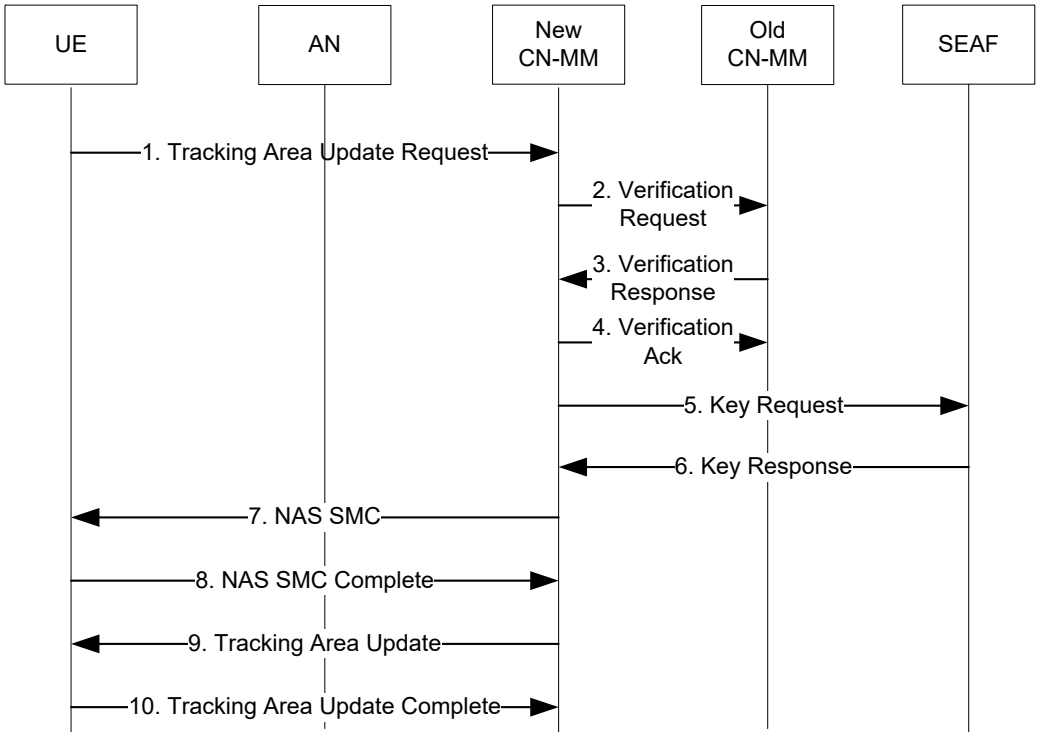


Figure 5.1.4.6.2.3.4-1: Security procedure during tracking area update

1. The UE sends a tracking area update (TAU) request to the network.

2. The new CN-MM identifies the old CN-MM based on the UE identifier (e.g., S-TMSI or GUTI) and requests TAU request message verification to the old CN-MM.

3. The old CN-MM verifies the TAU request and responds to the new CN-MM.

4. The new CN-MM acknowledges the receipt of the response message to the old CN-MM.

5. The new CN-MM requests a key to SEAF.

6. The SEAF derives a key for the new CN-MM and send the key to the CN-MM.

7. The new CN-MM and the UE performs NAS security mode command (SMC) procedure and tracking area update procedure as shown in step 7 – 10.

5.1.4.6.3 Evaluation

TBD

5.1.4.7 Solution #1.7: Serving functions all deployed in secure location

5.1.4.7.1 Introduction

This solution addresses key issue #1.14.

5.1.4.7.2 Solution details

Deploy all serving functions in secure location, even close to AN, makes the development of NextGen system easier to satisfy security requirement.

5.1.4.7.3 Evaluation

FFS

5.1.4.8 Solution #1.8: Key hierarchy for NextGen

5.1.4.8.1 Introduction

This solution addresses the key issue "#1.7 key hierarchy" and proposes a key hierarchy for NextGen network in accordance with reference architecture defined in TS23.501.

Editor's Note: Need of SM key and separate slice specific key for SM is FFS

The proposed key hierarchy supports (1) common C-plane keys for MM (Mobile Management) messages, (2) slice-specific keys for SM (Session Management) messages and U-plane data, (3) keys for other AN (Access Network) than 3GPP and (4) legacy keys for existing 3GPP radio network such as E-UTRAN and non-3GPP radio network.

5.1.4.8.2 Solution details

5.1.4.8.2.1 Architecture

The reference architecture for non-roaming scenario is shown in TS23.501.

In the architecture, AMF (Access and Mobility Management Function) includes Security Anchor Function (SEAF) and Security Context Management Function (SCMF). SEAF is a function that performs UE authentication for connection via different access networks, and interacts with AUSF for retrieving authentication data stored in UDM (Unified Data Management). SCMF manages security context for both C-plane and U-plane functionality. The C-plane functions for MM and SM messages are decoupled and handled by AMF and SMF (Session Management Function), respectively, while U-plane data is handled by UPF. This functional split requires new key hierarchy and corresponding security and key derivation procedures. In addition, the generation of keys for network slicing in NextGen system is also required to be addressed by this key hierarchy.

5.1.4.8.2.2 Key Hierarchy

A key hierarchy for the NextGen system is shown in Figure 5.1.4.8.2.2-1. In general, the key hierarchy is similar to that of SAE/LTE with the differences like (1) Separation of C-plane keys for NAS MM and SM (2) Ability to generate slice-specific keys for NAS SM and keys (K_{UP}) for termination of the UP security at a user plane gateway (3) Provision of keys for other AN than 3GPP (4) Provision of legacy keys for existing 3GPP and non-

3GPP radio network. It is assumed that network slicing exists only in core network and there's no network slicing in RAN.

The description of each key in the key hierarchy is as follows.

K	-	The subscriber credential that is held in the UE and UDM.
CK, IK	-	Confidentiality and integrity key for backward compatibility.
K_{SEAF}	-	Security anchor key derived from K for authentication and derivation of subsequent keys.
K_{NAS_MM}	-	Control plane key commonly used for NAS MM messages to derive integrity and encryption protection keys.
K_{NAS_SM}	-	Control plane key provided for NAS SM messages of each network slice to derive integrity and encryption keys.
K_{AN}/NH	-	Key provided to the AN (similar to KeNB/NH in LTE) to derive RRC and UP integrity and encryption keys.
K_{UP}	-	User plane key provided for each network slice when the user plane security terminates at the UPF.
K_{AN_other}	-	Key for other NextGen AN than 3GPP
K_{3GPP_AN}	-	Legacy key for existing 3GPP radio network

$K_{non\text{-}3GPP\_AN}$ - Legacy key for existing non-3GPP radio network

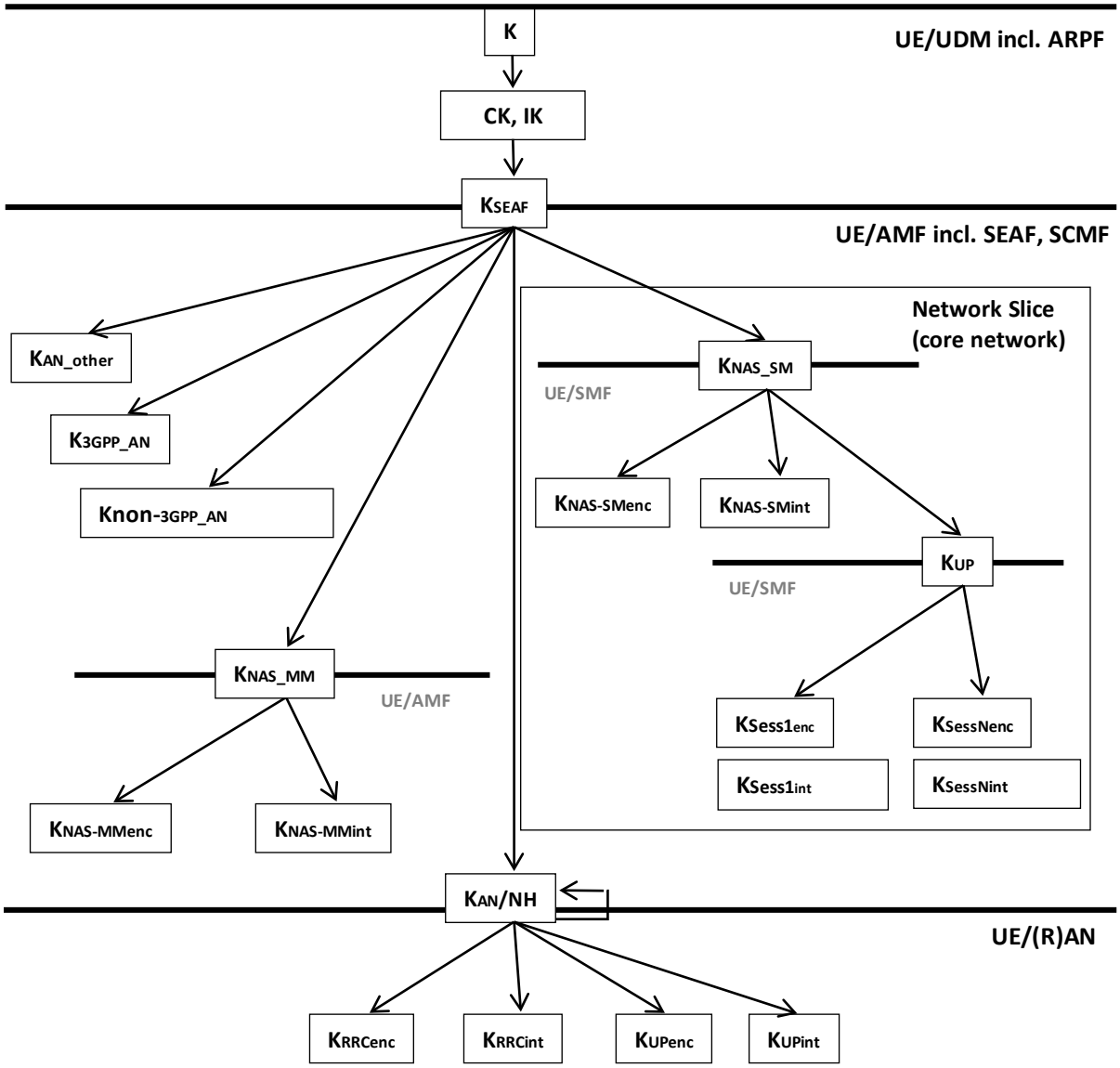


Figure 5.1.4.8.2.2-1: Key hierarchy of the NextGen system.

5.1.4.8.2.3 Key derivation

As well as key hierarchy, key derivation also includes similar process to that of SAE/LTE. Firstly, K_{SEAF} is derived during AKA (Authentication and Key Agreement) procedure in both UE and UDM, where NSSAI (Network Slice Selection Assistance Information) is additionally used as one of input parameters. A diagram of key derivation for the subsequent keys in the key hierarchy for NextGen system is shown in Figure 5.1.4.8.2.3-1. Each key is derived by inputting its upper layer key and parameters into KDF (Key Derivation Function). The three keys for NAS MM, NAS SM and AN are derived from K_{SEAF} with parameters of COUNT for NAS MM key, SST (Slice/Service Type) and SD (Slice Differentiator) for NAS SM key, and NAS Uplink Count for AN key, where COUNT is a value incremented with mobility event in AMF. RAN slice parameters should be input if there is network slice in AN. The key for U-plane (K_{UP}) is derived from NAS SM key with parameters of Counter, Time limit and Data volume, where Counter is incremented with update of K_{UP}, Time limit is the stipulated time for which K_{UP} is valid, and Data volume indicates the amount of data that is expected to be used. Finally, the keys for integrity and confidentiality protection, which have suffix of "int" and "enc", respectively, are derived with its upper layer key and algorithm ID, where a value of Counter is also input for derivation of

$K_{Sessint}$ and $K_{Sessenc}$.

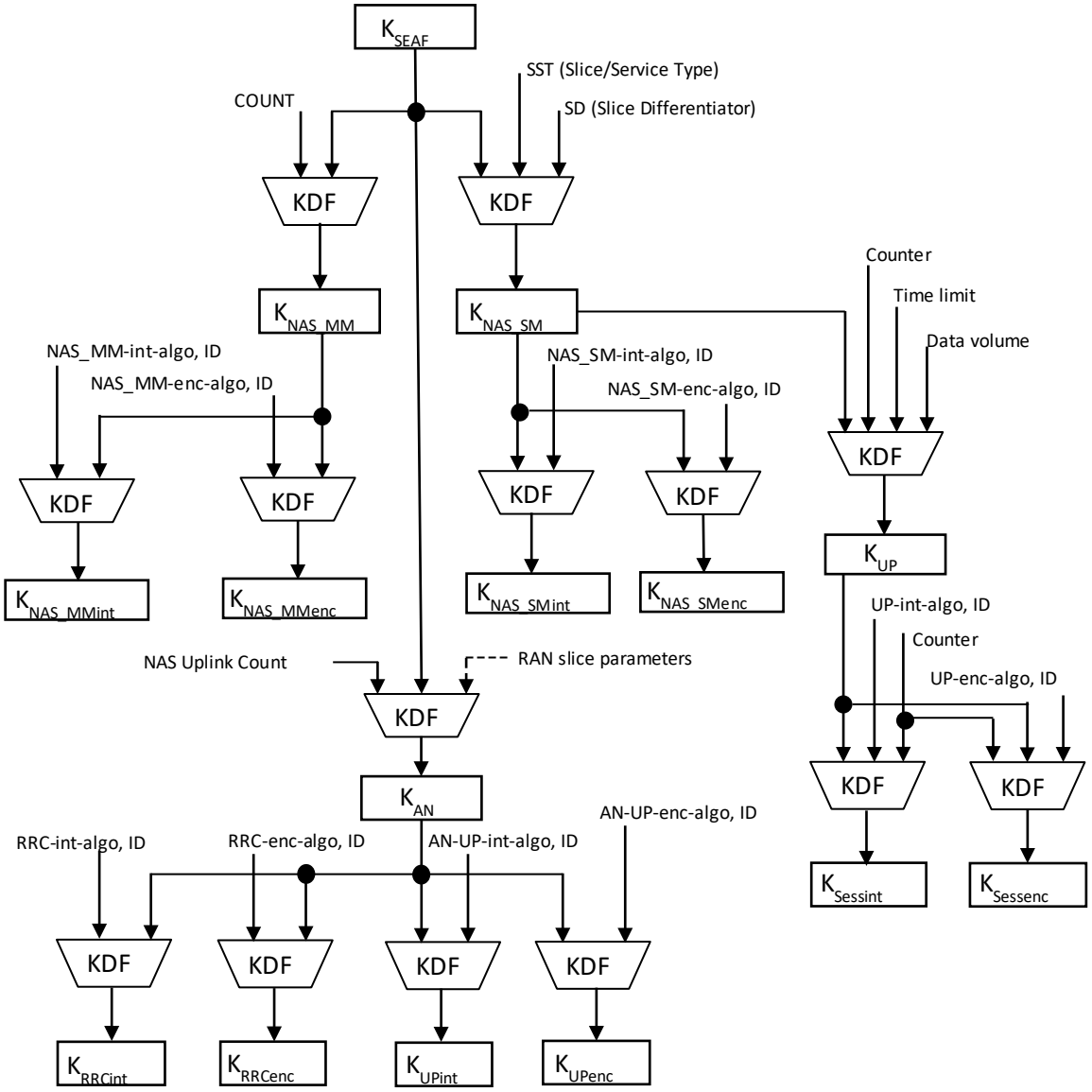


Figure 5.1.4.8.2.3-1: Key derivation diagram for the NextGen system.

Editor's Note: The use of data volume parameter in Key derivation is FFS.

5.1.4.8.3 Evaluation

5.1.4.9 Solution #1.9: Key hierarchy and the related procedure

5.1.4.9.1 Introduction

This solution proposes a key hierarchy and proposes solutions for the key hierarchy and its procedure. This key hierarchy addresses key issue #1.3" User plane integrity between UE and network", Key Issue #1.4 "User plane confidentiality between UE and network" and their related solution #1.5, and Key Issue #3.4 "Security context sharing" and its solution #3.3.

This solution includes the control plane protection of NAS and AS signalling, and user plane protection of PDU session. Some enhancements may be required to this solution for slicing scenario, e.g., support of separate NAS security for different slices.

Lenovo Ex. 1007
Page 80

The UP plane protection key addresses key issue #1.3, key issue #1.4 and their related solution #1.5. Keys used in different access technologies address the key issue #3.4 and solution #3.3. Also, a control plane key for the NAS signalling protection is proposed.

5.1.4.9.2 Solution details

5.1.4.9.2.1 Architecture

According to the solution 4.15 in SA2 TR 23.799, a common node i.e. NAS entry function, (figure 5.1.4.9.2.1-1) for the NAS connection was introduced, in order to route the NAS signalling to the related NAS handling network functions (i.e. NG-SM or NG-MM). NAS entry function could be co-located within MM, or independently deployed for the NAS routing. With this mechanism, UE only need to maintain one NAS security context for the NAS signalling protection.

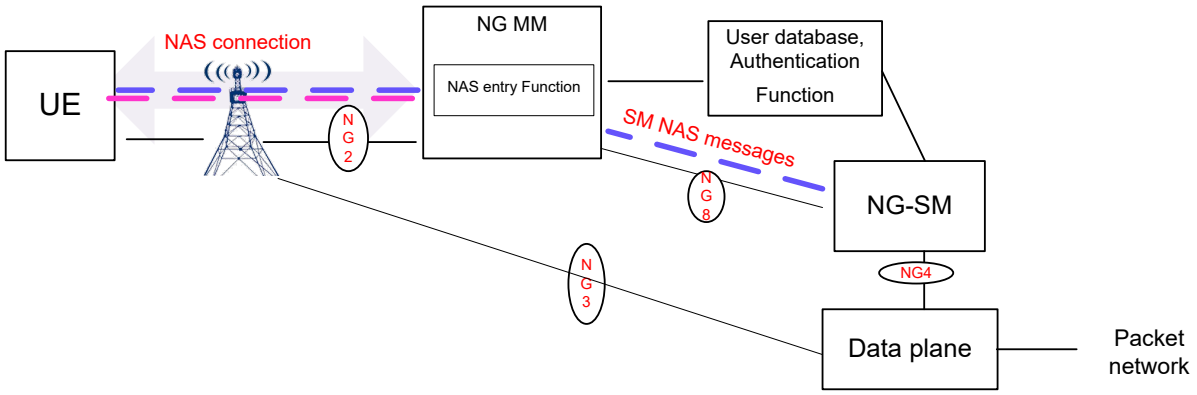


Figure 5.1.4.9.2.1-1: Common interfaces towards UE, AN with MM and SM decoupled

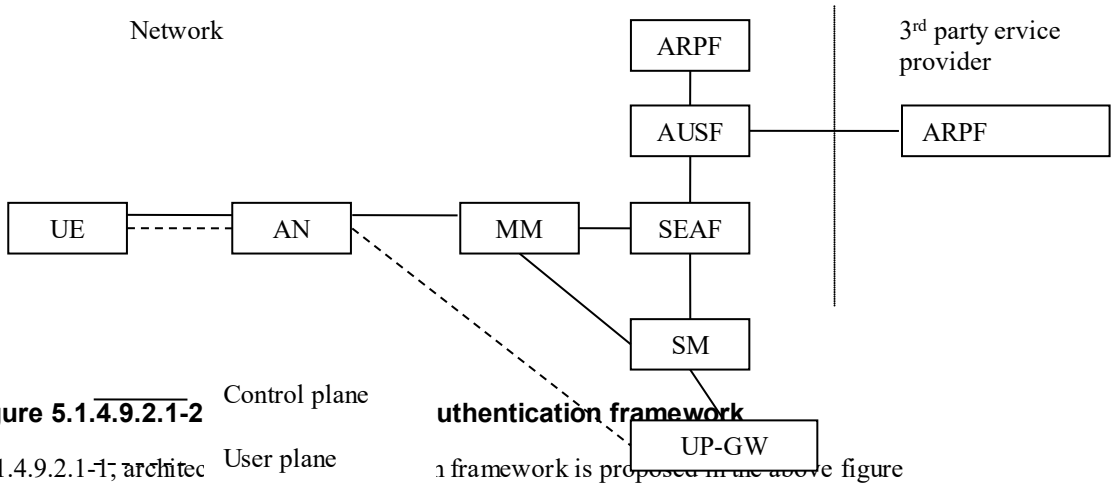


Figure 5.1.4.9.2.1-2 uthentication framework

According to the figure 5.1.4.9.2.1-1, architec ı framework is pro e figure 5.1.4.9.2.2.-2. For the above architecture, NAS entry function could be located in the MM. Definitions on the ARPF, AUSF, SEAF could be found in the security area #2 "authentication".

For 5G, the 3rd party service provider connectivity scenario shall be considered from the security point of view. The ARPF residing in the 3rd party system is controlled by the service provider (e.g. IoT service provider) is added in the architecture, which stores and manages the 3rd party service subscriptions. Symmetric key mechanism should be supported by the 3rd party service credential.

In case asymmetric key mechanism (e.g. Identity-based cryptosystem) is used for authentication, the intermediate key can be generated during the authentication procedure. The intermediate key is used as the shared key between UE and network.

Interface between AUSF- ARPF residing in the 3rd party system is established based on the assumption that mutual trust between the operator and the 3rd party service provider is established. Hence, 3rd party service subscription could be transferred with the interface AUSF- ARPF residing in the 3rd party system.

In conclusion, the key hierarchy is designed with the following assumptions:

Lenovo Ex. 1007
Page 81

- An aggregate node NAS entry function (e.g. NAS entry function in section 6.4.15) for all the NAS signalling protection between UE and CN is suggested.

5.1.4.9.2.2 Key hierarchy

In this section, a key hierarchy is proposed, according to solution #1.5 and #3.3, in order to addressing the security requirements from key issue #1.3, #1.4 (user plane protection), and #3.4 (security context sharing).

Several principles are listed as followed:

- A common node (i.e. AUSF) should be used for the unified authentication and unified security context for different access technologies.
- Control plane and user plane should be protected separately.
- User plane protection mechanism should be based on the sessions between UE and UP-GW.
- NAS security protection should be applied between the UE and NAS entry function. NAS entry function should maintain prioritized security algorithms list for NAS signalling protection.

According to the above principles, a key hierarchy is given in the following figure 5.1.4.X.2.2-2. Also the descriptions of the keys involved in the key hierarchy are as follows.

- K: the root key or subscription credential shared by USIM and ARPF.
- CK/IK: the cipher key and integrity key, derived from the root key, and shared by USIM and ARPF, compatible with the legacy key hierarchy, such as LTE, or UMTS.
- KNG: The next generation key (similar to the KASME in LTE), derived from CK/IK, and shared by UE, ARPF and authentication unit (AUSF/SEAF).

Keys for CP protection:

- KNAS: NAS signalling protection key, derived from the KNG, generated individually by UE and SEAF, and could be used to generate the NAS signalling encryption key and NAS signalling integrity protection key.

According to the above SA2 solution, NAS entry function is a different network function element from SEAF. Also, according to the above principle, NAS security protection should be applied between the UE and NAS entry function. Therefore, the NAS entry function should generate the NAS encryption and integrity protection key based on the NAS key KNAS received from SEAF.

  - KNASenc: the NAS encryption key, used for NAS signalling confidentiality protection.
  - KNASint: the NAS integrity protection key, used for the NAS signalling integrity protection.

- KANCP: AN signalling protection key, derived from the KNG, and generated individually by UE and AN, could be used to generate the AN signalling encryption key KRRCenc and AN signalling integrity protection key KRRCint.

NOTE: AN protection should support heterogeneous access, e.g. next generation access, Wifi access.

- KRRCenc: the AN encryption key, used for AS signalling confidentiality protection.
- KRRCint: the AN integrity protection key, used for the AS signalling integrity protection.

Keys for UP protection:

- KUP: a user plane protection root key for the user plane protection.

NOTE: KUP could be derived directly from KNG. For the 3rd party service protection, KUP derivation may also relate to the 3rd party service credential (Service authentication).

  - Ksession1-enc: a session confidentiality protection key, which is derived from KUP, is used for the UP protection between UE and UP-GW.
  - Ksession1-int: a session integrity protection key, which is derived from KUP, is used for the UP protection between UE and UP-GW.

Lenovo Ex. 1007
Page 82

One UE could have multiple PDU sessions according to its services. According to solution #1.5, the session protection is managed by one SM, and the keys for these sessions are derived from the key KUP.

Editor's Note: details on the key derivation function inputs are FFS.

Editor's Note: Terminating NAS traffic should be aligned with SA2.

Editor's Note: It's ffs whether the following key hierarchy should be needed.

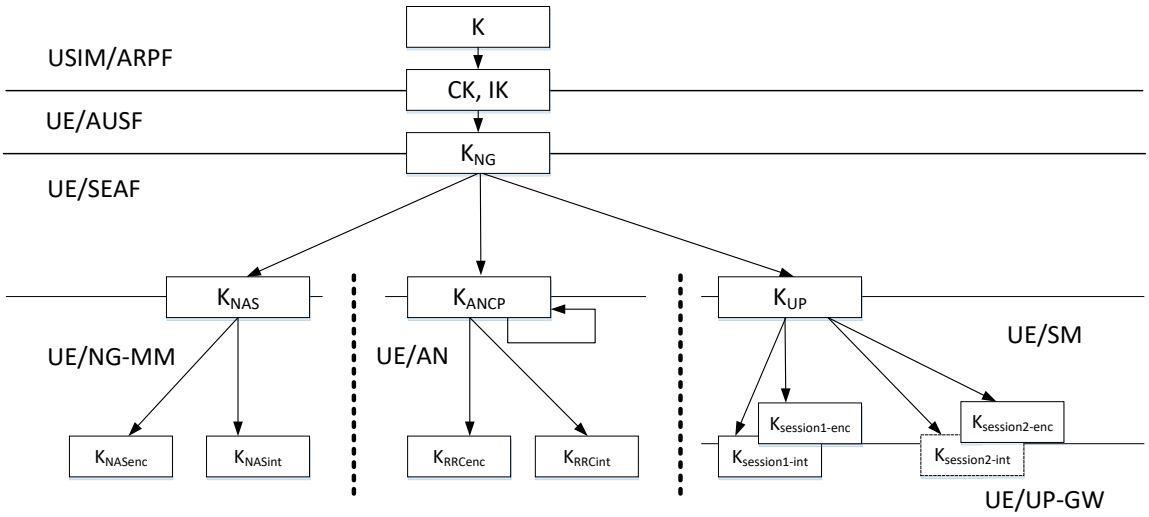


Figure 5.1.4.9.2.2-1: Key hierarchy architecture

Editor's Note: It is ffs if this key hierarchy will address the case of terminating UP security in AN, and if yes, how that is solved in this solution.

5.1.4.9.2.3 Security procedure

In this section, a high level security procedure (Figure 5.1.5.9.2.3-1) is given according to the above key hierarchy.

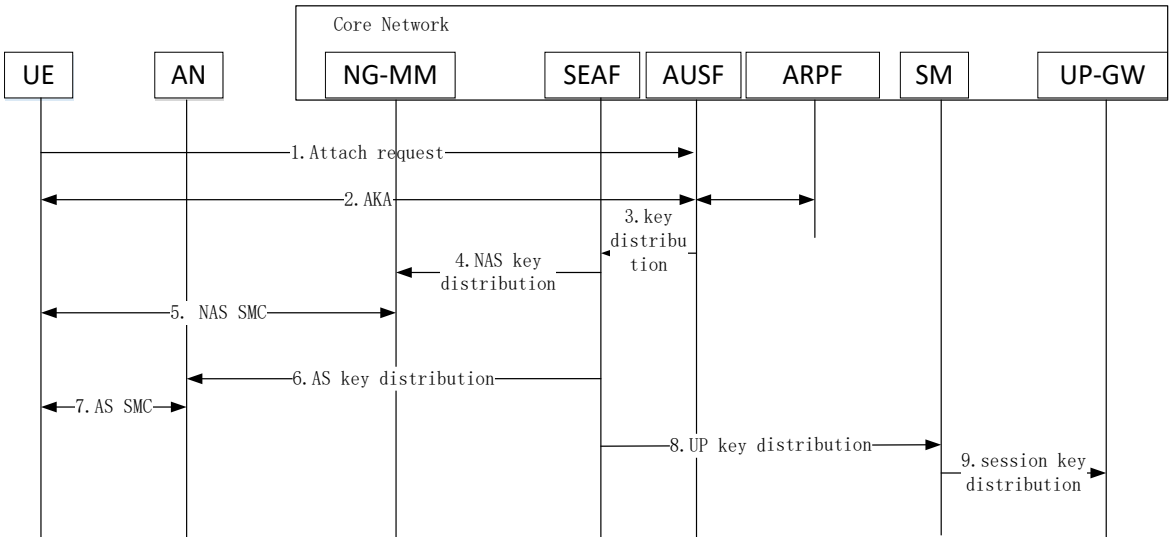


Figure 5.1.4.9.2.3-1: Procedure for the Next Generation protection

Next is the high level description of the procedure.

1. UE initiates the attach request to Network, including its identity (e.g. IMSI).
2. Next, UE and the Network could execute an authentication and key agreement procedure. After the successful authentication, both UE and AUSF/SEAF share the Next Generation key (i.e. KNG).

Lenovo Ex. 1007
Page 83

3. AUSF sends the next generation key K_{NG} to SEAF.
4. SEAF generates the NAS key (i.e. KNAS) for the NAS entry and distributes the NAS key to the NAS entry, which is located in NG-MM.
5. UE and NAS entry should make the NAS security mode command (SMC) procedure to generate the NAS signalling encryption and integrity protection key (i.e. KNASenc, KNASint) for the signalling protection between them.
6. SEAF generates the AN signalling protection key (i.e. KANCP) for the AN, and distributes the AN key to the AN.
7. UE and AN entry should make the AN security mode command (SMC) procedure to generate the AN signalling encryption and integrity protection key (i.e. KRRCenc, KRRCint) for the signalling protection between them.
8. SEAF generates the user plane protection key (i.e. KUP) using KNG, and distributes KUP to the SM. For the 3rd party service protection, KUP derivation may also relate to the 3rd party service credential (Service authentication).
9. SM derives the session key (i.e. Ksession1-enc, Ksession1-int) for this PDU session using KUP according to the security policy, which could be negotiated between UE and SM based on various security requirements, and SM distributes the session key and the security policy to the UP-GW, which is an anchor of the PDU session.

Similarly, UE could generates the user plane protection KUP with the same derivation function as SEAF, then derives the session key (i.e. Ksession1-enc, Ksession1-int) for this PDU session with the same derivation function as SM.

At last, both UE and UP-GW share the same session key and the same security policy, and the UP protection is applied between UE and UP-GW. Detail UP protection setup procedure and security policy negotiation procedure are described in solution 1.5

5.1.4.9.3 Evaluation

TBA.

5.1.4.10 Solution #1.10: UP protection for PDU session (re)establishment triggered by handover

5.1.4.10.1 Introduction

This solution addresses the Key Issue #1.3 and Key Issue #1.4. For the whole handover procedure, the location management procedure is similar to that of current LTE system. But for session management, there are already many options on how to trigger the update of PDU session during handover in SA2.

SA2 introduces a solution (section 6.6.1.2) for PDU session establishment and release triggered by handover as following:

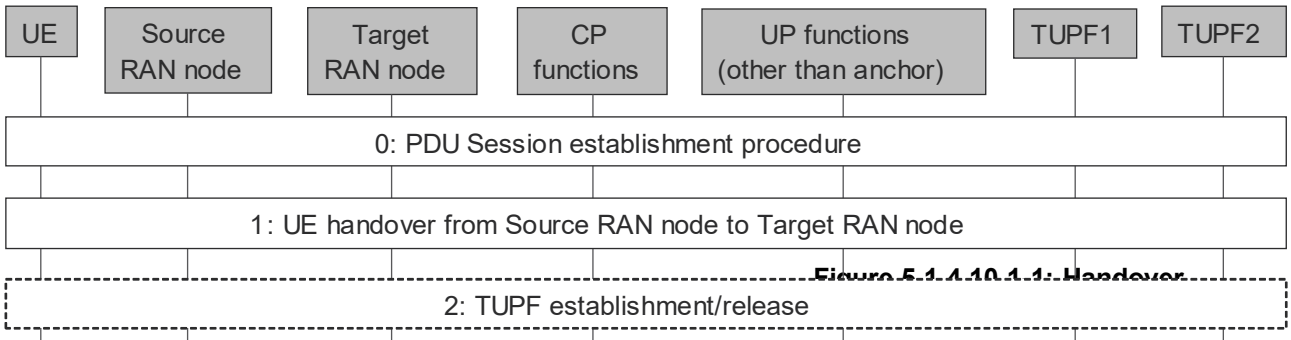


Figure 5.1.4.10.1.1: Handover

It's assumed that "a PDU session to exist between a UE and a user-plane function (called terminating user-plane function (TUPF)). The TUPF terminates the 3GPP user plane and interfaces with the data network." When UE performs handover from source RAN to Target RAN either for X2 or NG2 handover, the PDU session with new user plane path would be established, associating with the new TUPF, and also the new user plane path is from UE to TUPF2. Evenif the TUPF is not changed, the new user plane path is from UE to TUPF1 by TUPF2. In summary, the user plane path

Lenovo Ex. 1007
Page 84

would be updated because of the change of user plane termination point based on new PDU session establishment procedure.

Section 6.6.1.2.3 and Section 6.6.1.2.4 elaborated call flows about the establishment of the new TUPF for different SSC modes always triggered by the CP functions.

In particular, depicted in the following is the message flow illustrating how UE-requested PDU Session (SSC mode3) is established in clause 6.6.1.2.3 TR23.799.

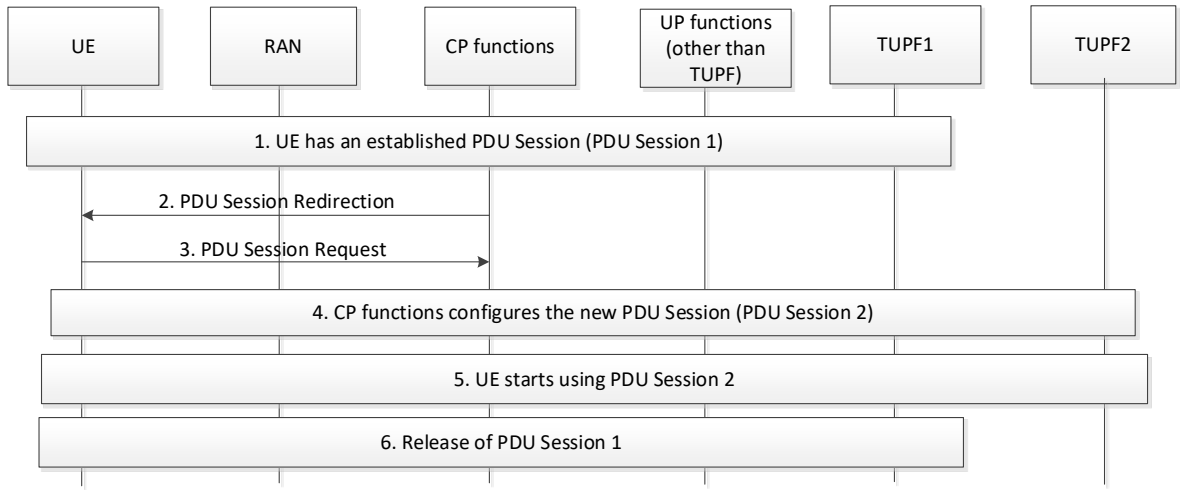


Figure 5.1.4.10.1-2: CN-provided trigger followed by UE-requested PDU Session

Another option Section 6.6.1.2.4 is applicable to multi-homed PDU session only, which depicted as following:

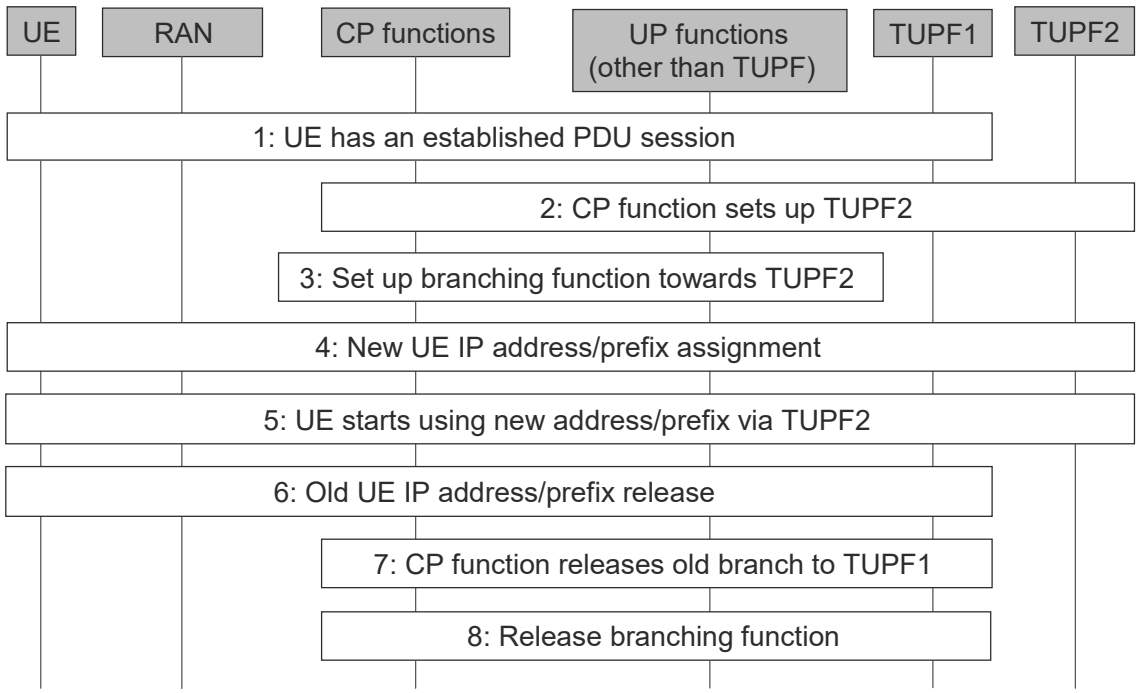


Figure 5.1.4.10.1-3: CN prepared PDU Session followed by notification to UE

According to this solution from TR23.799, this security solution gives the general NG user plane security protection method and main security aspects for handover case. No matter what kind of option, the user plane path would be updated during handover case, then the corresponding security protection should be updated as well.

Lenovo Ex. 1007
Page 85

5.1.4.10.2 Solution details

According to Key Issue #1.4 and Key Issue #1.5, the user plane security protection is session-based, therefore, if the session needs to be changed during the handover procedure, the UP security should also be updated accordingly. This solution addresses the Key Issue #1.4 and Key Issue #1.5. The following figures give the UP security solutions on PDU session (re)establishment triggered by handover.

Based on Key Issue #1.4 and Key Issue #1.5, when session is (re)establishment during handover, the following security aspects should be considered:

- Session security policy would be re-negotiated;
- UP protection key would be updated;

The high-level message flow for user plane security of session (re)establishment during handover is given in the figure as following:

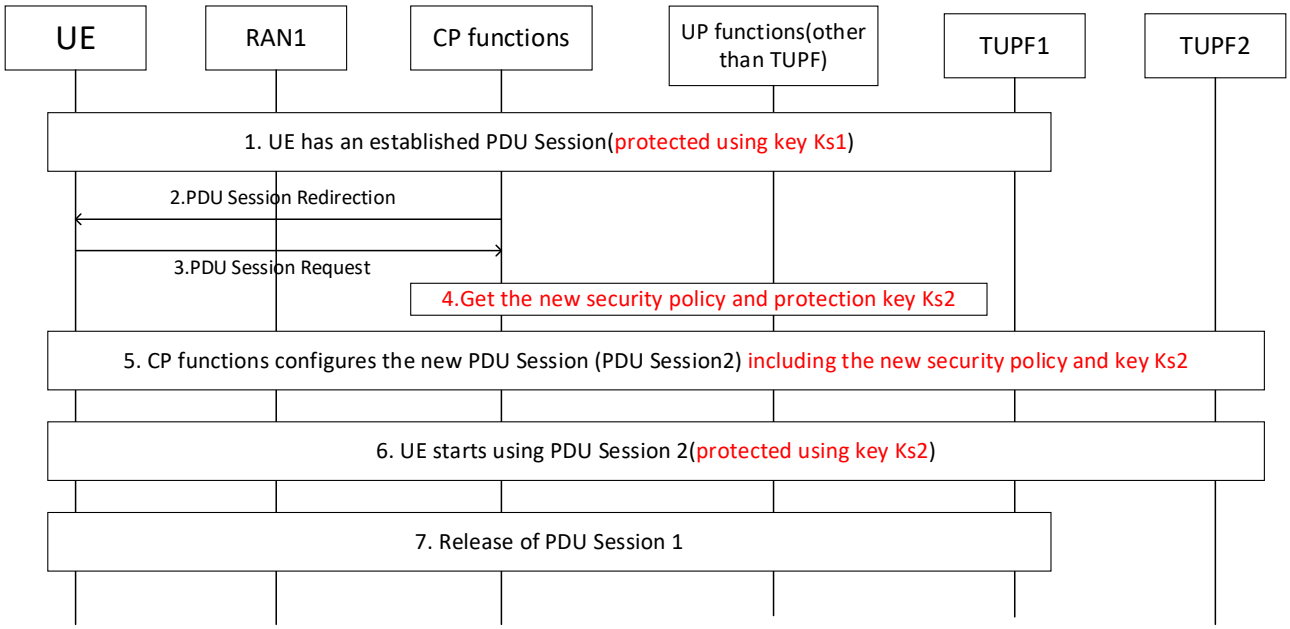


Figure 5.1.4.10.2-1: General UP security procedure for PDU session (re)establishment triggered by handover

1. UE has an established PDU Session (PDU Session 1) protected by using key Ks1. Key Ks1 is shared by UE and TUPF1.

2-3.New PDU Session request is triggered.

4. Before the new PDU Session is established, the new security policy and new key Ks2 for new session should be achieved or negotiated by CP functions and UP functions (other than TUPF). And the Ks2 could be derived based on the new session security policy and the user plane related key.

5. The CP functions configure the user plane path for PDU Session 2, including sending the Key Ks2 to the TUPF2 which would be used to protect the PDU Session 2.

6. UE starts using PDU Session 2 for all new traffic flows protected by key Ks2.

7. PDU Session is released.

In order to map the functional entities related to handover in TR23.799, the detailed security protection procedure of session (re)establishment during handover is given below. In the following solution, the assumptions are:

- SM function relocation is triggered by handover.

During the handover, if the MM/SM need to be relocated, the UE context including security context for the new session may need to be exchanged or updated to align with the new SMFor the user plane function, it is assumed the entity is

Lenovo Ex. 1007
Page 86

UP-GW. If HO happens, MM may trigger the session update through notifying the HO issue to the source SM. The source SM make the SM or UP-GW relocation and update the session for UE based on its policy, therefore, some security context for updated session would be transferred during this procedure.

- The UP-GW function maps to the TUPF.
- The CP functions are elaborated MM, SM.
- The Security Policy Function is a logical function to execute the security policy negotiation or determination.

NOTE: The Security Policy Function could be co-located with other NextGen nodes or it can be a standalone function entity.

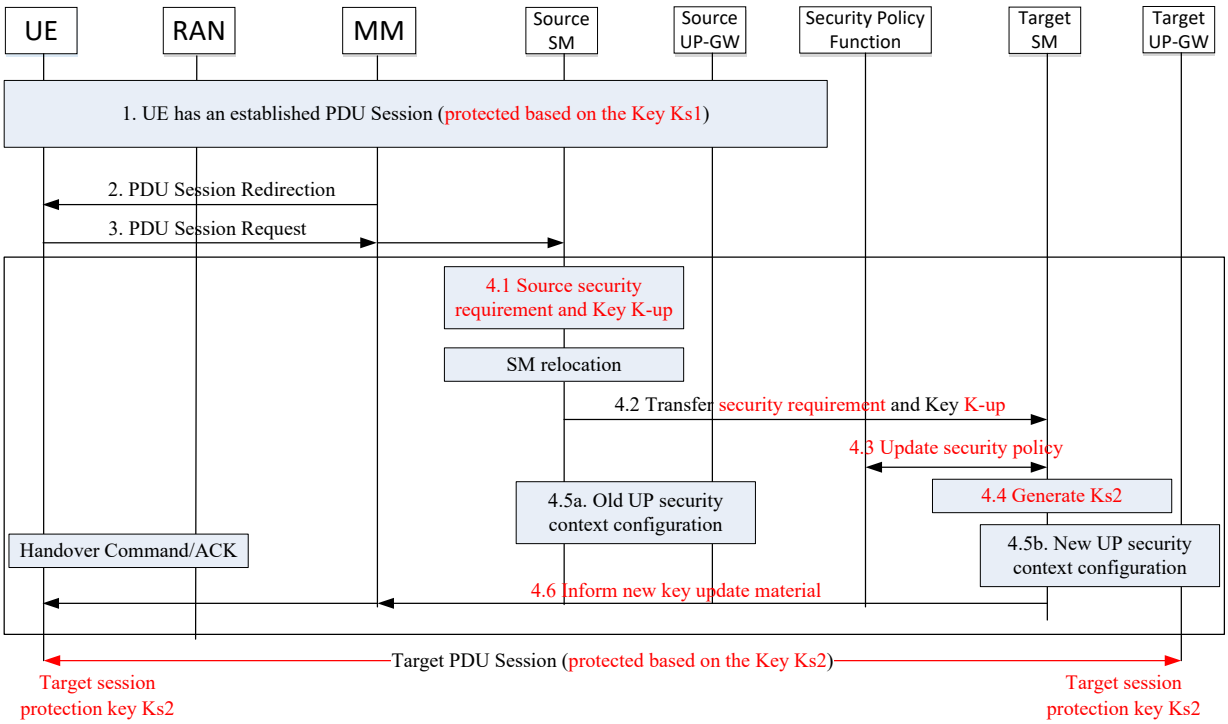


Figure 5.1.4.10.2-2: Detailed security procedure PDU session (re)establishment triggered by handover

Before the target session is established, there is an assumption that the source session is protected between the UE and the source UP-GW using the protection key Ks1. The next steps before step1 are the handover preparation and part of handover execution work. Until the MM receives the PDU Session Request containing UE ID, the source SM would start the security context update work for the new session.

1-3. UE has an established PDU Session (PDU Session 1) protected by using key Ks1. Key Ks1 is shared by UE and Source UP-GW. During handover, new PDU Session establishment request is triggered.

4.1 According to the solution #1.5, the security requirement and key K-up for the user plane data were already obtained or negotiated by source SM function. Also, the Source SM decides whether to relocate from source SM to a target SM or relocate to another UP-GW.

4.2. If the SM does not relocate, source SM and target SM are the same, and step4.2 is not executed. If SM relocation is needed, the source SM sends the security requirement (refers to solution#1.5) and K-up to the target SM via SM relocation message.

4.3. Target SM sends the update security policy request to Security Policy Function in order to achieve the final new security policy based on the security capabilities of target UP-GW.

4.4. Target SM generated Ks2 for the new session based on the final security policy and the K-up.

4.5a-4.5b. Source SM configures the UP security context to source UP-GW. Target SM configures the UP context to target UP-GW.

Lenovo Ex. 1007
Page 87

4.6. Target SM informs user plane security materials to UE by handover procedures, maybe these materials are transfered by the handover related messages in order to make UE generate the Ks2.

After the above procedures, the new session protection key Ks2 is shared by the UE and target UP-GW based on the new security policy.

5.1.4.10.3 Evalution

Tba.

5.14.11 Solution #1.11 High level of Security Architecture

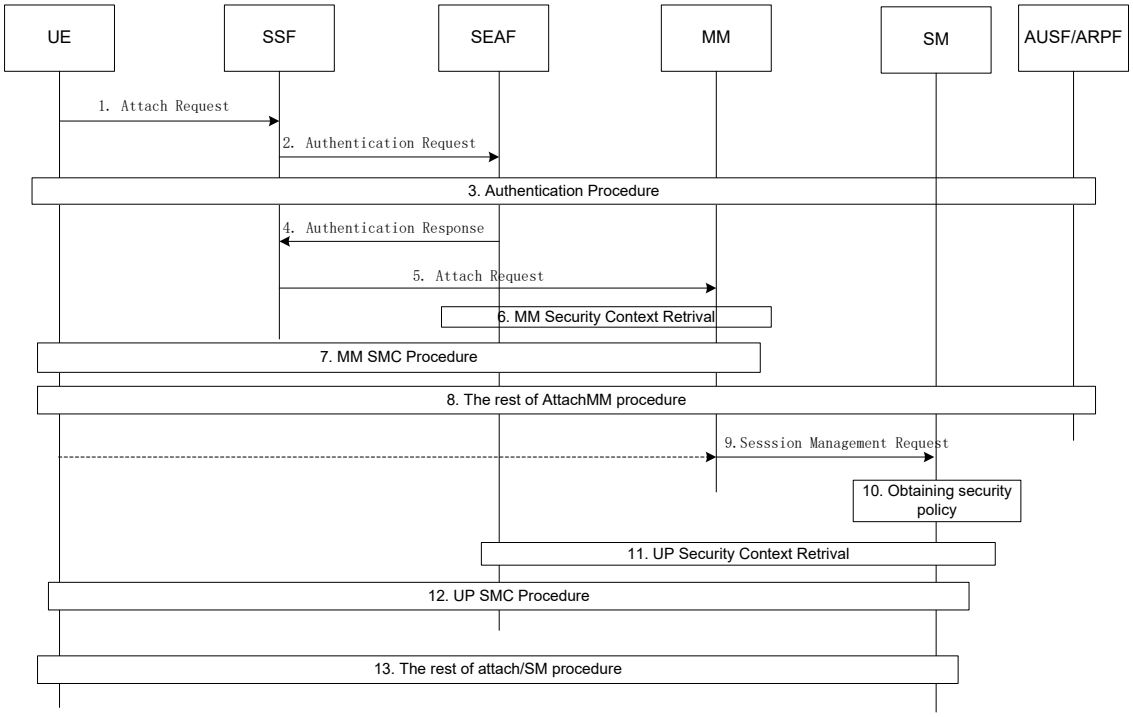
5.1.4.11.1 Introduction

This part is going to show the basic security call flow for the NextGen core part.

5.1.4.11.2 Solution details

Figure 5.1.4.11.2-1 shows a basic security call flow for initial attach. This solution makes following assumptions:

- According to solution #1.1 TR 23.799[2], the initial attach message may be forwarded to an entity which is not the suitable entity to handle the Mobility Management and the following Session Management. In the Figure 5.1.4.11.2-1, SSF/Default CCNF(Common Control-Plane NF) is used to represent this entity.
- The MM is the entity to perform Mobility Management.
- SM is the Session Management function in a specific slice.
- The ARPF stores UE'S profile and the security related information of the UE.



5.1.4.11.2-1: security call flow for initial attach

1. UE sends an initial attach request message to the NextGen.
2. The SSF initiates an authentication request to AUSF for user authentication.
3. The mutual authentication between UE and AUSF

Lenovo Ex. 1007
Page 88

4. The AUSF will notify the SSF the result of the authentication.
5. If the authentication is successful, the entity will forward the attach request to the corresponding entity or the entity in the dedicated network. The entity is the MM according to solution #1.1 of TR 23.799[2]
6. As the MM is not involved in the authentication procedure of step 3, it shall retrieve the Security context from AUSF.
7. The MM initiates the MM SMC Procedure to negotiate the algorithms and activate the security. The MM CP Signalling shall be protected after this procedure
8. The MM completes the rest of attach procedure or MM procedure according the solution in TR 23.799[2].
9. If the initial attach indicates that the SM procedure needs to be executed, the MM will forward the Session Management Request to the SM. If the initial attach does not contain SM procedure, then UE will send Session Management Request to SM some time later.
10. The SM obtains security policy.
11. The SM retrieves the UP security context from the AUSF.

Editor's Note: It is FFS whether SM needs separate NAS security in cases of slicing.

12. After the SM retrieve the UP security context, the SM performs the UP SMC Procedure for activiating UP security.
13. The SM performs the rest of SM procedure or the rest of the attach procedure.

Editor's Note: Terminating NAS traffic should be aligned with SA2.

5.1.4.11.3 Evaluation

5.1.3.12 Solution #1.12: Low latency security technique to protect user plane

5.1.3.12.1 Introduction

As mentioned in paragraph 5.1.3.13.1, the requirement of very low latency (~1 ms) for Next Generation 3GPP system makes the encryption of user data challenging. A trade-off between latency and security can be found for use cases where low value data are exchanged. However, for some other use cases, as industrial factory automation, low latency, integrity and reliability of user data are equally important [7]. It is therefore crucial to find solutions that allow security of communications with ultra-low latency and ultra-high reliability.

The solution presented in this paragraph aims at achieving this goal. It proposed the use of secrecy codes to provide both confidentiality and reliability of user data. The principle is to create radio propagation conditions such that only intended receiver can perfectly decode transmitted information whereas no information will be leaked to any other (potentially malicious) users.

This security scheme might for example combine Forward Error Correction (FEC) codes (for reliability and secrecy) with beamforming and/or artificial noise (to control radio propagation conditions).

5.1.3.12.2 Solution details

The solution assumes that an authenticated radio link has been established between the UE and the network.

This security scheme is based on secrecy codes that are FEC codes augmented with security capabilities. They are able to provide high reliability to legitimate users but are also able to confuse any eavesdropper by encoding the exchanged messages in the controlled radio advantage.

Editor's note: security properties of the solution should be described

Editor's note: the threat model should be detailed

This radio advantage can be achieved by:

Lenovo Ex. 1007
Page 89

beamforming of data towards the legitimate receiver,

combining beamforming with the emission of interfering signals (artificial noise) elsewhere.

The artificial noise power is controlled and the user signal is steered to both optimize the decoding capability for legitimate receivers while decreasing it for eavesdroppers.

As a result, a simplified implementation of the proposed scheme consists in:

artificial noise and beamforming from Channel State Information measured on the legitimate link,

FEC codes defined in 3GPP standards to provide high reliability,

nested polar or Reed Muller codes designed to achieve confidentiality without encryption.

Editor's note: the solution needs to be described with more details

5.1.3.12.3 Evaluation

TBA

5.1.4.13 Solution #1.13: Security of NAS signallings before security activation

5.1.4.13.1 Introduction

The solution addresses the key issue #1.5 Integrity protection for the control plane between UE and network.

The first attach/TAU request is sent before NAS security activation, and it is easy to be modified by man-in-middle-attack, which may lead to "bidding-down" attack or "DoS" attack. The solution in clause 5.1.4.13.2.1 will detect whether there is any modification.

The downlink messages in some error cases, such as Attach reject, TAU reject, Identity request message, etc., can also be sent before NAS security activation, and they are easy to be tampered with, forged and replayed by an attacker. A forged or replayed Attach/TAU reject message may lead UE into a "no-service" state, which is a form of DoS attack to the UE. And, a tampered Attach/TAU request message, may trigger network to send an Identity request message to retrieve UE's IMSI, and the attacker in the middle can get the IMSI in Identity response sent by UE if it is not protected. The solution in clause 5.1.4.13.2.2 will address these problems.

5.1.4.13.2 Solution details

5.1.4.13.2.1 Protection of the uplink message

The solution is similar to the solution in clause 7.2.4.4 of TS 33.401 [31].

The core network calculates a hash value of the attach/TAU request when it receives an unprotected attach/TAU request. The calculated hash value is sent back to the UE in NAS SMC message which is integrity protected (but not ciphered). The UE also calculates a hash value. The UE can check whether the attach/TAU request is modified or not by comparing its calculated hash value with the received hash value. If two hash values are different, the UE will resend the attach/TAU request in NAS Security Mode Complete message which is integrity protected, and the core network will complete the on-going attach/TAU procedure.

5.1.4.13.2.2 Protection of the downlink message

It is assumed that, for this solution, AMF is provisioned asymmetric cryptography parameter, and has the capability to generate signature based on the asymmetric algorithm. It is also assumed that UE have capability to validate the signature. The example of crypto to be used could be public/private key pair based on RSA/ECC (Solution #2.12), certificate in PKI (rf. Solution #4.1 or #7.2), and ID, SSK, PVT in IBC (rf. Solution #2.14).

In the solution, the response message is mainly protected by a signature with fresh value NONCE1 and NONCE2, which protects the message from being tampered with, forged or replayed by an attacker. However, the protection alone is not enough as there is an attack scenario that an attacker acting as man-in-the-middle could modify the GUTI in request message into an unknown identity for AMF so that AMF will respond the Identity Request message to UE.

Lenovo Ex. 1007
Page 90

Since the Identity Request message is signed by the AMF legally, UE will return its IMSI to AMF, which may be eavesdropped by the attacker. So, a hash value of request message is needed in the response message. It is used for protecting the Attach/TAU request message from being tampered with by the attacker.

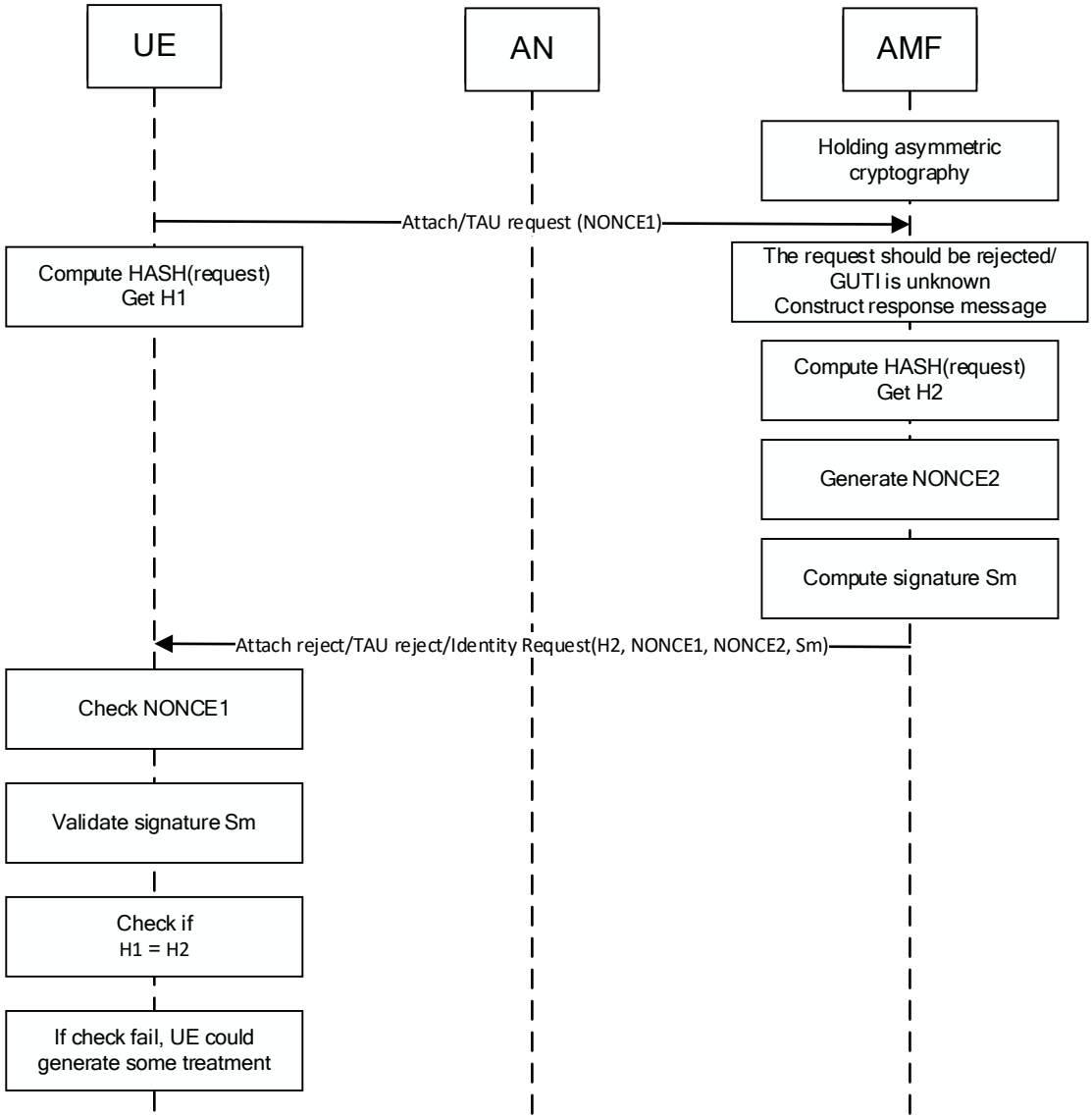


Figure 5.1.4.13.2.2-1 call flow for downlink NAS signalling protection

Editor's Note: the feasibility of an approach requiring all serving networks to have public/private key pair needs to be demonstrated, and details of the required global PKI need to be elaborated. The roaming scenario needs to be addressed.

1. UE sends Attach/TAU Request message to AMF including NONCE1 generated randomly by UE. Meanwhile, UE computes a hash value H1 of the request message. UE will store NONCE1 and H1 for a while.

2. AMF receives Attach/TAU Request message, and may respond to the abnormal message due to some reasons, e.g. EPS services not allowed, etc. Or when UE is unknown in AMF, the AMF will request UE to return the IMSI. So, AMF will construct original Attach reject/TAU reject/Identity request message.

3. AMF also computes a hash value H2 for received Attach/TAU Request message.

4. AMF generates NONCE2 randomly, and calculates signature of Attach reject/TAU reject/Identity request message including H2, NONCE1 and NONCE2 using private key of AMF.

Lenovo Ex. 1007
Page 91

5. AMF sends Attach reject/TAU reject/Identity request message including H2, NONCE1, NONCE2, and signature.

6. UE receives the message, and extracts H2, NONCE1, NONCE2, and Sm. UE checks NONCE1 whether it is the same as what it sends. And UE validates the signature Sm using public key of AMF. UE checks whether H1 equals H2.

7. If any check fails in step 6, UE will know it is being attacked, and will generate some treatment, e.g. ignore the message, and re-select a RAN to access the network again.

5.1.4.13.3 Evaluation

tba

5.1.4.14 Solution #1.14: Single termination point for NAS security

5.1.4.14.1 Introduction

The present solution addresses key issues 1.5 " Integrity protection for the control plane between UE and network" and 1.6 "Confidentiality protection for the control plane between UE and network".

The present solution specifically addresses signalling between the UE and the NG core over the NG1 interface. Different types of signalling are carried over NG1, e.g. Mobility Management (MM) signalling and Session Management (SM) signalling.

Editor's note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the security area.

5.1.4.14.2 Solution details

For the present solution, there is one termination point in the NG core (called 'NAS security termination' henceforth) for confidentiality and integrity protection of signalling messages sent over NG1. This means that the same confidentiality and integrity protection mechanisms are applied irrespective of the type of signalling, e.g. MM or SM.

When a signalling messages is received in the NG core from the UE over NG1 it is first routed to the NAS security termination for integrity-checking and (potential) decryption. It is then routed further to the entity that processes the corresponding type of signalling, e.g. SM or MM entity.

When a signalling messages is to be sent from the NG core to the UE over NG1 it is routed by the entity that processes the corresponding type of signalling, e.g. SM or MM entity, to the NAS security termination for adding the integrity-check value and (potential) encryption. It is then sent out to the UE over NG1.

The UE-specific security context available in the NAS security termination is (as is always the case with security contexts) tied to a particular user identity, called ID_NAS (only for the purposes of describing the present solution).

5.1.4.14.3 Evaluation

Whether this solution should be selected depends, to a large degree, on efficiency and complexity considerations.

Editor's note: Efficiency and complexity considerations are to be decided by SA2.

However, there are several security aspects to be taken into account:

Secure location:

The NAS security termination shall reside in a secure environment in an operator's network, which is not exposed to unauthorized physical access.

Lenovo Ex. 1007
Page 92

Inter-layer address spoofing:

TR 23.799 v080, clause 6.12.1.1.3, contains the following Editor's Note: "*Whether a single user identity or multiple user identities are needed for the various functionalities (e.g. MM, SM, etc.) is FFS, depends on the solutions for such functionalities, and requires SA3 input*."

This raises the prospect of having an ID_MM, an ID_SM etc., different from ID_NAS, and the entity that processes the corresponding type of signalling, e.g. SM or MM entity, would act only upon the identity ID_MM or ID_SM etc. If now the NAS security termination checked the NAS message origin authentication based on a different identity, namely ID_NAS, there would be the possibility for a UE to use the correct ID_NAS while spoofing the ID_MM or ID_SM. It is therefore a security requirement for this solution to work that such inter-layer address spoofing is prevented. It is envisaged that this could easily achieved in at least one of the two following ways:

- using a single identifier for ID_NAS, ID_MM and ID_SM;
- using a master identifier, e.g. IMSI or ID_NAS, to which all the other identifiers are securely tied. In this case, the NAS security termination has to communicate the verified master identifier to the signalling entities that process ID_MM or ID_SM for comparison.

Privacy:

If there was no single NAS security termination then the unencrypted part of a signalling message would have to contain parameters that would allow routing to the correct NAS entity, e.g. SM entity in a network slice. This information about the slice may give away information on the services used. However, user identity privacy should prevent that an eavesdropper can associate a particular signalling message with a particular subscriber.

Editor's Note: The above paragraph has been included for completeness. It is ffs whether leaving parameters unencrypted that are required for NAS-internal routing would endanger privacy.

Editor's Note: Additional security aspects are ffs: e.g. the case MM and SM are in separate domains and the case of moving UEs.

Editor's Note: Slice security isolation with this solution is ffs.

5.1.4.15 Solution #1.15: AES as a fast stream cipher

5.1.4.15.1 Introduction

This solution addresses the requirement in 5.1.3.13.3 that "for some services it shall be possible to encrypt the user-plane with a very fast stream cipher".

5.1.4.15.2 Solution details

Using AES in counter mode may be sufficient, given availability of dedicated hardware to execute AES operations quickly. Key and IV set-up (and initial keystream generation) could also be done pre-emptively in hardware to ensure ciphering can start immediately.

5.1.4.15.3 Evaluation

This solution meets the requirement provided the hardware implementation is fast enough to meet the aggressive latency targets (< 1ms). However, the costs of such a hardware implementation on low-end UEs must be considered. The choice of AES provides the greatest chance of a commodity hardware implementation.

5.1.4.16 Solution #1.16: Re-use of "Data efficient re-keying"

5.1.4.16.1 Introduction

This solution addresses the requirement in 5.1.3.13.3 that "It shall be possible to adequately authenticate subscriptions even if there is very low control-plane latency, without exposing sensitive assets (such as a long term authentication secret key) at the network edge."

Lenovo Ex. 1007
Page 93

5.1.4.16.2 Solution details

If low latency is required on the signalling plane, **then** the solution of "data efficient re-keying" discussed in TR 33.860 (Annex B2) could also allow for *low latency* re-keying of a security association, based on an intermediate key K_{med} held by both the visited network and the UE (e.g. within the UICC or other secure component).

5.1.4.16.3 Evaluation

This solution allows for reduced control plane latency (< 10ms) provided the intermediate key has already been derived and held by the visited network. There will still be sporadic longer latency in roaming scenarios to establish such a key (e.g. on first connection to the visited network) and there may be longer latency to update the K_{med}.

There may be security risks if the K_{med} lifetime is long (weeks or months); addressing these would require the K_{med} to be stored as securely by the visited network as the underlying K is stored in the HSS.

Editor's note: It is ffs whether the intermediate key Kmed could be the security anchor key held in the SEAF, cf. solution 1.2

The solution would still require a round-trip to the core of the visited network, so would be incompatible with ultra-low latencies (<1 ms). The visited network could try to replicate its own core security functions around the edge, but this is likely to be very expensive, and would compromise security, as there is much more risk of some of these functions being compromised.

5.1.4.17 Solution #1.17: Delegated Subscriber Server

5.1.4.17.1 Introduction

This solution addresses the requirement in 5.1.3.13.3 that "It shall be possible to adequately authenticate subscriptions even if there is very low control-plane latency, without exposing sensitive assets (such as a long term authentication secret key) at the network edge."

5.1.4.17.2 Solution details

A solution could be to delegate some of the functions of the HSS to the visited network. We might call it a Delegated Subscriber Server (DSS). There will be only one "real" HSS, but there could be multiple DSSs. Using the term "K" for the long term subscriber secret key:

- K remains only in the HSS.
- Each DSS needing to authenticate this subscriber receives a key K', derived from K in a one-way fashion. No DSS should be able to work out the actual Ki, nor the K' that's provided to any other DSS.
- The authentication and key agreement algorithm takes K' as input. The USIM (or its NextGen equivalent) also has the necessary information to derive K'.
- K' could be derived just once for any DSS, or could be refreshed periodically.

Editor's note: It is ffs whether the derived key K' could be the security anchor key held in the SEAF, cf. key issue 1.2, i.e. whether the DSS and SEAF roles could merge

5.1.4.17.3 Evaluation

This solution allows for reduced control plane latency (< 10ms) provided the derived key K' has already been derived and held by the visited network. There may be sporadic longer latency in roaming scenarios to establish such a key (e.g. on first connection to the visited network) and there may be longer latency to update the K'.

There are security disadvantages with this approach since it places authentication and related billing controls in the visited network, creating a risk (e.g. fraud) for the home operator. It is important to note that the home operator cannot control how securely long-term keys are stored in the visited network. There is also a need to standardize the authentication and key agreement algorithms used between the UE and the DSS.

The solution would still require a round-trip to the core of the visited network, so would be incompatible with ultra-low latencies (<1 ms). The visited network could try to replicate its own core security functions around the edge, but this is likely to be very expensive, and would compromise security, as there is much more risk of some of these functions being compromised.

Lenovo Ex. 1007
Page 94

5.1.4.18 Solution #1.18: Combining Low Latency on User Plane with High Latency on Control Plane.

5.1.4.18.1 Introduction

This solution addresses the requirement in 5.1.3.13.3 that "To support some critical services, such as remote surgery and industrial control, it shall be possible to provide integrity protection and replay protection for user plane even if very low latency is requested."

5.1.4.18.2 Solution details

The proposed solution combines low latency on the user plane with high latency on the signalling plane. User plane latency can be minimized by re-using the keys from an existing security association (SA). If that SA has expired, then in parallel to the user plane usage, the network will initiate AKA and acquire a new security association.

5.1.4.18.3 Evaluation

The solution provides some key material to be used by the UE immediately. However it would still impose a high latency at initial attachment to a network (before the first SA is established), and would require persistent caching of old SAs by both the UE and visited network, so weakening security to some extent (there is somewhat greater risk of an old key leaking and being abused). Further, if either the UE or visited network node has purged the old SA, the user plane will have to wait while a new SA is established. This may be unacceptable for some use cases.

5.1.4.19 Solution #1.19: Next Generation USIM

5.1.4.19.1 Introduction

The solution is to use a secure component which resides within and may not be removable from the UE. It executes both the legacy USIM functions inherited from previous standards (UMTS and LTE), and other functions required for NextGen UE security. It can be abbreviated as the "NextGen USIM".

This solution addresses several key issues, especially Key Issue #1.8 UEs with Asymmetric Keys; but also, based on meeting this, Key Issue #2.4: Equipment identifier authentication; Key issue #2.5: Non-AKA-based authentication; Key Issue #2.8: Authentication of the user; Key Issue #12.2: Remote credential provisioning for IoT devices; Key Issue #4.1: AS security during RRC idle mode; Key Issue #7.1: Subscription identifier privacy.

This solution also addresses Key issue 5.1 Secure storage and processing of credentials and identities.

5.1.4.19.2 Solution details

The solution uses a secure element as defined by ETSI SCP, but does not specify a physical form factor. This could be a UICC or a SSP (Smart Secure Platform). Only the logical interface to the NextGen USIM needs to be defined within 3GPP; the NextGen USIM resides on a platform defined by ETSI SCP within the scope of the ETSI work item on "Smart Secure Platform".

The core functionality and physical design of the NextGen USIM component shall permit robust security evaluation e.g. against a Common Criteria protection profile.

To provide support for multiple (and extendable) UE security functions, the NextGen USIM component will have access to secure storage and support a random number generator for generating new key material.

The interface to the NextGen USIM shall provide a trustworthy indication of which component of the device is communicating with the NextGen USIM to request use of any particular key or application (e.g. baseband, application processor, id/hash of requesting application). Specific solutions for detailed standardization may include reserving logical channels to various device components or by having separate sessions with separate "accounts" which are authenticated.

Editor's note : The security required to authenticate the components in the UE is FFS.

The NextGen USIM will have the functionality to generate new symmetric keys, using existing key material, and to encrypt and integrity-protect new keys using existing key material.

Lenovo Ex. 1007
Page 95

The NextGen USIM may have the functionality to generate new asymmetric key-pairs and integrity protect the public keys using existing key material. The NextGen USIM may also be able to install new trusted public keys, integrity protected using existing trusted key material.

Specific solutions for detailed standardization include:

i) Directly digitally signing a new public key using an existing trusted key

ii) Authenticating a DH key exchange using an existing trusted key, and then deriving new keys from the DH shared secret and existing trusted key, or using these derived keys to protect transmission of a new key. See also Solutions #2.1, #2.2 and #2.6.

iii) Integrity protection (and encryption) of new keys using an existing SIM OTA key

iv) Deriving new keys from a subscription key (K), based on GBA or GBA-U, or using these derived keys to protect transmission of a new key.

To provide for quantum-safety, the NextGen USIM should have a general capability to support lattice-based public key cryptography (which is considered by [54] to be the most-studied of quantum safe solutions) as detailed in Key issue #17.2: Quantum safe cryptography. The exact public key algorithm (or suite of algorithms) is for further standardization, but a general capability to update the lattice-based crypto-algorithms used should be supported by the NextGen USIM. For security reasons, basic lattice operation primitives might need to be implemented at production of the NextGen USIM (suitably-protected against side channel attacks), but the exact combination of operations used in a crypto-algorithm may be provided by a later remote update.

Editor's note: Details and solutions for initial provisioning of the NextGen USIM are detailed in security area #12.

5.1.4.19.3 Evaluation

This solution addresses several key issues, especially Key Issue #1.8 UEs with Asymmetric Keys; but also, based on meeting this, Key Issue #2.4: Equipment identifier authentication; Key issue #2.5: Non-AKA-based authentication; Key Issue #2.8: Authentication of the user; Key Issue #12.2: Remote credential provisioning for IoT devices; Key Issue #4.1: AS security during RRC idle mode; Key Issue #7.1: Subscription identifier privacy. This solution also addresses key issue 5.1 - Secure storage and processing of credentials and identities.

The trust issues identified in 5.2.8.3 are resolved by, for example, enabling a network operator to receive a new public key from the NextGen USIM integrity protected using an existing key that is already trusted by the operator (for example a subscription key or SIM OTA key). Or the operator will be able to provide the NextGen USIM with a new public key to verify network components, integrity protected using an existing operator key trusted by the NextGen USIM (for example a subscription key or SIM OTA key).

5.1.4.20 Solution 1.20: Flexible UP security termination point

5.1.4.20.1 Introduction

This solution addresses key issue 1.15 about flexible UP security termination by introducing a UP-STF that is tasked with terminating the User Plane Security.

5.1.4.20.2 Solution details

For security reasons it is desirable to terminate the UP security beyond the gNB. For reasons of flexibility it is desirable to be able to terminate the UP security at different points in the network depending on the service offered. For example: traffic with ultra-low latency requirements must be terminated in a location close to the UE, while other traffic from the same UE for other services needs protection through the whole backhaul. As such, it is proposed to define a specific function that is tasked with terminating the UP security. This newly introduced function is called the UP-STF. It is logically positioned between the gNB and the NG Core, or is collocated with a function in the NG Core depending on the service offered.

5.1.4.20.3 Evaluation

This solution straightforwardly addresses KI#1.15 by introducing a UP-STF that terminates the UP security.

Lenovo Ex. 1007
Page 96

5.1.4.21 Solution 1.21: Flexible UP security termination point

5.1.4.21.1 Introduction

This solution addresses key issue 1.15 about flexible UP security termination by introducing a UP-STF that is tasked with terminating the User Plane Security.

5.1.4.21.2 Solution details

The proposed solution is based on the assumption that the UP Security should be handled by a dedicated extra-layer named for convenience UP-L.

The UP-L should manage all the UP security functions including UP security negotiation (keys, algorithms and so on), security algorithms agreed for user traffic confidentiality and integrity.

At UE-side, the UE should implement the UP-L on the top of PDCP layer in the radio protocol stack in order to guarantee its indipendence.

At the network side, the UP-L should be implemented in the UP-STF. In order to properly cover all scenarios, the UP-STF should be implemented both by RAN and UPF. In particular the UP-L should be on the top of:

– PDCP layer in the 5G RAN Radio protocol stack

– GTP layer in the UPF N3 protocol stack

This solution assumes that the UP-STF is not contemporary enabled in the RAN and in the UPF. The enabling of the UP-STF on the RAN or on the UPF is based on configuration options during the deloyment phase.

When UP-STF is enabled in the UPF, no other security over the air (e.g. no additional encription is required by the RAN) is required. In this case RAN will have all the elements to divert the traffic accordingly, since only the UP traffic will be encrypted and all the other headers provided by the lowest stack layer are in clear text.

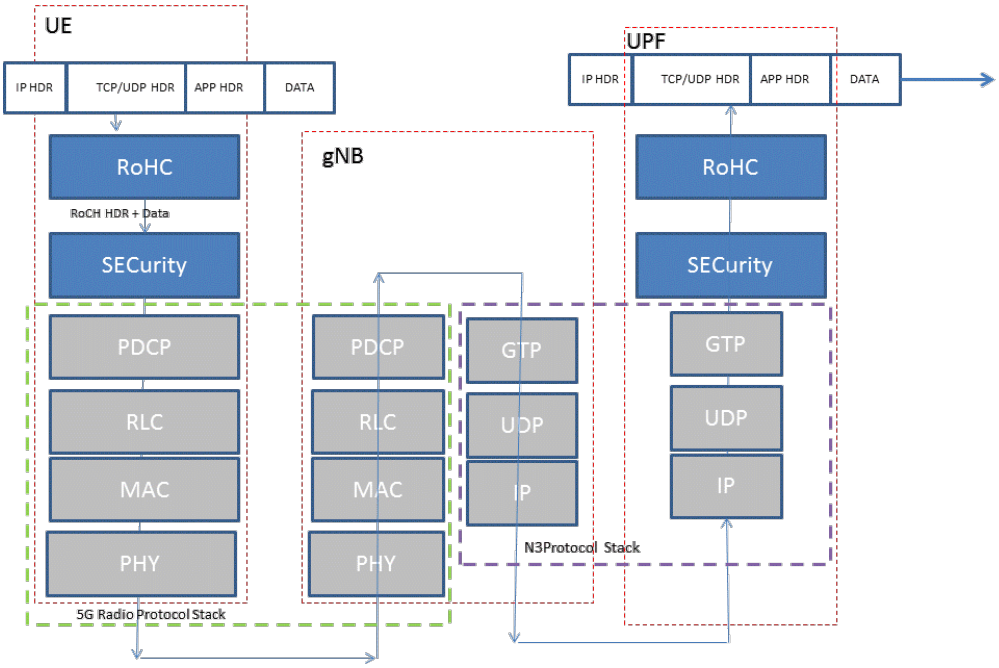


Figure 5.1.4.21.2-1: NETWORK CONFIGURATION ENABLING THE UP-STF in the UPF.

Lenovo Ex. 1007
Page 97

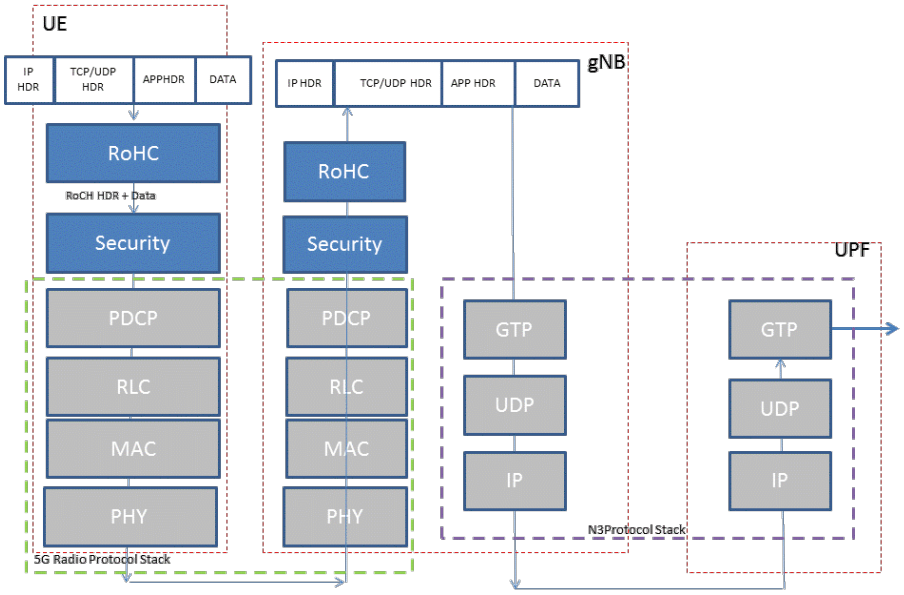


Figure 5.1.4.21.2-2: NETWORK CONFIGURATION ENABLING THE UP-STF in the RAN.

For the UE the termination of the UP Security is intended to be totally transparent.

The AMF/SMF should deliver to the UP-STF the proper Key for deriving the UP Security Keys using the control plane signalling interface. For this reason, the UP-STF needs to register towards the AMF/SMF.

The UP Security Keys negotiation should occur when the UP is set up (i.e. contextually to a DNN request).

5.1.4.21.3 Evaluation

This solution straightforwardly addresses KI#1.15 by introducing a UP-STF that terminates the UP security. It is also aligned with the 5G system architecture agreed in TS 23.501 and is able to address the potential security requirements listed in clause 5.1.3.15.3.

The main advantages of this solution are:

- Flexibility of UP-STF location based on static configuration options.
- Untrusted RAN deployments (e.g. scenario #2) can be made secure natively without the usage of VPN protocols like IPSec.
- UP security is ensured without the need to use over-the-top security solutions.
- To avoid the need to use additional network elements like SEGs.

The main drawback is that the UP-STF needs to be implemented in two different Network Elements (i.e. gNB and UPF).

5.1.4.22 Solution #1.22: Terminating user plane security in the AN

5.1.4.22.1 Introduction

This solution addresses key issue 1.15 "Termination point of UP security".

This solution proposes terminating security over the air interface in the access network. A main feature of the solution is the possibility to place the security termination point in a central unit of the gNB that may be assumed to reside in a secure location.

Lenovo Ex. 1007
Page 98

5.1.4.22.2 Solution details

Split of protocol stack over the 5G NR radio interface

The virtualization of RAN entities ("RAN cloud") offers the possibility to consider a protocol stack split, but without the risk of centralized units becoming a bottleneck.

One of the deployment scenarios for the RAN architecture described in TR 38.801 [72] (clause 5.4) supports the centralization of the upper layers of the NR radio stacks as illustrated by Figure 5.1.4.22.2-1. In relation to this, all the agreed options for the functional split between the central and the distributed units do place both the RRC and PDCP layers in the central unit. In addition, the RAN architecture will support the non-centralized deployment scenario where the full protocol stack is supported at the gNB (clause 5.2 of TR 38.801 [72]) with no protocol stack split at all.

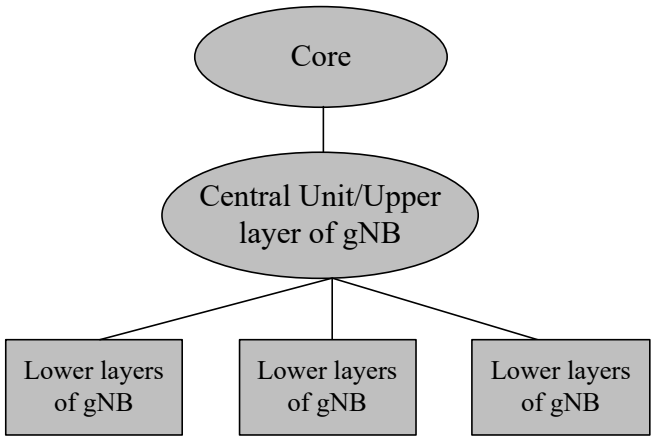


Figure 5.1.4.22.2-1: Centralized deployment (from TR 38.801)

In LTE, radio interface security is provided by the PDCP layer, both for the control and user planes. Assuming that security can be also provided in the PDCP layer for 5G NR, the functional split between central and distributed unit that is described in TR 38.801 [72] allows to terminate security where PDCP terminates, i.e. the central unit. And this central unit could be assumed to reside in a secure location.

Solution 22.1

For this solution, it is assumed that there is no protocol stack split of the gNB. In particular, there is no central unit where security could terminate.

For this case, the solution is largely identical to the one in LTE, i.e. security terminates in a PDCP layer in a monolithic gNB. The same platform security requirements as for the eNB in LTE would apply. Backhaul link protection is needed on N3, cf. solution 1.23.

Solution 22.2

For this solution, it is assumed that there is a protocol stack split of the gNB, and the PDCP layer resides in the central unit of the gNB. User plane security terminates in this central unit. This unit may be assumed to reside in a secure location so that no dedicated platform security requirements would be required. As the central unit may be assumed to reside in a RAN cloud, backhaul link protection may be provided in two ways (cf. solution 1.23):

- In the same way as for LTE, cf. TS 33.401 [31], clause 12.
- Realizing backhaul link security between the central unit and the 5G core by using generic protection mechanisms of the virtualized infrastructure.

5.1.4.22.3 Evaluation

One of the main objections against terminating security in the access network, namely that the security endpoint would reside in an exposed location, could be considered addressed when placing the security termination in the central unit of a gNB. For deployment scenarios of gNBs with no central unit, the platform security requirements from TS 33.401 [31] and TS 33.102 [73] would still apply to gNBs. But the deployment model would be an operator's choice.

Lenovo Ex. 1007
Page 99

The complexities of dedicated backhaul link security in the way of TS 33.310 [37] could be avoided when terminating UP security in a central unit.

The constraints posed by Header compression and the application of policies based on packet headers can be fulfilled as the IP headers remain unencrypted.

It is possible to provide the same protection mechanism for all types of PDU payloads, i.e. IP packets, non-IP PDUs and Ethernet frames.

The need for an additional user plane security gateway is avoided (cf. solution 1.23).

If UP integrity is applied and terminated in the AN, false traffic can be stopped already in AN

5.1.4.23 Solution #1.23: Security for the AN-CN User Plane

5.1.4.23.1 Introduction

This solution addresses key issue 1.10 "Security features for AN-CN User Plane". The AN-CN User Plane is realized by the N3 interface defined in TS 23.501 [74]. The analogue of the AN-CN User Plane in LTE is the S1-U interface, also referred to as the backhaul user plane link.

5.1.4.23.2 Solution details

Two solution variants apply, depending on the user plane security termination point and the AN architecture.

Solution 1.23.1:

Here, the user plane security termination point is assumed to reside in the AN. As explained for solution 1.24.1 "Security for the AN-CN Control Plane", in the centralized deployment scenario supported in the RAN architecture, the protocol stack of the gNB is split into a central unit (CU) and distributed units (DUs). This is further described in clause 5.4 of TR 38.801 [72]. The proposed solutions are also similar to solution 1.24.1 "Security for the AN-CN Control Plane".

Two cases need to be considered:

- The user plane security termination point resides in the distributed unit.
    - The solution proposed here for this case is a copy of the solution for LTE, i.e. use of IPsec as described in TS 33.401 [31], clause 12.
- The user plane security termination point resides in the central unit. Then two solution variants are possible:
    - The solution proposed here for this case is a copy of the solution for LTE, i.e. use of IPsec as described in TS 33.401 [31], clause 12.
    - A CU could (or would even be likely to) be realized in a RAN cloud; this would open the possibility to realize backhaul link security between this central unit and the 5G core by using generic protection mechanisms of the virtualized infrastructure.

Editor's Note: the term "generic protection mechanisms of the virtualized infrastructure" needs clarification.

Solution 1.23.2:

Here, the user plane security termination point is assumed to reside in the CN.

Then one can deploy the same solution as for LTE, i.e. use of IPsec as described in TS 33.401 [31], clause 12.

But this solution is not necessarily required for this case: again, two subcases need to be considered:

- The user plane security termination point resides at the edge of the CN.
  In this subcase, no additional protection on N3 may be needed.
- The user plane security termination point resides in UPFs distributed across the core network, e.g. UPFs in separate slices in the serving network, or even UPFs in the home network.

Lenovo Ex. 1007
Page 100

In this subcase, an additional user plane security gateway (UP Sec GW) may be required, similar to the ones deployed on other entry points to the operator network from the Internet. This is so because

- physical protection of N3 may not be considered sufficient, e.g. because N3 may be carried over the Internet;
- the operator wants to be able to block rogue traffic at the edge of the core network, and not let it reach distributed entities in the core network;
- the operator may consider it advantageous to provide and maintain the firewalling properties required for blocking external rogue traffic in central places at the edge of the core network rather than in many distributed places, e.g. because keeping the hardening measures up-to-date is more easily achieved in a central place.

5.1.4.23.3 Evaluation

For the evaluation of solution 1.23.1, we refer to that of solution 1.24.1 for the backhaul link control plane.

Solution 1.23.2: The consequence of this solution is that either UP security between UE and core network is terminated somewhere at the edge of the CN or else, a user plane security gateway may be required. But such a UP security termination point at the edge, or a user plane security gateway show much similarities to the subcase of solution 1.23.1 where UP security is terminated in a central unit of the gNB. After all, it does not matter very much whether the entity protecting the access to the core is considered part of the AN (but close to the core) or part of the CN (but close to the AN).

5.1.4.24 Solution #1.24: Security for the AN-CN Control Plane

5.1.4.24.1 Introduction

This solution addresses key issue 1.9 "Security features for AN-CN Control Plane". The AN-CN Control Plane is realized by the N2 interface defined in TS 23.501 [74]. The analogue of the AN-CN Control Plane in LTE is the S1-MME interface, also referred to as the backhaul signalling link.

5.1.4.24.2 Solution details

Two solution variants apply, depending on the AN architecture.

The RAN architecture will support several deployment scenarios as described in TR 38.801 [72] clause 5. In the centralized deployment (clause 5.4), the gNB protocol stack is split into a central unit (CU) and distributed units (DUs) as depicted in the following figure:

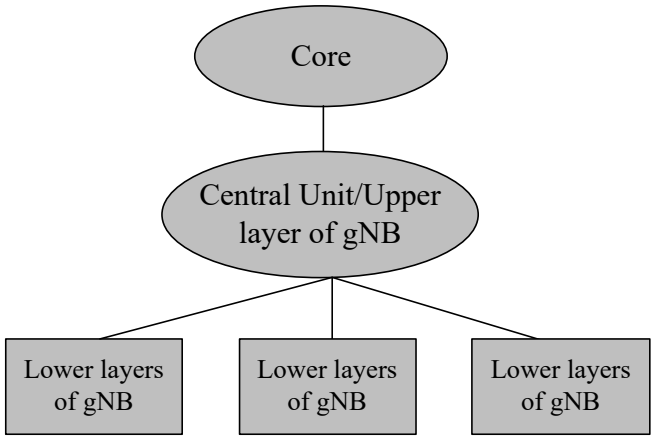


Figure 5.1.4.24.2-1: Centralized deployment scenario from TR 38.801

In the non-centralized deployment (clause 5.2) there is no protocol stack split at all.

Lenovo Ex. 1007
Page 101

For security purposes, it only matters whether the RRC layer extends between the UE and the CU or the UE and the DU as, from a security point of view, the main purpose of the N2 interface is the provisioning of keys and other security parameters to protect the RRC layer.

Variant 1: RRC layer extends between the UE and the gNB in case of no protocol stack split.

Then also the layer providing confidentiality and integrity for the RRC layer (which is PDCP in LTE and, possibly, again in 5G) must reside in the(distributed) gNB. This means that backhaul link signalling protection must extend between the gNB and the 5G core.

- *Solution 1.24.1*: The solution proposed here for this case is a copy of the solution for LTE, i.e. use of IPsec as described in TS 33.401 [31], clause 11.

Variant 2: RRC layer extends between the UE and the CU

Then PDCP also resides in the CU, according to the decisions made in RAN. PDCP is the layer providing confidentiality and integrity for the RRC layer in LTE and, most likely, again in 5G.

This then allows two subvariants for the backhaul signalling protection:

- *Solution 1.24.2.1:* The solution proposed here for this case is a copy of the solution for LTE, i.e. use of IPsec as described in TS 33.401 [31], clause 11.
- *Solution 1.24.2.2:* A CU could (or would even be likely to) be realized in a RAN cloud; this would open the possibility to realize backhaul link security between this central unit and the 5G core by using generic protection mechanisms of the virtualized infrastructure.

Editor's Note: the term "generic protection mechanisms of the virtualized infrastructure" needs clarification.

5.1.4.24.3 Evaluation

When an operator has a deployment where RRC extends between the UE and distributed units at least for some of the gNBs, and the operator believes that physical security of the backhaul link is not enough, then, per the above solution 1.24.1, the operator needs to deploy IPsec.

- **Conclusion**: For distributed RRC security, the operator cannot avoid IPsec-based backhaul link security, which includes the complexities of the certificate management as specified in TS 33.310 [37]. This is true irrespective of the user plane security solution.

When an operator has a deployment where RRC extends only between the UE and central units for all the gNBs, and the operator believes that physical security of the backhaul link is not enough, then, per the above solution 1.24.2.2, the operator has an alternative to deploying IPsec, namely using generic security mechanisms of the virtualized infrastructure.

Editor's Note: the term "generic protection mechanisms of the virtualized infrastructure" needs clarification.

- **Conclusion**: For centralized RRC security, the operator has an alternative to IPsec-based backhaul link security.

5.1.4.25 Solution #1.25: Protocol stack options for the user-plane security terminating at the UPF

5.1.4.25.1 Introduction

This solution proposes protocol stack options for the user-plane security terminating at a user-plane function (UPF) in the NextGen systems as a solution for the key issue #1.15: Termination point of UP security.

5.1.4.25.2 Solution details

For the user-plane security terminating at the UPF, the UPF is provisioned with a key shared with the NG-UE (i.e., K_{UPF}) and security configuration information (e.g., ciphering and integrity protection algorithms, key identifier, key lifetime) by the SMF. When the user-plane security is configured at the UPF, the corresponding counter is initialized (e.g., to zero).

Lenovo Ex. 1007
Page 102

NOTE 1: UP security is configured in a bearer basis. More generally, per-bearer security configuration can be allowed in 5G.

Option 1:

The user-plane (UP) security is implemented right above the PDCP layer. The UP security requires a new security header that includes at least a counter and a key id. If ciphering is turned on, the SDU received from the upper-layer (excluding the UP security header) is encrypted based on the ciphering algorithm. If integrity protection is turned on, the SDU received from the upper-layer and the UP security header are integrity protected based on the integrity protection algorithm.

In this option, the UP security can be implemented regardless of the upper layer protocol, i.e., IP or non-IP.

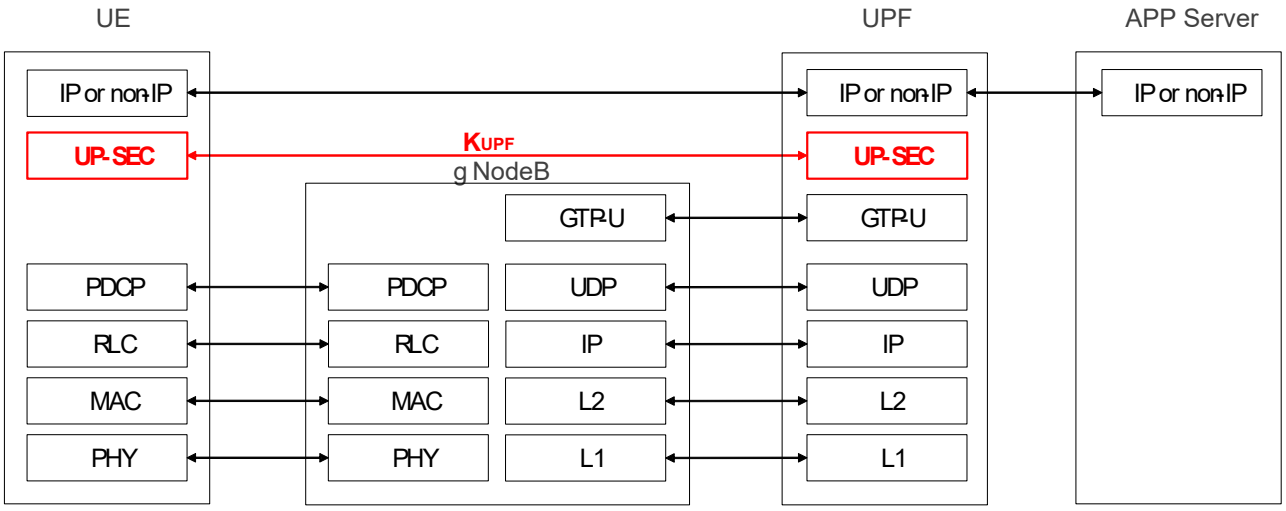
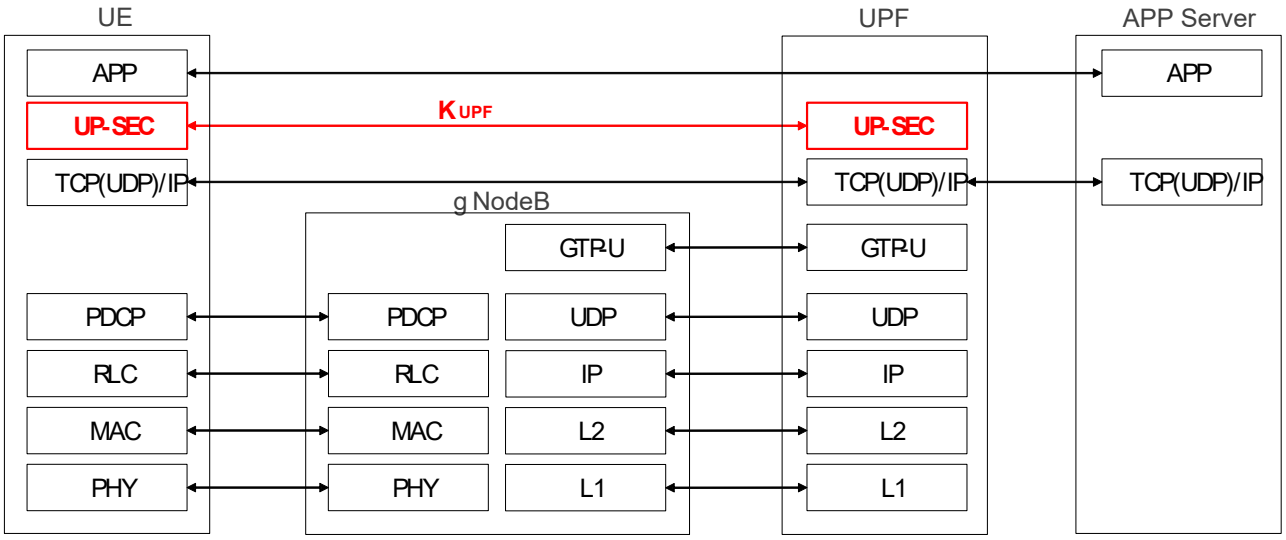


Figure 5.1.4.25.2-1. User-plane security protocol stack option 1 – security header above the PDCP

Option 2:

The user-plane (UP) security is implemented above the TCP(UDP)/IP layer. The UP security header is placed right above the transport header (e.g., TCP/UDP). If ciphering is turned on, the application payload is identified (excluding the transport and IP header) and encrypted based on the ciphering algorithm. If integrity protection is turned on, the application payload is identified (excluding the transport and IP header) and the UP security header are integrity protected based on the integrity protection algorithm. In case of UL transfer, the UPF processes the UP security (e.g., decrypts the packet or verifies the integrity of the packet) based on the UP security header and removes the UP security header before further forwarding the packet to the next hop. In case of DL transfer, the 5G-UE processes the UP security (e.g., decrypts the packet or verifies integrity of the packet) based on the UP security header and removes the UP security header before further forwarding the packet to the upper-layer.



Lenovo Ex. 1007
Page 103

Figure 5.1.4.25.2-2. User-plane security protocol stack option 2 – security header above the TCP(UDP)/IP

5.1.4.25.3 Evaluation

Option 1: If the security header is located right above the PDCP header, the UP security can be employed regardless of the upper-layer protocol. In other words, the upper-layer can be either an IP or a non-IP SDU. In this case, the RAN node (i.e., gNB) should have a routing information for the PDU associated to the NG-UE, which is established during the PDU session setup. Based on the routing information, the PDU from the NG-UE is transported to the UPF using a GTP-U.

If the UP security is configured between the NG-UE and the UPF, the RAN node cannot employ the ROHC for the data carried beteween the NG-UE and that UPF. In practice, the ROHC is configured for the VoIP traffic, hence the UP security associated with the VoIP traffic may well terminate at the RAN as in LTE and for such bearers, the UPF security may not be used. Similar treatment can be applied for other data that use ROHC at the RAN.

In case that there is a clear benefit of ROHC, alternatively, for bearers that are configured to use UPF security, ROHC can be implemented at the UPF.

Option 2: If the security header is located above the TCP(UDP)/IP layer (or above the RTP), the VoIP traffic can still make use of ROHC, thereby taking the advantage of low bandwidth and wider cell coverage. This is a distinct advantage of the option 2 over the option 1. Futhermore, this option enables a packet inspection at the RAN node (though limited to the transport header and IP header) if needed.

However, the option 2 requiers more packet processing at the NG-UE and RAN node, e.g., locating the payload to which security (e.g., encryption, integrity protection) is applied, decomposing the original PDU by squeezing in/taking off the security header between the TCP(UDP)/IP header and the payload. This packet processing incurs substantial performance penalty especially on the high-rate traffic. Furthermore, the option 2 does not work for non-IP PDUs.

5.1.4.26 Solution #1.26: Untrusted non-3GPP access

Editor's Note: The acronym ‘NG-PDG’ needs to be changed to ‘N3IWF’ to align with SA2.

5.1.4.26.1 Introduction

This solution addresses key issue #3.9 on "Untrusted non-3GPP access". It also relates to key issue #2.1 "Authentication framework".

5.1.4.26.2 Solution details

Architectural aspects:

The key issue states. "... an additional layer of security on top of whatever security is provided in the access network is required. This additional layer needs to extend between the UE and an entity considered trusted by the core network. "

We name this entity Non 3GPP Interworking Function (N3IWF).

The N3IWFhas the following interfaces:

- The N3IWF exchanges IP packets with the UE across the untrusted access network.
- The N3IWF exchanges signalling messages over IP with one or more control plane functions in the NG core. For simplicity, for the purposes of the present solution we subsume these control plane functions under the name Core Control Function (CCF). The CCF, in general, includes Mobility Management Function (MMF), Session Management Function (SMF), Security Anchor Function (SEAF), and Security Context Management Function (SCMF).

Editor's Note: This solution does not take a stance on whether reference points should be defined between the various functions subsumed under CCF. This is for SA2 to decide.

- The N3IWFexchanges user data over IP with user plane function UPF in the NG core.

Editor's Note: it is ffs whether N3IWFis located in serving network or home network or both.

Lenovo Ex. 1007
Page 104

Protocol aspects:

- The additional layer of security between UE and N3IWF is provided by IPsec.
- IKEv2 is used to establish IPsec security associations between UE (IKEv2 initiator) and N3IWF (IKEv2 responder).
- UE authentication is achieved using IKEv2 procedures using either a valid anchor key available at the SEAF or EAP methods.

NOTE1: The concepts of security anchor and anchor key are discussed in security areas #1 and #2 in various places. An anchor key is the intermediate key received by the SEAF from AUSF as a result of the NG-UE authentication process. This anchor key could have resulted from a prior access of the NG-UE to the 5G core using any access network. It could even result from the run of a different authentication method (e.g. EAP-AKA used with IKEv2 over non-3GPP access, and EAP-AKA' or EPS AKA used over NR 3GPP access).

NOTE2: The use of a key derived from a valid anchor key for IKEv2 authentication detailed below is an optimization that avoids the need for full EAP authentication.

Editor's Note: IKEv2 requires the use of certificates on the responder side to mitigate the so-called lying NAS (Network Access Server) problem. (This problem is better known in 3GPP as serving/access network impersonation). It is ffs whether an appropriate use of EAP-AKA' , together with IKEv2, could obviate the need for responder certificates as EAP-AKA' already provides access network authentication.

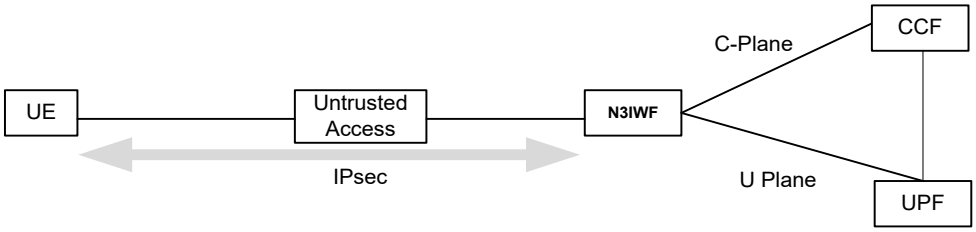


Figure 5.1.4.26-1:

Procedural aspects:

- The UE establishes IP connectivity with the access network. How this is done is not within 3GPP remit.
- The UE determines that the access network is untrusted.

NOTE3: Rules for such a determination can be found in TSs 33.402 and 23.402.

- The UE initiates IKEv2 with the N3IWF.

Editor's Note: It is ffs which parameters the UE should include in various IKEv2 messages (e.g. configuration payload to obtain IP addresses). This will also be determined by needs expressed by SA2 and CT1.

- UE sends the IKE_AUTH request to the N3IWF by including Identity of the UE in the IDi payload. The Identity, formatted as an NAI, includes either a UE temporary identifier that points to a valid anchor key at the SEAF (in which case the AUTH payload is included and is generated using a key K_NG-PDG derived from the anchor key) or an UE identifier that resolves to the permanent subscription identifier at the AUSF (in which case the AUTH payload is not included). The realm part of the identifier is used by the N3IWF for routing to the SEAF in the CCF. Furthermore, it is also assumed that the UE identifier includes information to identify the authentication method (e.g., similar to the way NAIs are formatted for non-3GPP access in clause 19.3 of TS 23.003).
- The key K_NG-PDG is derived from the anchor key either at the time of initial EAP authentication via the NG-PDG or from the anchor key that is available from a previous full authentication that is performed over a different access network, by using at least the NG-PDG identity as input for the key derivation. The SEAF sends K_NG-PDG to the NG-PDG in an Auth Response (Identifier, K_NG-PDG) message, together with EAP

Lenovo Ex. 1007
Page 105

Success message if EAP authentication was performed. The NG-PDG may store the K_NG-PDG along with the UE identifier for further use in IKEv2 re-authentications.

- The N3IWF sends an Auth Request (Identifier, Indication of whether AUTH payload included) message to the SEAF part of the CCF.

Editor's Note: The above bullet expresses the security needs. In the interest of an access-agnostic mobility management framework, this initial message sent from the NG-PDG to the CCF could take the form of a generic Attach request. This is, however, for SA2 to decide.

- If a valid anchor key is available at the SEAF and can be used, the SEAF decides whether a full EAP authentication run is required or not. If not, the SEAF derives a K_NG-PDG key and sends it in a Auth Response message to the N3IWF and the N3IWF uses the K_NG-PDG as a preshared key for the verification of the AUTH payload and establishment of IPsec security association between the UE and N3IWF. If AUTH verification fails, the IKE_AUTH procedure is rejected and the UE may retry IKEv2 authentication without including the AUTH payload in the IKE_AUTH message. Otherwise,
    - if the SEAF has determined that a new EAP authentication is required, the SEAF maps the received UE temporary identifier to a UE identifier that the AUSF can resolve and sends the EAP Identity Response message to the AUSF.
    - if the SEAF cannot find an anchor key related to the received UE temporary identifier the SEAF sends an error message to the NG-PDG, and the NG-PDG indicates a failure to the NG-UE. The NG-UE may then retry IKEv2 authentication without including the AUTH payload in the IKE_AUTH message.

NOTE4: In IKEv2, the omission of AUTH payload by the initiator is used as an indication to the responder to start the EAP authentication. In this solution, the decision of whether to start EAP authentication is left to the SEAF rather than the IKEv2 responder.

- Based on the received UE identity, the AUSF determines the EAP method to be used and initiates EAP method specific message exchanges (including, if required, EAP-method specific Identity request/response exchange) with the UE with the SEAF performing the functions of a 3GPP AAA proxy, as defined in TS 23.402, as far as proxying EAP messages between N3IWF and AUSF (which takes the role of EAP server) is concerned.
- At the end of the EAP authentication process, the SEAF sends (possibly via another function in the CCF) the EAP Success message and a key to the N3IWF.
- The N3IWF uses this key to complete the authentication of the UE within IKEv2.
- The UE and the N3IWF complete the establishment of an IPsec security association.
- IP packets protected between the UE and the N3IWF can now be exchanged between the UE and the NG core. These include user plane packets as well as NAS messages sent over IP.

Editor's Note: It is ffs by SA2 whether any further NAS messages need to be sent.

Editor's Note: It is ffs whether there are security implications of IP address assignment. IP address assignment as such is within the remit of SA2 and CT1.

Security context management aspects:

- The role of the anchor key, from which further keys are derived, is explained in NOTE1 above.
- The SEAF takes an active role in key delivery as explained in the procedural aspects above.

NOTE5: For the purposes of IKEv2 between UE and N3IWF, the derived key takes the role of either preshared key for IKEv2 UE authentication or of that MSK takes in 33.402, clause 8.

- With the procedure described above, an anchor key can be used over multiple instances of untrusted access: this is so because for each NG-PDG, a separate derived key K_NG-PDG, bound to the identity of the NG-PDG, is generated. Re-authentications between an NG UE and the same NG-PDG avoid replay attacks through the nonce exchange inbuilt in IKEv2.

Lenovo Ex. 1007
Page 106

Editor's Note: it is ffs whether EMSK should be used to derive the anchor key instead of using MSK as the anchor key in case an EAP method other than EAP-AKA' is used (to achieve serving network binding).

- The UE performs a corresponding key derivation of derived key from the anchor key.
- In case, NAS messages are sent after the establishment of an IPsec security association then they can be protected as follows:
    - Use of NAS layer security: The SCMF derives NAS keys from the anchor key MSK and delivers the NAS keys to the MMF and SMF, as appropriate. This would be in line with an access-agnostic handling of NAS security. It would have the downside, though, of double protection, by IPsec and by NAS security. This may be acceptable, though, as signalling messages are rare.

Editor's Note: The possibility of protecting NAS messages by some form of IP address binding is ffs.

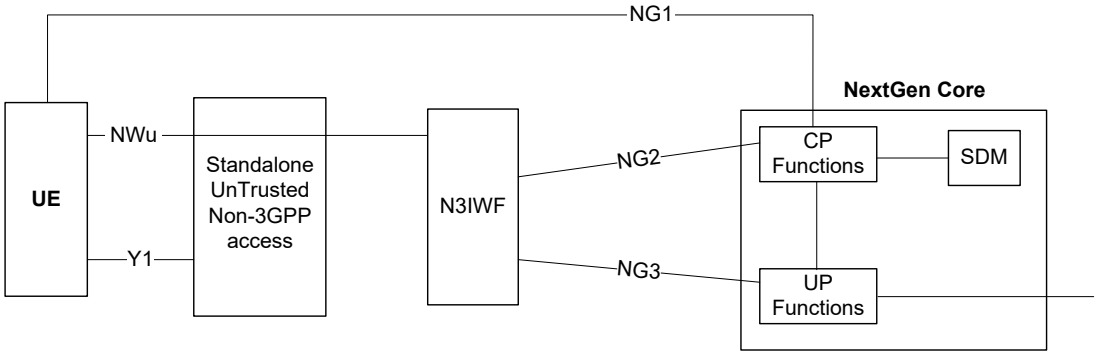
Editor's Note: Impact on EAP fast re-authentication is ffs.

5.1.4.26.3 Evaluation

5.1.4.27 Solution #1.27: Authentication and Key Agreement procedure for untrusted non-3GPP Access

5.1.4.27.0 General

The following high-level architecture is used for standalone untrusted non-3GPP accesses. The details of this architecture are specified in the TR 23.799.



5.1.4.27.1 Solution Overview

As shown in Figure 5.1.4.27.1.1, upon successful IP connection of a UE to a non-3GPP access followed by N3IWF discovery, the N3IWF starts the IKEv2/EAP exchange to authenticate UE to AUSF and establish an IPsec SA between the UE and N3IWF.

After successful UE authentication and IPsec SA establishment, the UE and AMF exchange NAS messages via IPsec between UE and N3IWF, and over N1 interface between N3IWF and AMF.

Lenovo Ex. 1007
Page 107

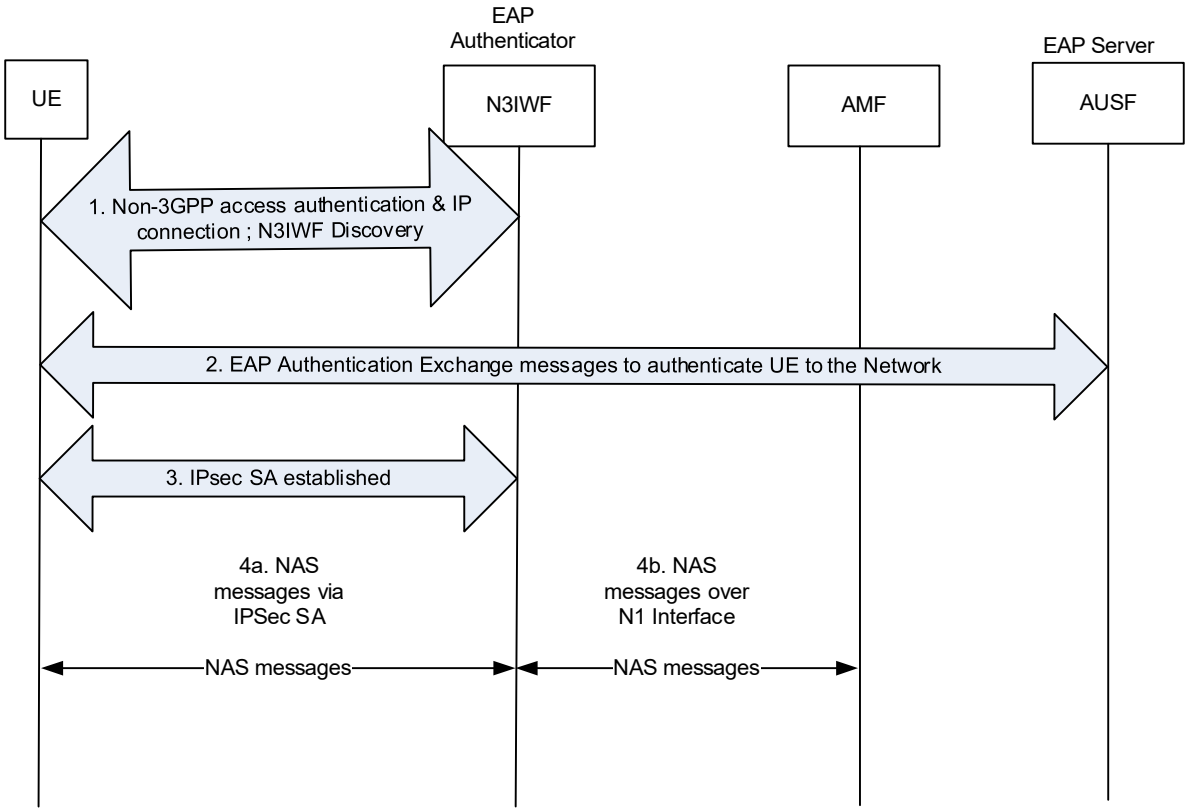


Figure 5.1.4.27.1.1: High-level Control Plane Procedure for Untrusted non-3GPP Access

Figure **5.1.4.27.1.2** depicts the protocol stack for Untrusted non-3GPP access.

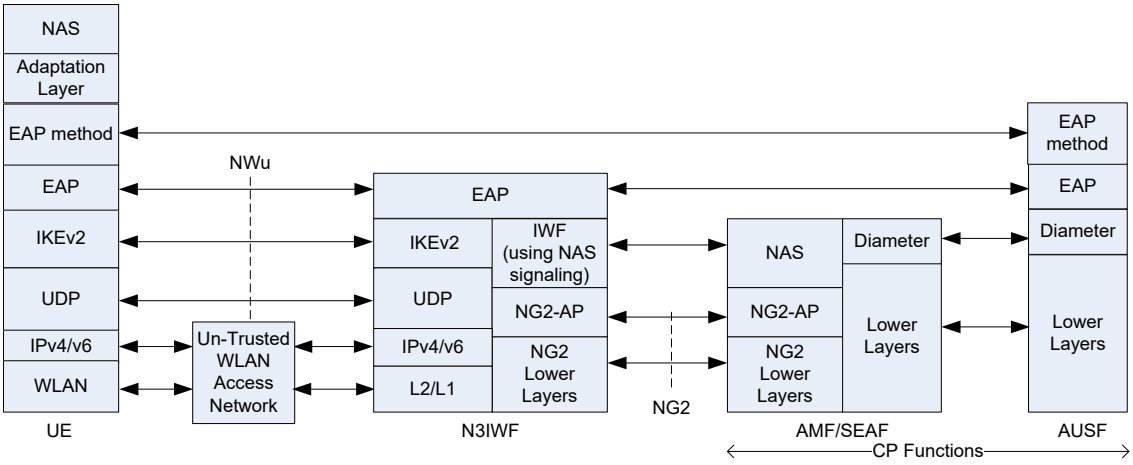


Figure 5.1.4.27.1.2: Control Plane Protocol Stack for untrusted non-3GPP Access

Editor's Note: UE and non-3GPP connectivity and N3WIF discovery are outside the scope of this solution.

5.1.4.27.2 Attach and UE Authentication Procedure via Untrusted non-3GPP Access

This section describes the Attach and UE Authentication procedure with flow between the UE and AMFfor Untrusted non-3GPP access, as depicted in Figure 5.1.4.27.1.4.

Lenovo Ex. 1007
Page 108

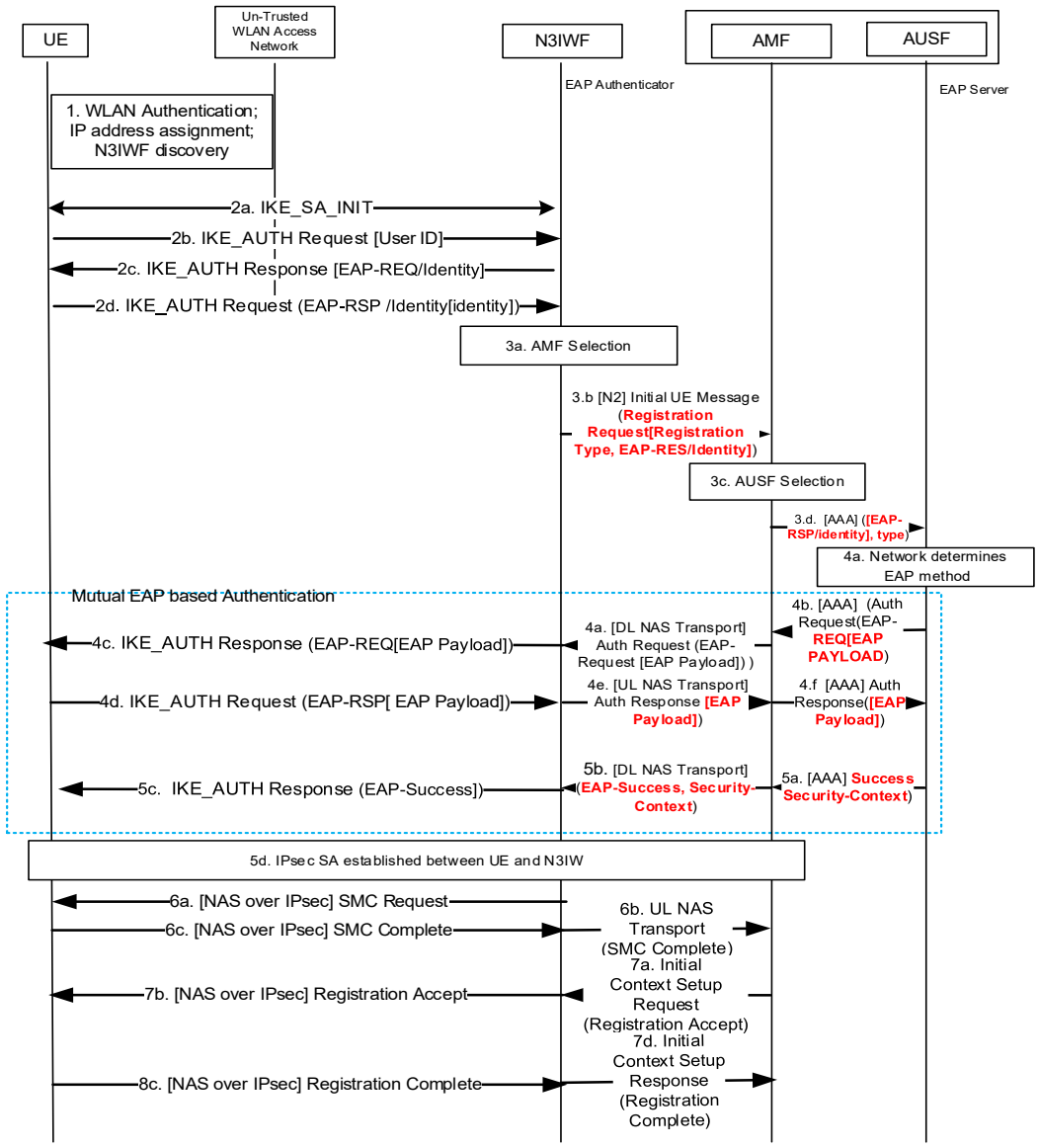


Figure 5.1.4.27.1.4: UE Authentication via Untrusted WLAN

1. The UE discovers and associates with the WLAN. Any non-3GPP authentication method can be used, e.g. no authentication (in the case of a free WLAN), EAP with a pre-shared key, username/password, etc. When the UE decides to connect to NextGen core, the UE discovers the IP address of N3IWF by executing the existing procedure for ePDG discovery and proceeds with the establishment of an IPsec SA as discussed below.

2. The normal IKEv2 signaling initiates as per RFC7296 (IKEv2) and RFC5998 (EAP-only authentication in IKEv2). The N3IWF behaves as EAP authenticator and retrieves the identity of the UE (step 2d).

3a-b. N3IWF shall construct a Registration Request (EAP-RES-identity, Registration-type) message on behalf of the UE and sends this message to the AMF over N2 interface. The Registration-identity shall contain the UE identity in NAI format. The Registration-type shall indicate the type of requested registration (e.g., Initial Registration) that this is a registration request over untrusted non-3GPP access.

3c-b. Upon receipt of the Registration-Request message, AMF shall select AUSF, according to procedure specified in TR 23.799. AMF then shall request AUSF to authenticate the UE by sending the EAP-RES-Identity payload to AUSF over AAA interface.

4. The AUSF (operating as an EAP server) shall select the EAP method to authenticate the UE based on received UE information and optionally information retrieved from UDM. The AUSF shall send EAP-Authentication Request to the UE.

Lenovo Ex. 1007
Page 109

Several EAP authentication request/response messages may take place between the UE and ASUF until EAP-based mutual authentication is completed. Between AUSF and AMF, EAP authentication request / response messages are encapsulated within NAS authentication request / response messages over N2 interface. Between UE and N3IWF, EAP authentication request / response messages are encapsulated within IKEv2 messages.

5a. When the EAP-based mutual authentication procedure is successfully completed, AUSF shall send EAP Success and security-context to AMF over AAA interface. The security-context shall contain one or more master session keys which are used by AMF to derive NAS security keys and security keys for N3IWF.

5b. In turn, the AMF shall send the Security-Context, received from AMF, and optionally Security Mode Command (SMC) request message to N3IWF. At this point, N3IWF creates a UE context which store UE-specific information such as UE identity, security context, etc.

5c-d. The N3IWF shall send an IKEv2 Authentication-Response (EAP-Success) message to UE which completes establishment of IPsec SA between the UE and N3IWF.

Editor's Note: it is FFS to use IPsec transport mode or in tunnel mode for carrying NAS messages.

6. Via the established IPsec SA, the N3IWF shall send SMC request received from AMF in step 6a. The UE responds with a NAS SMC complete messages, which shall be forwarded to AMF.

7. The AMF shall send a Registration Accept message to N3IWF, which shall be forwarded to UE via the established IPsec SA. Finally, the UE shall respond with Registration Complete message which shall be forwarded by N3IWF to AMF.

5.1.4.27.3 Evaluation

1) The Solution does not impact NextGen N1 or N2 interfaces

2) The solution supports unified EAP authentication framework for 3GPP and non-3GPP access.

The Solution uses a standard EAP framework and hence any IETF defined EAP method selected by SA3 can be used.

5.1.4.28. Solution #1.28: Authentication and Key agreement procedure for NextGen architecture with stand-alone non-3GPP access

5.1.4.28.1 Solution Overview

Upon successful IP connection of the UE to a non-3GPP access followed by N3IWF Gateway discovery, the UE starts the IKEv2 protocol exchange with N3IWF gateway to encapsulate 3GPP NAS messages used for the Attach procedure with EPS AKA messages between the UE and CP function as shown in Figure 5.1.4.28.1-1.

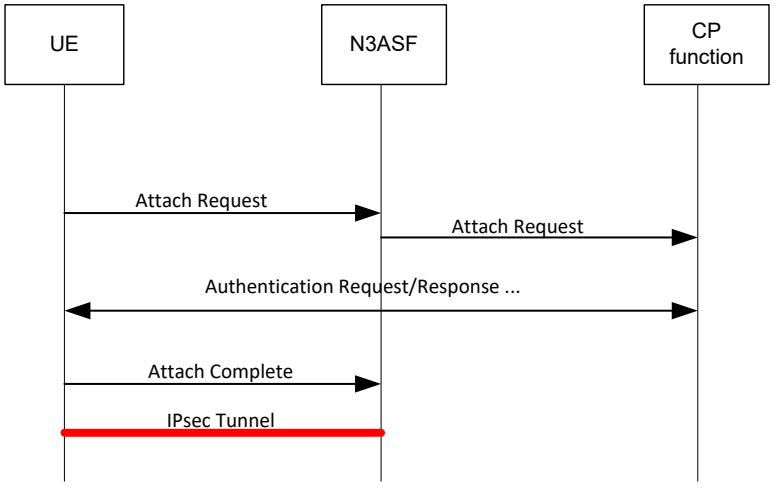


Figure 5.1.4.28.1-1: High-level 3GPP EAP-AKA flow for Non-3GPP Access

Lenovo Ex. 1007
Page 110

As shown in Figure 5.1.4.28.1-2, 3GPP Attach messages from the UE to N3IWF are encapsulated inside IKEv2/EAP. The N3IWF decapsulates Attach message received from the UE, and forwards it to the CP function over NG2 interface. And the reversed flow works similarly over NG2 interface from CP function to the N3IWF, and IKEv2/EAP encapsulation over IP interface from the the N3IWF to the UE.

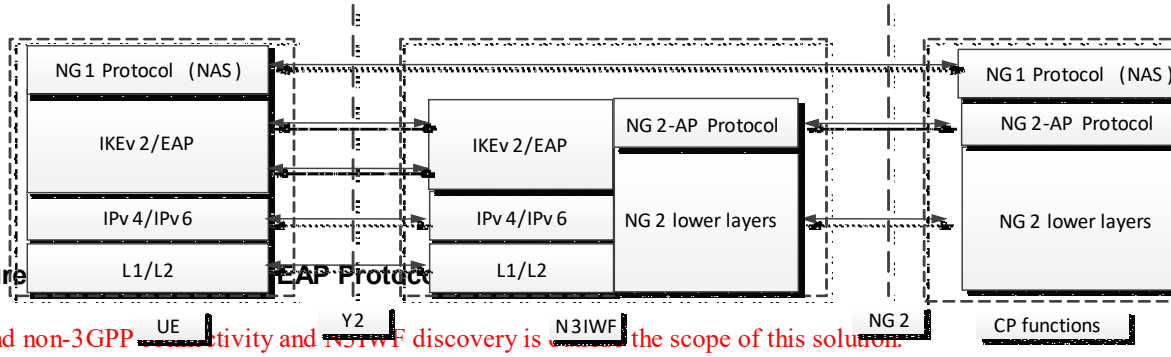


Figure EAP Protocol

Editor's Note: UE and non-3GPP connectivity and N3IWF discovery is out of the scope of this solution.

Upon successful completion of the 3GPP Attach procedure with EPS AKA, the security association between the UE and CP, and the UE and N3IWF are established. The UE-CP security association used for protecting end-2-end control plane message exchanges between the UE and CP. And UE-N3IWF security association is used for establishing IPsec tunnel between the UE and N3IWF.

The security mode message exchanges between the UE and CP may stay the same as defined in the Attach procedure with EPS AKA for 3GPP access. The security mode message exchanges between UE and eNB as defined in the Attach procedure with EPS-AKA for 3GPP access shall be skipped – this will be done as part of IKEv2 protocol.

Editor's Note: New EAP method needs to be defined to carry 3GPP Attach messages inside IKEv2.

Editor's Note: The security of NG2 and NG3 interfaces are outside the scope of this solution.

5.1.4.28.1.2 Attach Procedure with EPS-AKA for non-3GPP Access

This section describes the Attach procedure with EPS-AKA flow between the UE and CP function. Figure 5.1.4.28.1.2-1 describes the Attach procedure with EPS-AKA via non-3GPP access.

Editor's Note: It is FFS whether a different AKA method from EPS-AKA is to be used for NextGen.

Lenovo Ex. 1007
Page 111

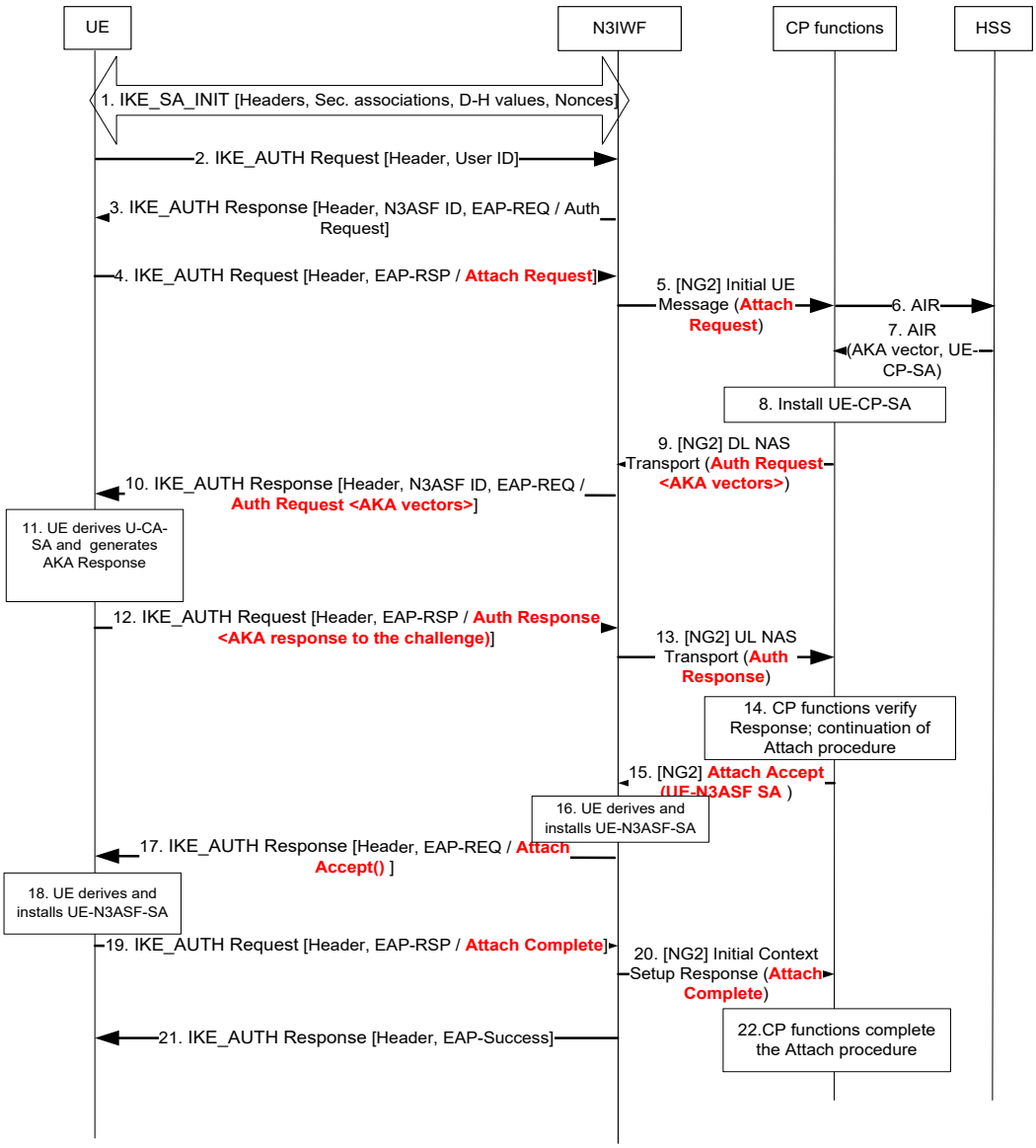


Figure 5.1.4.28.1.2-1: Attach with EPS-AKA flow for Non-3GPP Access

The Attach with EPS-AKA flow for Non-3GPP access is as follows:

1. Before attempting IKEv2 connection establishment, the UE first needs to discover a N3IWF. This is achieved by configuring in the UE one or more of the following:

   - An IP address (or set of IP addresses) of N3IWF node(s).

   - An FQDN (or set of FQDNs) that can be resolved into IP address of a N3IWF.

- using DHCP configuration.

2. UE sends IKE_AUTH Request

3. N3IWF triggers Auth request using EAP-REQ

4. UE sends Attach request encapsulated inside EAP-RSP.

5. The N3IWF forwards the request to the CP Functions

6-8. CP Functions Derives key material and retrieves Authentication Vectors for generating key material from Authentication Entity e.g. AAA or HSS. Authentication Entity also generates UE-CP Security association which is installed by CP-Functions.

Lenovo Ex. 1007
Page 112

9-10. N3IWF responds with an IKE_AUTH Response including the NAS authentication request. Payload contains the Authentication vectors for key derivation.

11. UE generates UE-CP-SA using Authentication vectors received as part of Authentication Request

12. The UE sends the IKE_AUTH Request with response to AKA challenge

13. The N3IWF processes the EAP request and Authentication response over NG2 to the CP Functions.

14. CP Functions verify response and continue attach procedure.

15, 16. Step 15 provides the access independent security context that is to be used by the N3IWF to derive keying material for the protection of the N3-ASF connection. UE-N3IWF-SA is installed in step 16.

17, 18. The CP Functions complete the authentication procedure towards the UE and provides the security context for the UE, including the generic attach security context and the security context for the setup of the IPsec Tunnel. The CP functions forward the security context for the establishment of the IPsec Tunnel over NG2 to the N3IWF

19, 20. Upon successful completion of the Attach procedure with EPS-AKA, the security association between the UE and CP function is established.

Upon a successful Attach with EPS-AKA procedure, an IPsec SA is established between the UE and N3IWF. As part of IKEv2 phase 2, in addition to an IPsec SA the UE also receives an inner IP address that it will be bounded to this IPsec SA. The inner IP address will be used as a source IP address for IP packets carrying NAS messages from UE to CP – also referred to as NAS bearer.

The UE uses the same IPsec tunnel to route control and user plane traffic to the core network. When the UE performs the detach procedure, the UE and N3IWF shall release the IPsec tunnel.

5.1.4.28.3 Evaluation

Editor's Note: Evalutaion content is FFS.

Editor's Note: Clarification is needed how IKEv2 could be successfully completed and IPsec SAs can be set up using EPS AKA, and not any EAP method for authentication of UE in its role as IKE initiator.

Editor's Note: It is ffs how an entire Attach request message can be included in an EAP Identity response message.

Editor's Note: It is ffs how the definition of a new EAP method could help as the EAP Identity response message is EAP method independent.

Editor's Note: It needs to be clarified why NAS Attach/authentication messages needs to be carried over EAP.

5.1.4.29 Solution #1.29: A solution for KDF negotiation

5.1.4.29.1 Introduction

The solution addresses the key issue #1.18 flexible security capability negotiation in control plane.

NextGen has a long lifetime, a suitable KDF may be discovered. However, in LTE, KDF is implemented stably, and cannot be negotiated, it is the only way to upgrade KDF that replace all the devices related to KDF.

However, in this solution, KDF can be updated in a comfortable way. There are five different KDFs including gNB-KDF, AMF-KDF, SEAF-KDF, SMF-KDF and ARPF-KDF according to different communication peers, so that UE could negotiate KDF with different NEs separately for a suitable KDF algorithm. Firstly, KDF can be added in UE and different NEs at different time. Secondly, when KDF algorithm addition is complete in two devices, the devices could use a suitable KDF to generate communication keys after KDF negotiation procedure. Finally, when all the devices have been added suitable KDF algorithm completely, all of them could use a suitable KDF. During the whole updating period, solution ensures that there is no communication barriers because of partly updating.

However, it is not means that UE shall implement 5 different KDF algorithms. The 5 different KDF could just be one KDF algorithm, the only difference is the communication peer in negotiation procedure.

Lenovo Ex. 1007
Page 113

5.1.4.29.2 Solution details

5.1.4.29.2.0 General

In figure 5.1.4.9.2.2-1 in solution #1.9, there are 5 different kind of KDFs:

gNB-KDF: the KDF for K_{ANCP} to generate K_{RRCenc} and K_{RRCint} at both UE and gNB

AMF-KDF: the KDF for K_{NAS} to generate K_{NASenc} and K_{NASint} at both UE and AMF

SEAF-KDF: the KDF for K_{NG} to generate K_{NAS}, K_{ANCP} and K_{UP} at both UE and SEAF

SMF-KDF: the KDF for K_{UP} to generate Ksession-enc and Ksession-int at both UE and SMF

ARPF-KDF: the KDF for K to generate K_{NG} at both UE and ARPF

For this solution, UE will inform it's supported KDFs to gNB, AMF, SEAF, SMF and ARPF, and will negotiate with them respectively. In the solution, gNB-KDF is negotiated in AS SMC procedure, AMF-KDF and SEAF-KDF are negotiated in MM SMC procedure, SMF-KDF is negotiated in SM SMC procedure, and ARPF-KDF is negotiated in AKA procedure.

5.1.4.29.2.1 gNB-KDF negotiation

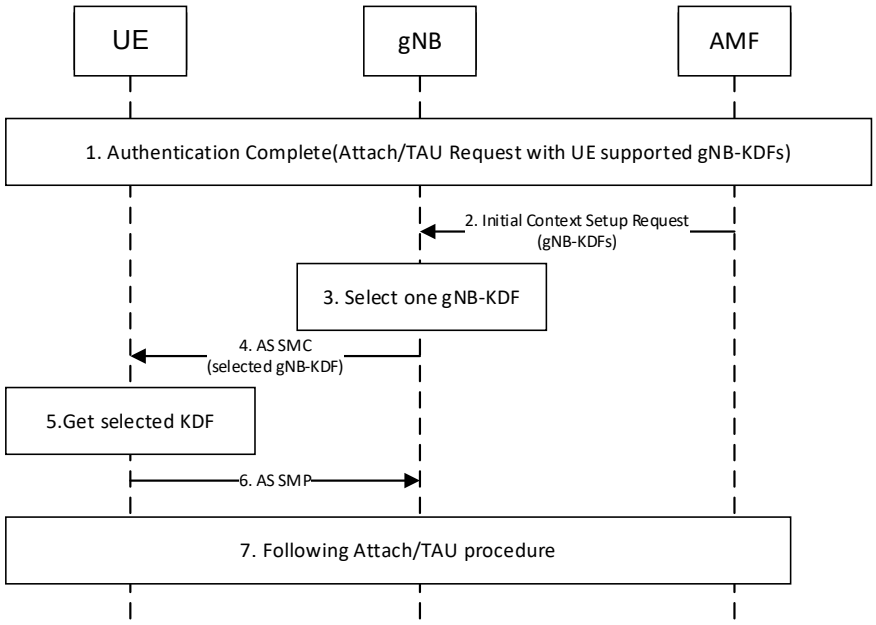


Figure 5.1.4.29.2.1-1:

1. UE has been authenticated to network, and the supporting UE's gNB-KDFs can be included in UE network capability and be informed to AMF in attach/TAU request.
2. AMF informs the UE's gNB-KDFs to gNB via NG2 interface, like initial context setup request signalling through S1 in LTE.
3. The gNB selects one KDF used to derive K_{RRCenc} and K_{RRCint}.
4. GNB sends AS SMC message to UE including selected gNB-KDF.
5. UE receives AS SMC message, and knows the gNB-KDF selected by gNB.

Lenovo Ex. 1007
Page 114

5.1.4.29.2.2 AMF-KDF negotiation

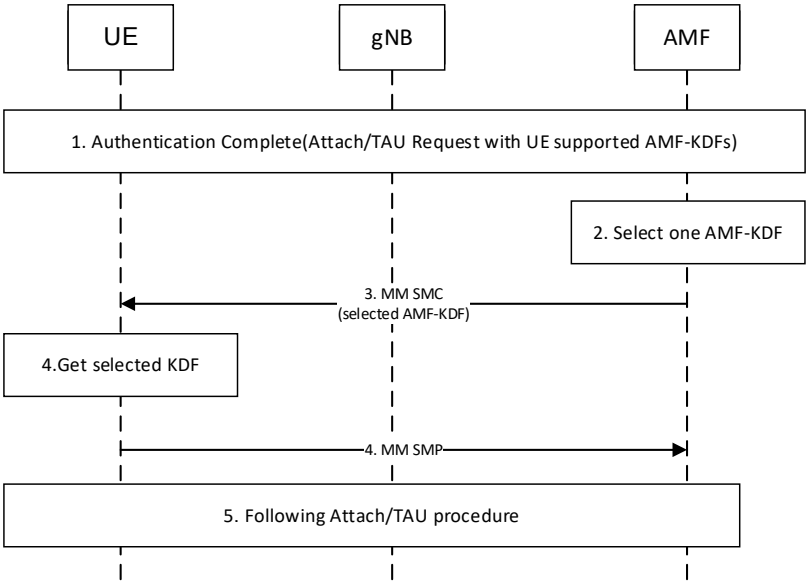


Figure 5.1.4.29.2.2-1:

1. UE has authenticated to network, and the supporting UE's AMF-KDFs can be included in UE network capability and informed AMF in attach/TAU request.
2. AMF selects one KDF used to derive K_{NASenc} and K_{NASint}.
3. AMF sends MM SMC message to UE including selected AMF-KDF.
4. UE receives MM SMC message, and knows the AMF-KDF selected by AMF.

5.1.4.29.2.3 SEAF-KDF negotiation

SEAF-KDF negotiation procedure is similar to AMF-KDF negotiation procedure.

The supporting UE's SEAF-KDFs can be included in UE network capability and informed AMF in attach/TAU request. AMF will inform the UE's SEAF-KDFs to SEAF. SEAF will select an SEAF-KDF used to derive K_{NAS}, K_{ANCP}, K_{UP} and inform the KDF to UE passed by AMF via MM SMC procedure.

Editor's Note: it is ffs whether a separate SEAF-KDF negotiation procedure is needed.

Lenovo Ex. 1007
Page 115

5.1.4.29.2.4 SMF-KDF negotiation

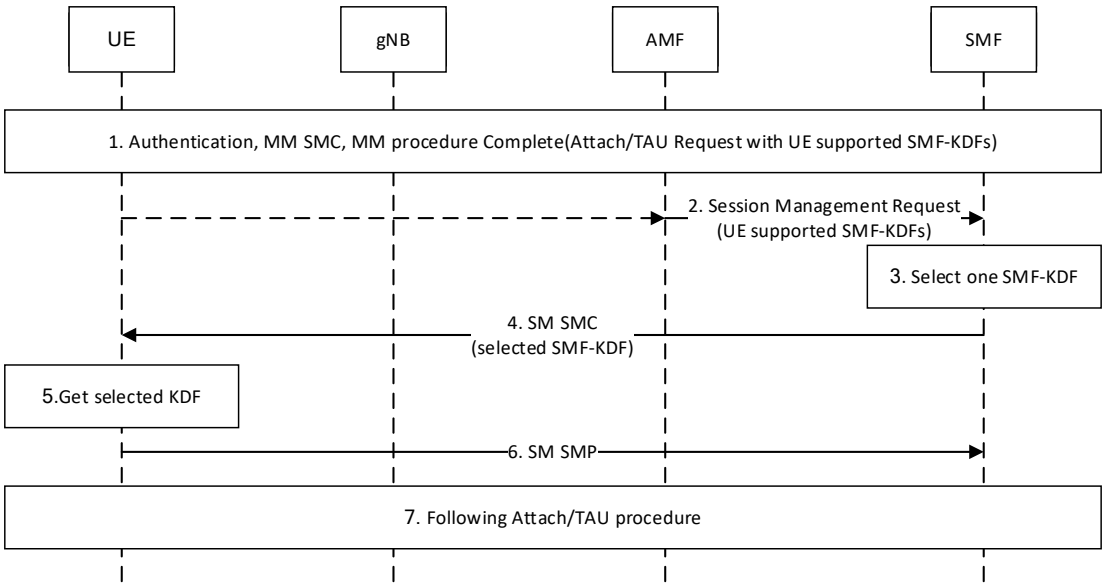


Figure 5.1.4.29.2.4-1:

1. UE has authenticated to network, and the supporting UE's SMF-KDFs can be included in UE network capability and informed AMF in attach/TAU request.
2. AMF informs SMF UE supported SMF-KDFs in SM procedure.
3. SMF selects one KDF used to derive $K_{session\text{-}enc}$ and $K_{session\text{-}int.}$
4. SMF sends SM SMC message to UE including selected SMF-KDF.
5. UE receives SM SMC message, and knows the SMF-KDF selected by SMF.

Editor's Note: it is ffs whether a separate SMF-KDF negotiation procedure is needed.

5.1.4.29.2.5 ARPF-KDF negotiation

ARPF-KDF must be negotiated between UE and ARPF. However, UE only has communication in authentication procedure with ARPF, and there is no need to add another signalling for ARPF to indicate the selected algorithm. So, the solution indicates the UE in AMF in AV, not in NAS SMC.

Lenovo Ex. 1007
Page 116

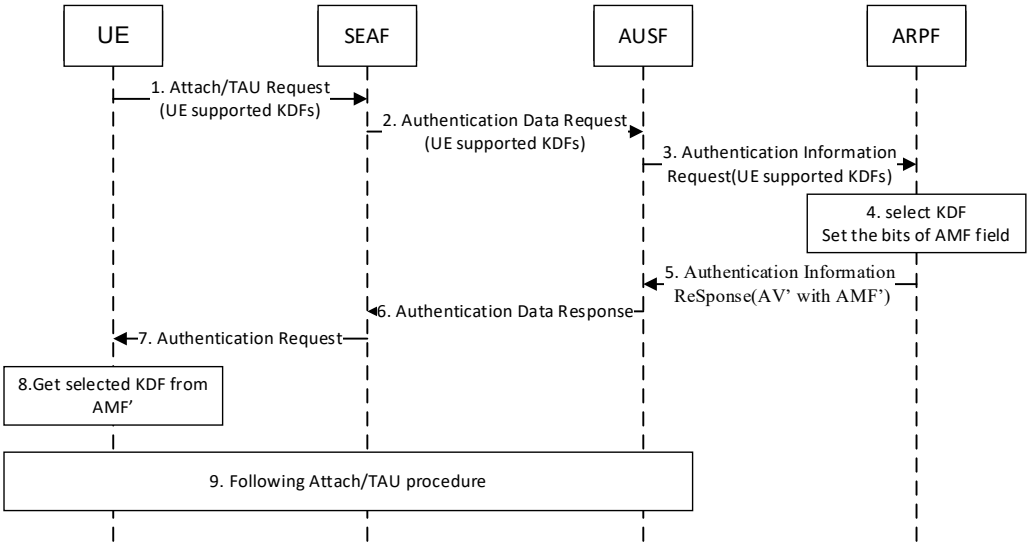


Figure 5.1.4.29.2.5-1:

1. UE sends Attach/TAU Request message to SEAF, the UE network capability included in Attach Request/TAU message will include the ARPF-KDFs supported by UE.

2. SEAF decides to run an AKA procedure, and sends Authentication Data Request message to AUSF, the ARPF - KDFs supported by UE is included in Authentication Data Request message.

3. AUSF sends Authentication Information Request message to ARPF, which includes at least IMSI or temporary ID of UE, ARPF-KDFs supported by UE, etc.

4. ARPF receives the Authentication Information Request and achieves the ARPF-KDFs supported by UE, and then ARPF selects one KDF used to derive Kng according to the configured allowed list of security capabilities of the ARPF and sets certain bits in the AMF field of AUTN to indicate the selected KDF of Kng, and gets new AV' with AMF'.

5. ARPF sends Authentication Information Response message to AUSF which includes RAND and AUTN' with AMF'.

6. AUSF sends Authentication Data Response message for transiting RAND and AUTN' to UE.

7. SEAF sends Authentication Request message to UE for transiting RAND and AUTN'.

8. UE receives Authentication Request message, and checks the certain bits of AMF in AUTN and knows the ARPF-KDF selected by ARPF.

Editor's Note: it is ffs whether the use of AMF bits is the right approach as the number of such bits is very limited.

Editor's Note: it is ffs whether it would be more suitable to negotiate the KDF together with an AKA algorithm set such as MILENAGE or TUAK.

5.1.4.29.3 Evaluation

Security:

1) Bidding-down attack to the uplink message

The KDFs supported by UE in the first Attach/TAU request message may be tampered by an attacker, the attacker could change the KDFs into weak ones, which impacts the network's decision, and UE may negotiate a weak KDF with the network. However, solution#1.13 has solved the problem.

2) Bidding-down attack to the downlink message

Lenovo Ex. 1007
Page 117

The integrity of all selected KDF is protected, because certain bits in the AMF field of AUTN indicates ARPF-KDF selected by ARPF, whose integrity is protected by MAC in AUTN, and gNB-KDF, AMF-KDF, SEAF-KDF, SMF-KDF is included in SMC, whose integrity is protected by K_{NASint}. So, the negotiated KDF will not be tampered by an attacker.

Flexibility:

1) Evolutionary

NextGen has a long lifetime, a suitable KDF may be discovered. However, in LTE, KDF is implemented stably, and cannot be negotiated, the way to upgrade KDF is that replace all the devices related to KDF, e.g. UE, gNB, AMF, SMF, ARPF and so on. Otherwise, during the updating period, e.g. gNB and UE have been updated, but AMF has not done, UE cannot communicate with AMF because they have the different KDF algorithm, which results in failure for UE to attach the network. So, it is a difficult way to update the KDFs.

However, the solution solve the problem. The upgrade infects little about protocol, and could update the devices one by one without any communication barriers. For example, UE updates its supporting gNB-KDFs, and gNB also updates its supporting gNB-KDFs in the same way, then UE could negotiate a suitable KDF with gNB. During the updating period, e.g. gNB has been updated, and UE has not done, UE could still communication with gNB with former KDF. The solution makes two elements using a suitable KDF easily and cheaply.

2) Partly-Upgrade

The upgrade in the solution is partly implemented, the system is communicable all the time, whenever UE and other NEs upgrade their supported KDFs, because KDF negotiation in different NE is separated. There are some update scenarios.

UE has updated the KDF, other NEs has not done: UE will negotiate an old KDF with other NEs.

UE has not done, other NEs have updated the KDF: UE will negotiate an old KDF with other NEs.

UE has updated the KDF, NE1 (e.g. ARPF) has done, NE2 (e.g. gNB) has not done: UE will negotiate a new KDF with NE1 to generate Kng, and negotiate an old KDF with NE2 to generate K_{RRCenc} and K_{RRCint}.

So, the negotiation system is flexible, and it is easy to evolve.

Overhead：

1) Communication:

The solution is a based on the existing security procedure in TR 33.899, e.g. AS/MM/SM SMC, AKA, so there is no additional signalling. The communication overhead is based on the additional length of the message.

All the UE supported KDFs are included in UE network capability in Attach/TAU request. In LTE, UE supported ciphering/integrity protection algorithm is indicated by two octets in UE network capability. So, UE supported KDFs could also do like that. Since there are 5 kind of KDFs, and assume that each KDF has 8 possible algorithms, the maximum increasing length of Attach/TAU request is 5 bytes. However, considering that different kind of KDFs may use the same KDF algorithm, and there may be some combination of NEs and reduction of supported algorithms, the increasing length could be shorter.

The selected KDF is returned by NE in AS/MM/SM SMC message or AMF in Authentication Information Response. In LTE, selected ciphering/integrity protection algorithm by MME is indicated by an octet in NAS security algorithms with 1 bit for spare and 3bits for indication of each algorithm. Meanwhile, selected ciphering/integrity protection algorithm by eNB is indicated by 2 IEs (2 octets) in SecurityAlogrithmConfig. So, the selected KDF could also do like that. Since there are 2 KDFs returned in MM SMC, 1 KDF returned in SM SMC, and 1 KDF returned in AS SMC, the maximum increasing length of SMC message are separately 2, 1, and 1 bytes. Meanwhile, if the number of ARPF supporting KDFs are 8, 3 bits in AMF be used. However, consider that there may be some combination of NEs, or supported algorithms may be decreased, the increasing length could be shorter.

In summary, there is no additional signalling for the solution, and it is low-cost on message length, so, the communication overhead is cheap.

2) Computation:

The additional computation for the solution is also cheap, UE and NEs just need a selection operation for indicating the selected KDF algorithm, which could be ignored.

Lenovo Ex. 1007
Page 118

3) Storage:

Though there are 5 different kind of KDFs, but the algorithm they use may be the same in a large probability, or UE may support 2 different KDF algorithms at the same time for compatibility with non-updated NEs. If the solution is just used for KDF upgrade, the unused KDF could be remove in the next upgrade, and just keep at most 2 KDF algorithms in UE. So, the algorithms implemented in UE are acceptable.

Summary:

In this solution, KDF could be negotiated separately between UE and NEs with tiny overhead on communication, computation and storage resource, which introduces a flexible and safe negotiation system. A suitable KDF could be updated in different NEs and UE so that UE and NE could negotiate a new KDF in a comfortable way without any communication barriers during the long lifetime usage of NextGen.

5.1.4.30 Solution #1.30 Registration Procedure for NextGen network

5.1.4.30.1 Introduction

This solution explains the registration procedure for NextGen network.

5.1.4.30.2 Solution details

Figure 5.1.4.30.2-1 shows the call flow for registration procedure of non-roaming scenario.

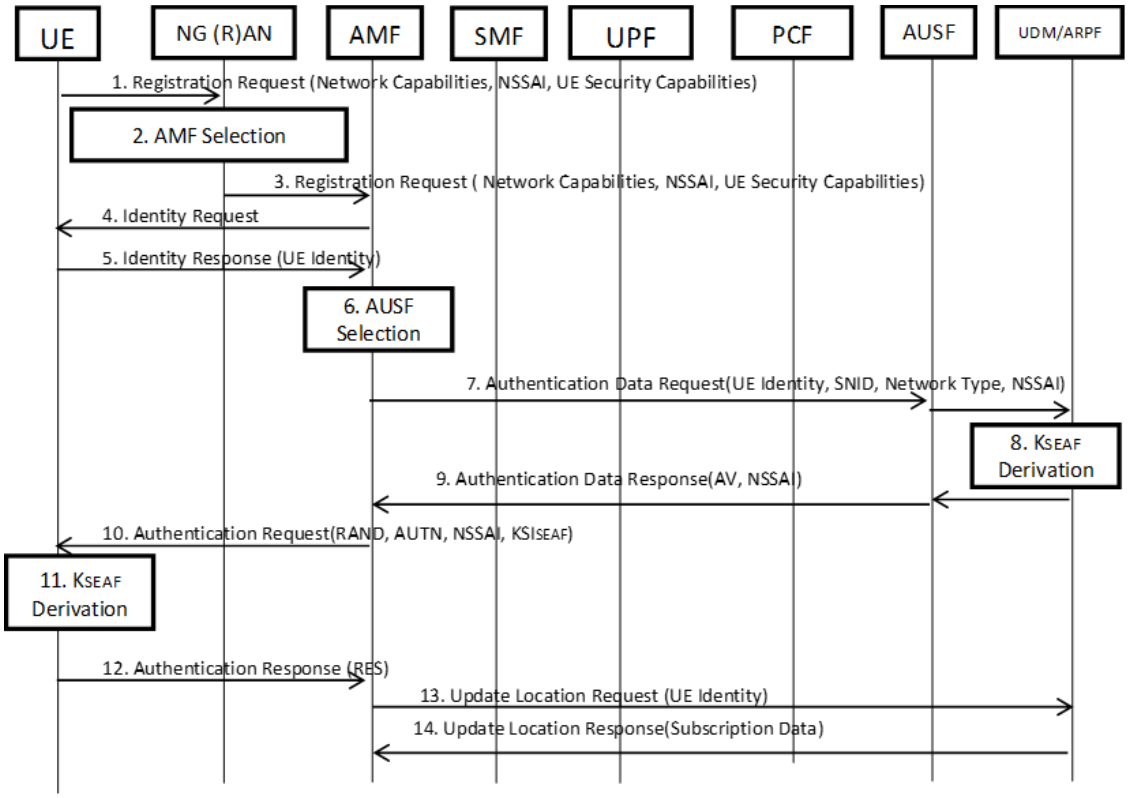


Figure 5.1.4.30.2-1 Call flow for Registration procedure of non-roaming scenario

1. UE sends the Registration Request (Network Capabilities, NSSAI, UE Security Capabilities) to the NG (R)AN.
2. The NG (R)AN selects the appropriate AMF based on the NSSAI provided by the UE (ref. TR 23.799 v 2.0.0 clause 8.1 Agreements on Network Slicing).
3. The NG (R)AN then forwards the Registration Request to the appropriate AMF.
4. The AMF sends the Identity Request to the UE.

Lenovo Ex. 1007
Page 119

5. The UE sends the Identity Response(UE Identity) to the AMF.
6. The AMF selects the appropriate AUSF.
7. The AMF sends the Authentication Data Request(UE Identity, SNID, Network Type, NSSAI) to the AUSF. The AUSF then forwards this to the UDM/ARPF.
8. The UDM/ARPF derives the K_{SEAF} and generates the AV to be sent to the UE.
9. The UDM sends the Authentication Data Response(AV, NSSAI) to the AMF via the AUSF.
10. The AMF then sends the Authetication Request(RAND, AUTN, NSSAI, KSI_{SEAF}) to the UE.
11. The UE derives the K_{SEAF} and checks the authentication token derived to authenticate the network ($AUTN_{SEAF}$ = $AUTN_{UE}$).
12. The UE then sends the Authentication Response (RES) to the AMF which checks the RES with the XRES to authenticate the UE.
13. The AMF then sends the Update Location Request(UE Identity) to the UDM.
14. The UDM/ARPF responds with the Update Location Response to the AMF.

Note: This registration procedure follows the existing AKA procedure

Editor's Note - Possibility of sending the device identity in the service request message instead in steps 4 and 5 is for FFS

5.1.4.30.3 Evaluation

FFS

5.1.4.31 Solution #1.31 Security mode command procedure for NextGen network

5.1.4.31.1 Introduction

This solution addresses the security mode procedure for NextGen network.

5.1.4.31.2 Solution details

Security mode procedure in the NextGen consists of NAS security mode procedure, AS security mode procedure and UP security mode procedure. The reason for introduction of UP security procedure is to handle user plane security between UE and UPF.

This solution makes following assumptions:

- AKA procedure precedes Security Mode procedure.

5.1.4.31.2.1 NAS security mode command procedure

Figure 5.1.4.31.2.1-1 shows the detailed procedure to establish NAS Security UE and AMF.

15. After the UE is authenticated, the AMF derives K_{NAS_MM} from K_{SEAF}.
16. The AMF then request the algorithm to establish NAS security from the SPCF.
17. The SPCF selects a suitable algorithm based on the security capabilities of the UE and sends the algorithm information to the AMF in the Security Algorithm Response message.
18. The AMF uses the algorithm selected by the SPCF to derive K_{NAS_MMint} and K_{NAS_MMenc}, the integrity and encryption keys for NAS Security.
19. The AMF then sends the NAS Security Mode Command(KSI, Replayed UE Security Capabilities, Replayed NSSAI, NAS Algorithms, NAS-MAC) to the UE.
20. The UE derives K_{NAS_MM}, K_{NAS_MMint} and K_{NAS_MMenc} keys using the parameters received from the AMF.
21. The UE sends the integrity protected and encrypted NAS Security Mode Complete (NAS-MAC) to the AMF.

Lenovo Ex. 1007
Page 120

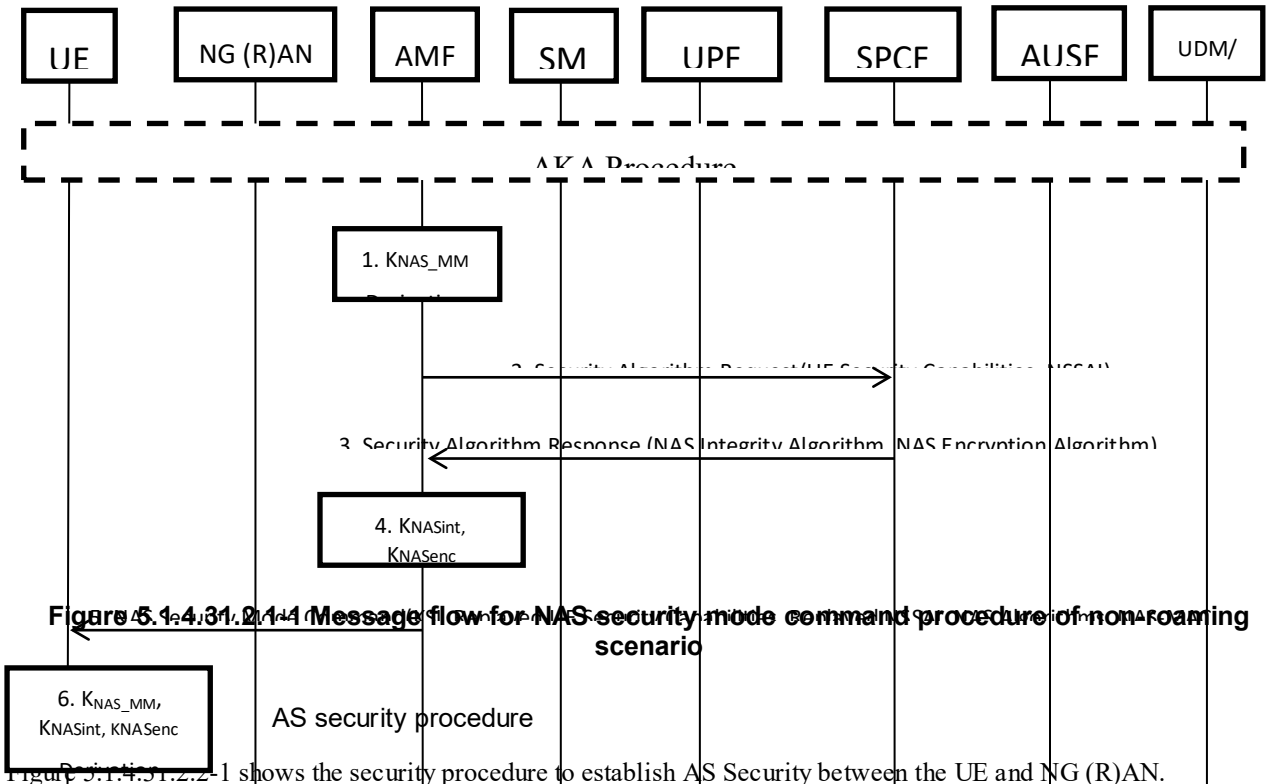
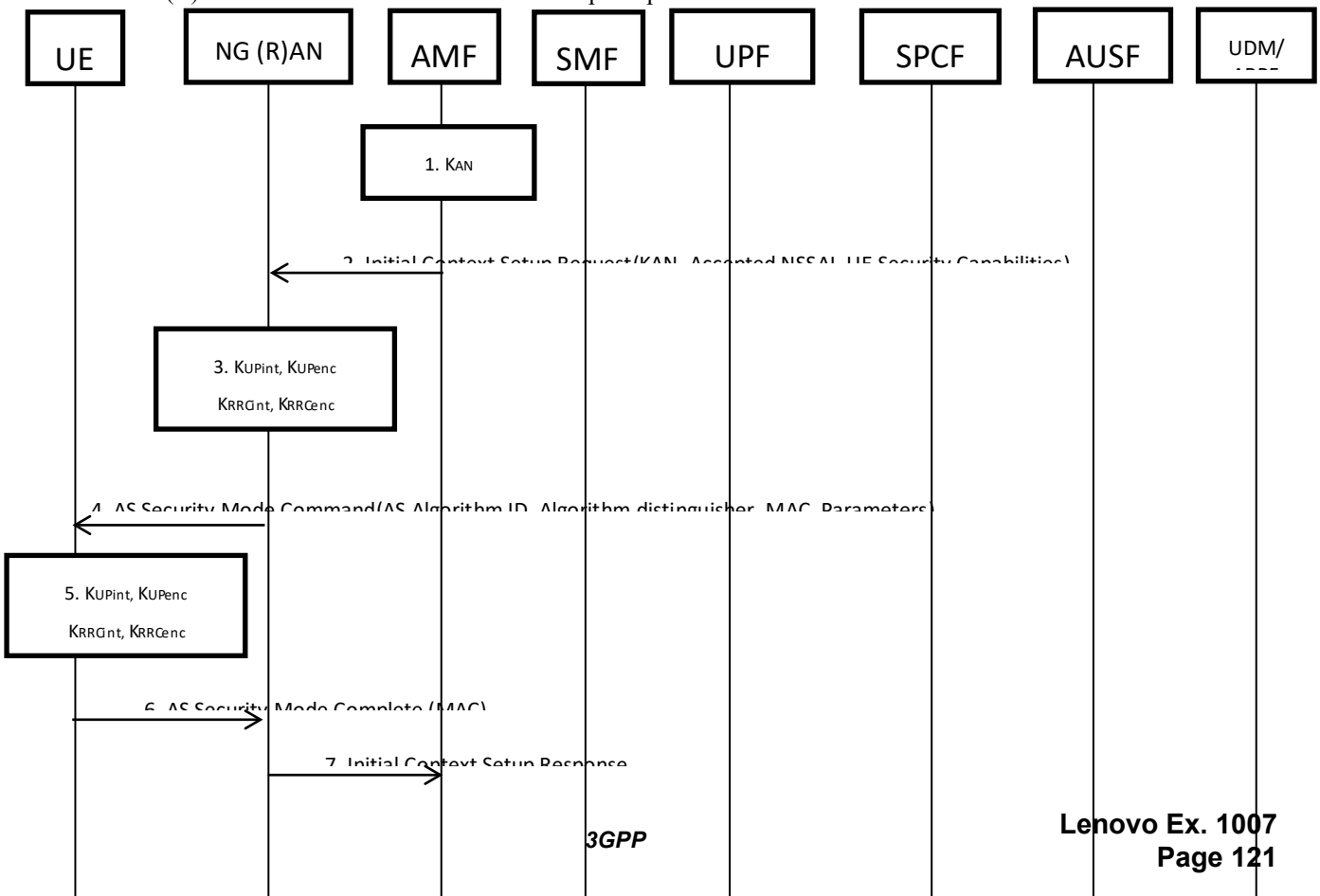


Figure 5.1.4.31.2.1-1 Message flow for NAS security mode command procedure of non-roaming scenario

Figure 5.1.4.31.2.2-1 shows the security procedure to establish AS Security between the UE and NG (R)AN.

1. The AMF derives K_{AN} from K_{SEAF}.
2. The AMF sends the Initial Context Setup Request(K_{AN}, Accepted NSSAI, UE Security Capabilities) to the NG (R)AN.
3. The NG (R)AN selects the algorithms for UP and RRC keys derivation and derives K_{UPint}, K_{UPenc}, K_{RRCint} and K_{RRCenc}.
4. The NG (R)AN sends the integrity protected AS Security Mode Command(AS algorithm ID, AS algorithm distinguisher, MAC) to the UE.
5. The UE derives the K_{AN} and corresponding RRC and UP integrity and encryption keys.
6. The UE then sends the AS SM Complete command along with MAC to authenticate the AS SMC message.
7. The NG (R)AN then sends the Initial Context Setup Response to the AMF.



Lenovo Ex. 1007
Page 121

Figure 5.1.4.31.2.2-1 Message flow for AS security mode command procedure of non-roaming scenario

5.1.4.31.2.3 UP security mode command procedure

Figure 5.1.4.31.2.3-1 shows the procedure to establish UP Security between UE and UPF. The UP Security Mode procedure is initiated when the UE requests to access a service (and a PDU session needs to be established).

1. The UE sends the Service Request to the CN(AMF) along with its security capabilities and SM-NSSAI.
2. The AMF then selects the suitable SMF based on the SM-NSSAI.
3. The AMF forwards the Service Request to the selected SMF.
4. If the SMF does not have the subscription data for the UE, it sends the Subscription Data Request to the UDM.
5. The UDM sends UE's subscription information to the SMF in the Subscription Data Response.
6. The SMF selects the appropriate UPF for the slice.
7. The SMF then derives K_{UP}, the key for UP protection.
8. The SMF sends requests the algorithm for generating the UP keys from the SPCF.
9. The SPCF sends the algorithm ID and distinguisher in the Security Algorithm Response to the SMF.
10. The SMF derives Ksessint, Ksessenc keys using the algorithms selected by the SPCF.
11. The SMF sends the UP Security Mode Command to the UE via the AMF.
12. The UE derives K_{UP}, Ksessint and Ksessenc using the parameters it receives.
13. The UE then sends the UP Security Mode Complete(NS-MAC) to the SMF via the AMF.
14. The SMF then sends the Service Accept(Ksessint, Ksessenc) to the UPF to establish UP Security between UE and UPF.

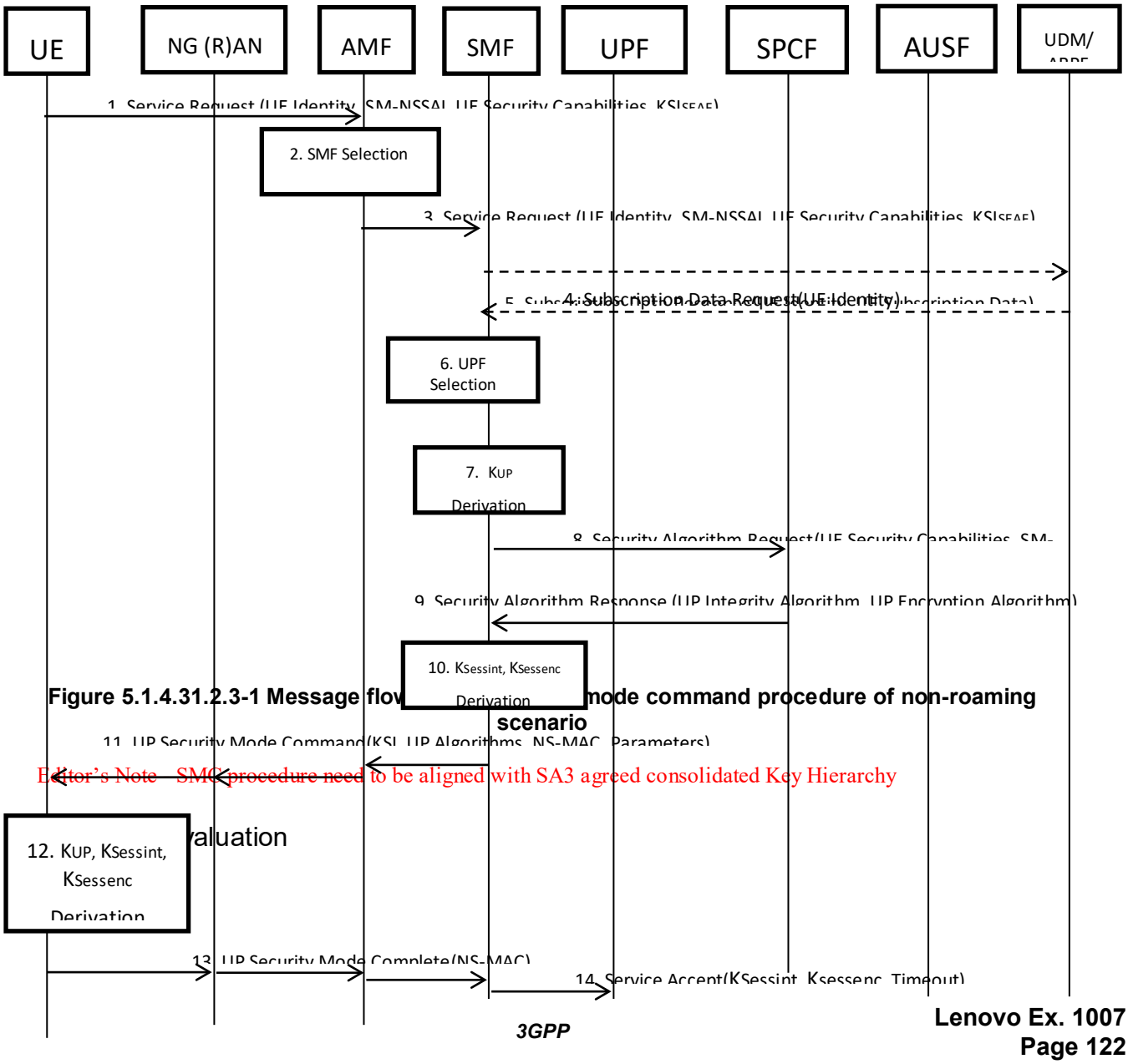


Figure 5.1.4.31.2.3-1 Message flow for UP security mode command procedure of non-roaming scenario

Editor's Note: SMC procedure need to be aligned with SA3 agreed consolidated Key Hierarchy

Lenovo Ex. 1007
Page 122

5.1.4.32 Solution #1.32 Security mode command procedure for NextGen network with NAS-SM

5.1.4.32.1 Introduction

This solution addresses the security mode procedure for NextGen network.

5.1.4.32.2 Solution details

Security mode procedure in the NextGen consists of NAS security mode procedure, AS security mode procedure, NAS-SM security mode procedure and UP security mode procedure. The reason for introduction of UP SM procedure is to establish user plane security between UE and UPF and the introduction of NAS-SM Security Mode procedure is to establish security for messages between UE and SMF.

This solution makes following assumptions:

- AKA procedure precedes Security Mode procedure.

5.1.4.32.2.1 NAS security mode command procedure

Figure 5.1.4.32.2.1-1 shows the detailed procedure to establish NAS Security UE and AMF.

22. After the UE is authenticated, the AMF derives K_{NAS_MM} from K_{SEAF}.
23. The AMF then request the algorithm to establish NAS security from the SPCF.
24. The SPCF selects a suitable algorithm based on the security capabilities of the UE and sends the algorithm information to the AMF in the Security Algorithm Response message.
25. The AMF uses the algorithm selected by the SPCF to derive K_{NAS_MMint} and K_{NAS_MMenc}, the integrity and encryption keys for NAS Security.
26. The AMF then sends the NAS Security Mode Command(KSI, Replayed UE Security Capabilities, Replayed NSSAI, NAS Algorithms, NAS-MAC) to the UE
27. The UE derives K_{NAS_MM}, K_{NAS_MMint} and K_{NAS_MMenc} keys using the parameters received from the AMF.
28. The UE sends the integrity protected and encrypted NAS Security Mode Complete (NAS-MAC) to the AMF.

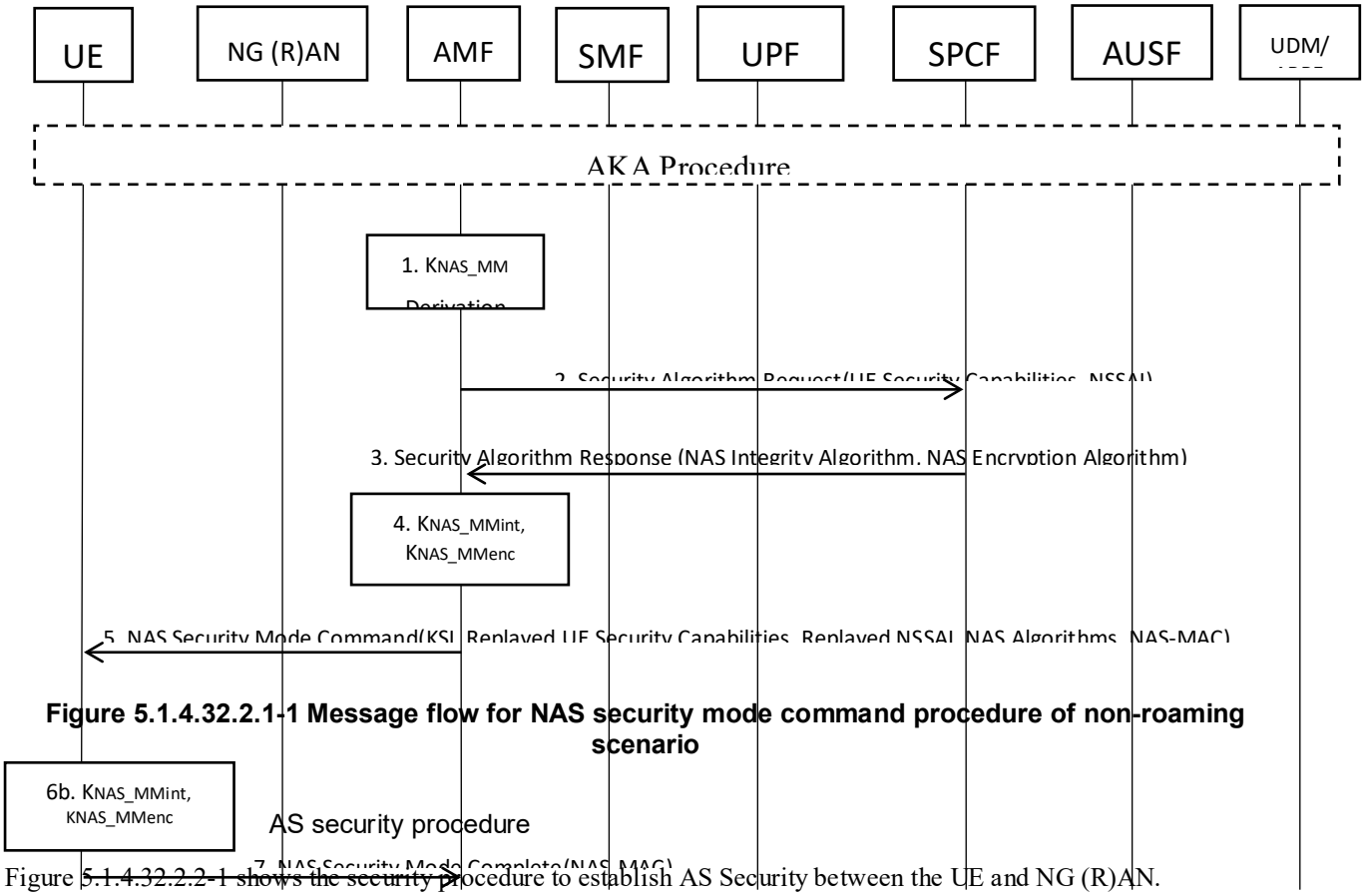
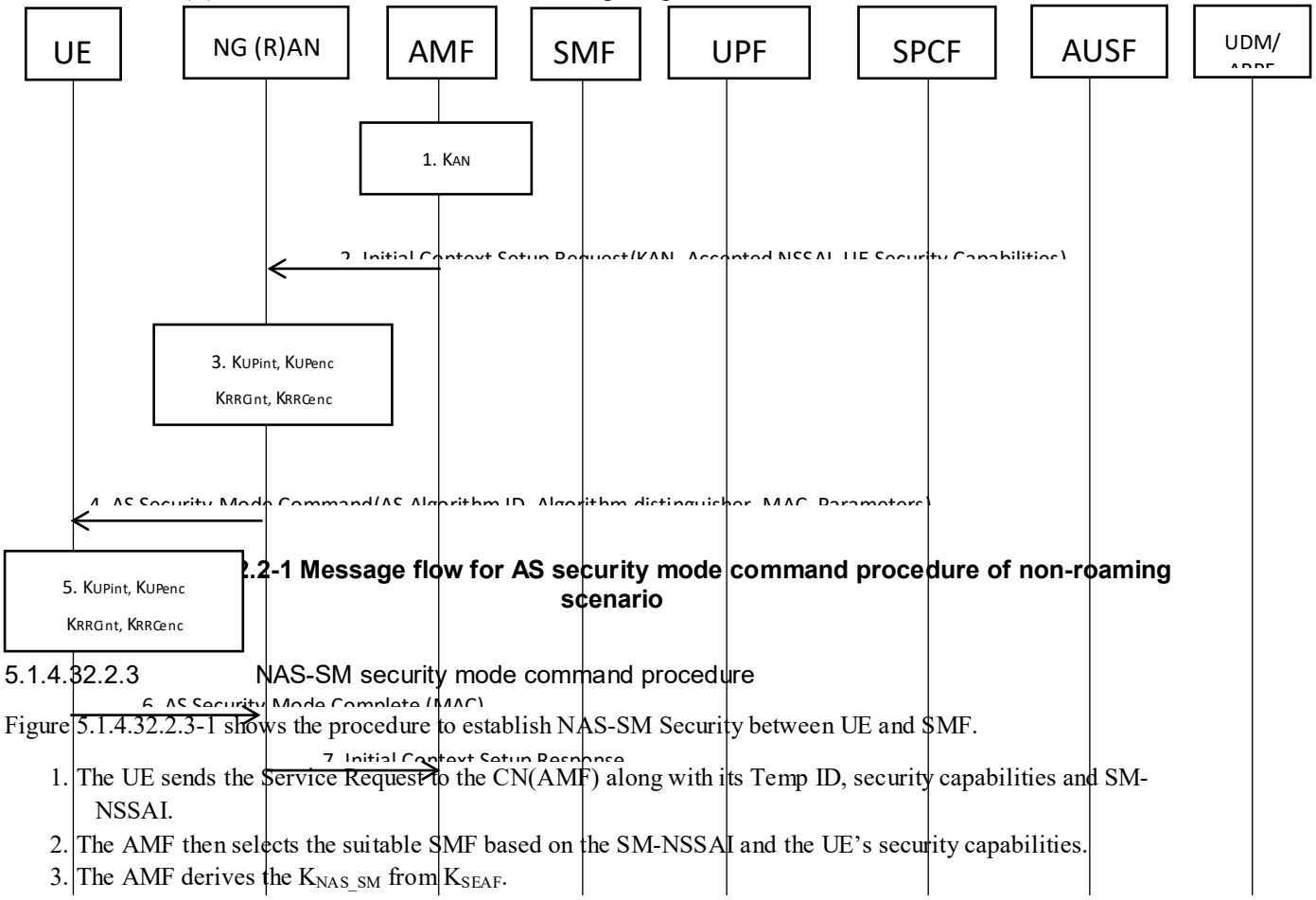


Figure 5.1.4.32.2.1-1 Message flow for NAS security mode command procedure of non-roaming scenario

Figure 5.1.4.32.2.2-1 shows the security procedure to establish AS Security between the UE and NG (R)AN.

Lenovo Ex. 1007
Page 123

8. The AMF derives K_{AN} from K_{SEAF}.
9. The AMF sends the Initial Context Setup Request(K_{AN}, Accepted NSSAI, UE Security Capabilities) to the NG (R)AN.
10. The NG (R)AN selects the algorithms for UP and RRC keys derivation and derives K_{UPint}, K_{UPenc}, K_{RRCint} and K_{RRCenc}.
11. The NG (R)AN sends the integrity protected AS Security Mode Command(AS algorithm ID, AS algorithm distinguisher, MAC) to the UE.
12. The UE derives the K_{AN} and corresponding RRC and UP integrity and encryption keys.
13. The UE then sends the AS SM Complete command along with MAC to authenticate the AS SMC message.
14. The NG (R)AN then sends the Initial Context Setup Response to the AMF.



2.2-1 Message flow for AS security mode command procedure of non-roaming scenario

5.1.4.32.2.3 NAS-SM security mode command procedure

Figure 5.1.4.32.2.3-1 shows the procedure to establish NAS-SM Security between UE and SMF.

1. The UE sends the Service Request to the CN(AMF) along with its Temp ID, security capabilities and SM-NSSAI.
2. The AMF then selects the suitable SMF based on the SM-NSSAI and the UE's security capabilities.
3. The AMF derives the K_{NAS_SM} from K_{SEAF}.
4. The AMF forwards the Service Request with the K_{NAS_SM} to the selected SMF.
5. If the SMF does not have the subscription data for the UE, it sends the Subscription Data Request to the UDM.
6. The UDM sends UE's subscription information to the SMF in the Subscription Data Response.
7. The SMF requests the algorithm for generating the NAS_SM integrity and encryption keys from the SPCF.
8. The SPCF sends the algorithm ID and distinguisher in the Security Algorithm Response to the SMF.
9. The SMF derives K_{NAS_SMint}, K_{NAS_SMenc} keys using the algorithms selected by the SPCF.
10. The SMF sends the NAS-SM Security Mode Command to the UE to the SMF via the AMF.
11. The UE derives K_{NAS_SM}, K_{NAS_SMint} and K_{NAS_SMenc} using the parameters it receives.
12. The UE then sends the NAS-SM Security Mode Complete(NAS_SM-MAC) to the SMF via the AMF.

Lenovo Ex. 1007
Page 124

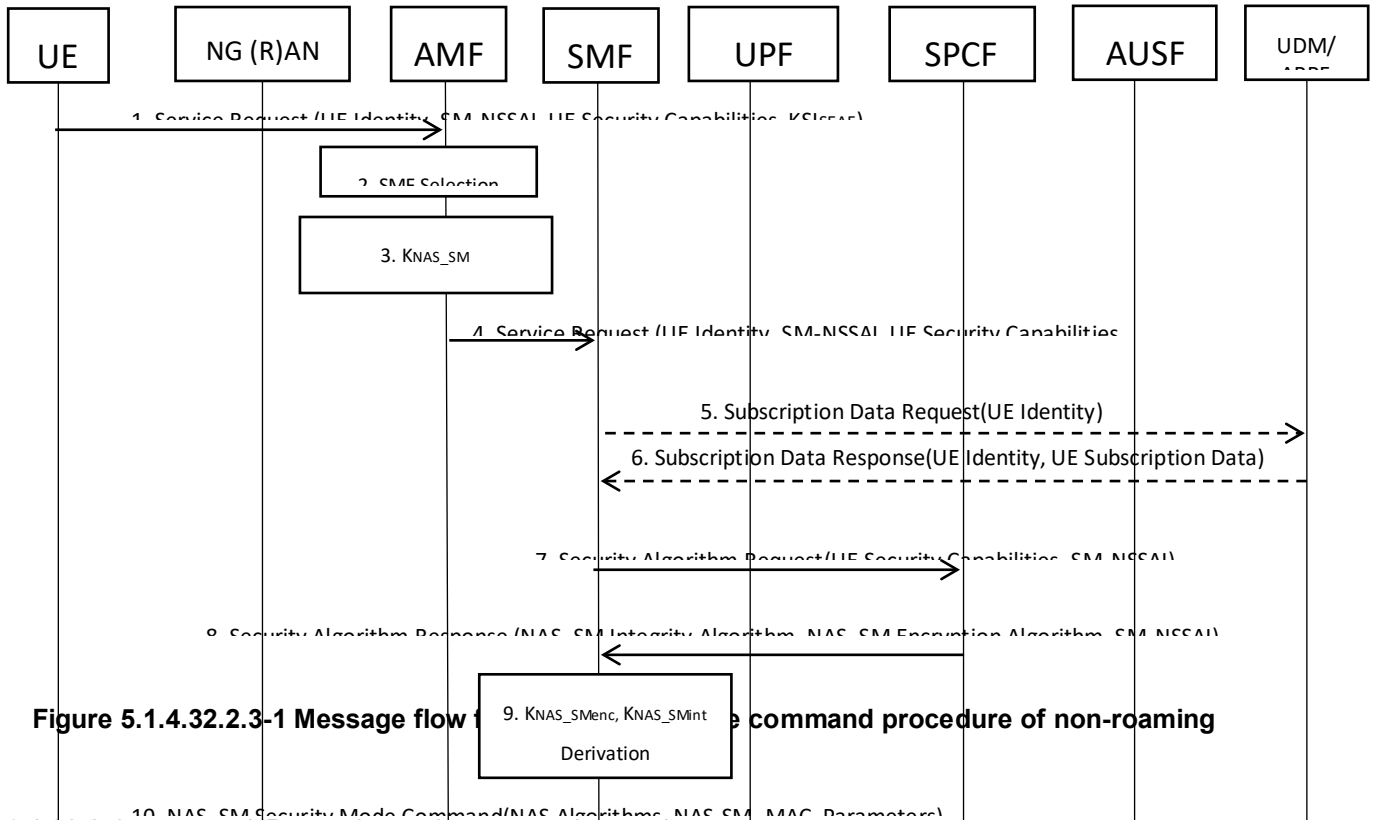
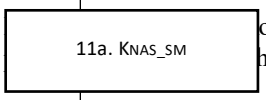
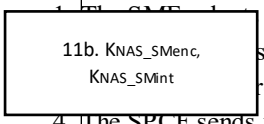


Figure 5.1.4.32.2.3-1 Message flow f… command procedure of non-roaming

5.1.4.32.2.4 UP security mode command procedure





…ows the procedure to establish UP Security between UE and UPF. The UP Security Mode …hen the UE requests to access a service (and a PDU session needs to be established).

1. The SMF selects the appropriate UPF for the requested service.
2. The SMF derives K_{UP}, the key for UP protection.
3. The SMF requests the algorithm for generating the UP keys from the SPCF.
4. The SPCF sends the algorithm ID and distinguisher in the Security Algorithm Response to the SMF.
5. The SMF derives Ksessint, Ksessenc keys using the algorithms selected by the SPCF.
6. The SMF sends the UP Security Mode Command to the UE via the AMF.
7. The UE derives K_{UP}, Ksessint and Ksessenc using the parameters it receives.
8. The UE then sends the UP Security Mode Complete(NS-MAC) to the SMF via the AMF.
9. The SMF then sends the Service Accept(Ksessint, Ksessenc) to the UPF to establish UP Security between UE and UPF.

Lenovo Ex. 1007
Page 125

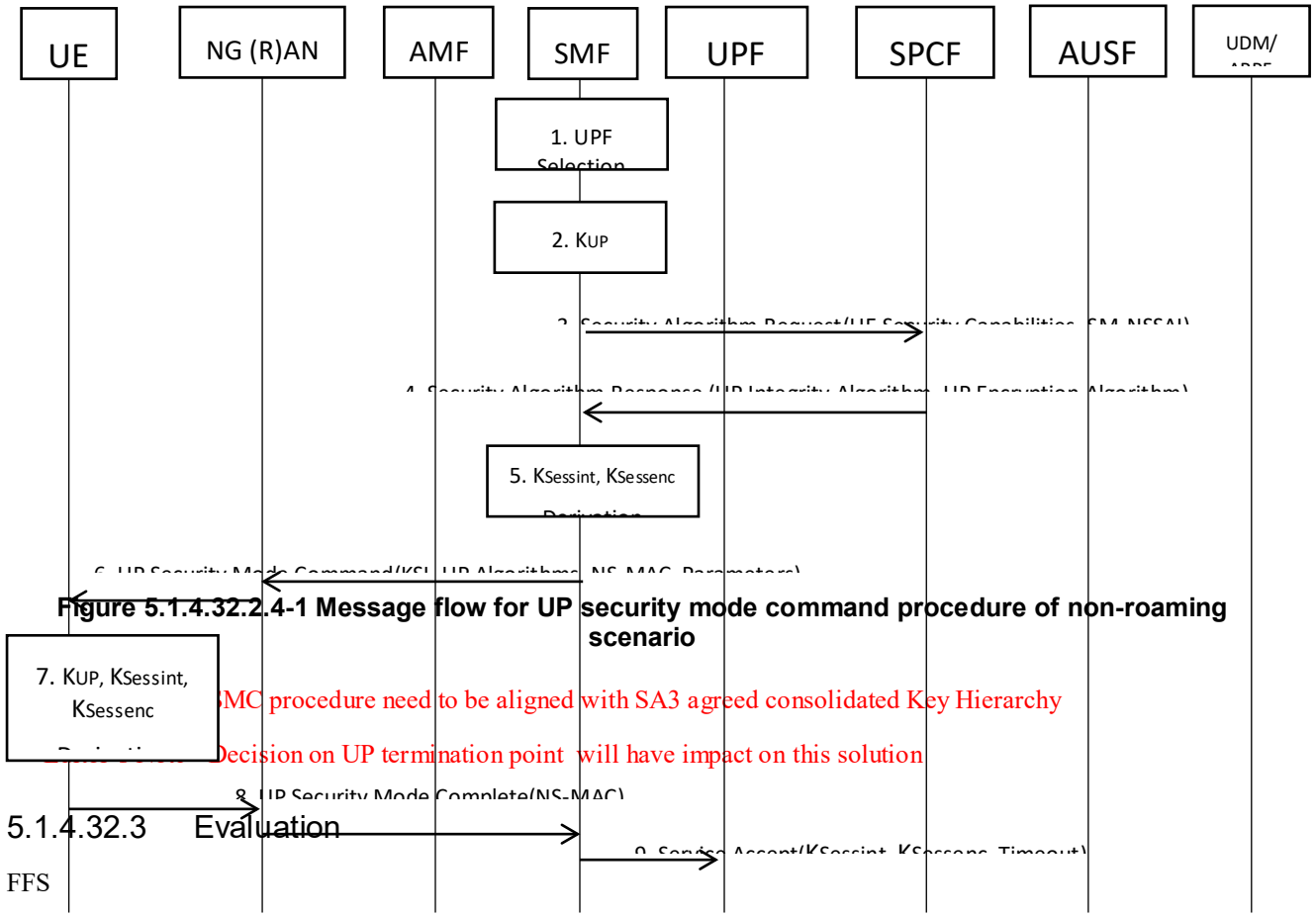


Figure 5.1.4.32.2.4-1 Message flow for UP security mode command procedure of non-roaming scenario

5.1.4.32.3 Evaluation

FFS

5.1.4.33 Solution #1.33: Consolidated Key hierarchy for NextGen

Editor's Note - Decision on Key Hierarchy Solution Options and variations will be based on SA3 agreement of Key Issues #1.4 and #1.7

5.1.4.33.1 Introduction

This pCR proposes two consolidated key hierarchy options for NextGen networks, incorporating key features of Key hierarchies proposed in solutions #1.4, #1.6, #1.8, #1.9, #8.7 and #8.8 in TR 33.899. This solution mainly addresses the requirements of Key Issue #1.7 Key Hierarchy. The potential requirements specified in Key Issue #1.7 clause 5.1.3.7.3 Potential security requirements are:

- Keys for confidentiality and integrity of control plane shall be provided
- Keys for confidentiality and integrity of user plane shall be provided
- Keys to support network slicing shall be provided
- Keys to support new radio (NR) shall be provided
- Keys to support non-3GPP RAT (Radio Access Technology) access shall be provided, such as the keys for
- ePDG in LTE.
- Keys to support backward compatibility with SAE/LTE shall be provided

5.1.4.33.2 Solution details

5.1.4.z.33.1 Architecture

Figure 5.1.4.33.2.1-1 describes the reference architecture for non-roaming scenario (copy of Figure 8.12.2-2 of version 2.0.0 of TR 23.799).

Lenovo Ex. 1007
Page 126

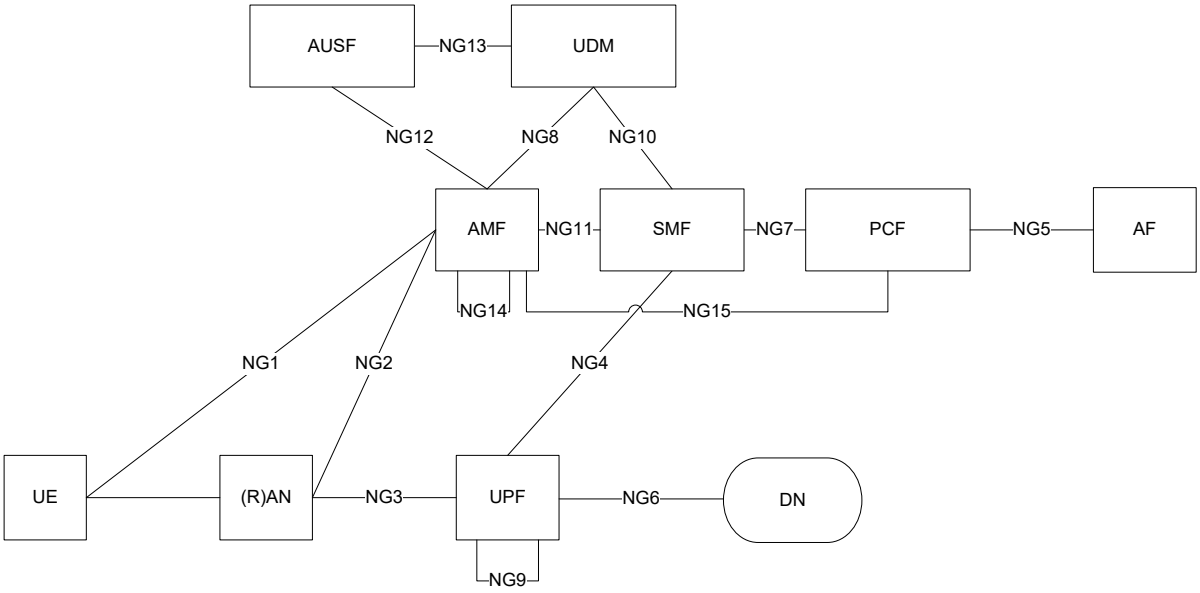


Figure 5.1.4.33.2.1-1: Reference architecture for non-roaming scenario

In the architecture, AMF (Access and Mobility Management Function) includes Security Anchor Function (SEAF) and Security Context Management Function (SCMF). SEAF is a function that performs UE authentication for connection via different access networks, and interacts with AUSF for retrieving authentication data stored in UDM (Unified Data Management). SCMF manages security context for both C-plane and U-plane functionality. The C-plane functions for MM and SM messages are decoupled and handled by AMF and SMF (Session Management Function), respectively, while U-plane data is handled by UPF. This functional split requires a new key hierarchy and a corresponding security and key derivation procedure. In addition, the generation of keys for network slicing in NextGen Systems is also required to be addressed by this key hierarchy.

5.1.4.33.2.2 Key Hierarchy

Key Issue #1.7 mentions the potential requirements for the key hierarchy for NextGen networks. This pCR proposes two variations of the consolidated key hierarchies, incorporating key features of solutions #1.4, #1.6, #1.8, #1.9, #8.7 and #8.8. The Key Hierarchies consist of the following keys. The justification for each key is given in detail in the evaluation section. The key hierarchies can be extended further if separate keys for RAN slices are required. In such a case, the K_{AN} can be slice-specific.

Lenovo Ex. 1007
Page 127

Table 5.1.4.33.2.2-1

K	The subscriber credential that is held in the UE and UDM.
K_{SEAF}	Security anchor key derived from K for authentication and derivation of subsequent keys.
K_{CP-CN_MM}	Control plane key commonly used for NAS MM messages (between the UE and the AMF) to derive integrity and encryption protection keys.
K_{SMF}	Control plane key provided for NAS SM messages (between the UE and the SMF) of each network slice to derive integrity and encryption protection keys.
K_{AN}/NH	Key provided to the AN to derive RRC and UP integrity and encryption protection keys.
K_{UP}	User plane key for UP provided for each network slice when the user plane security terminates at the UPF.
K_{AN_other}	Key for other NextGen AN than 3GPP.
K_{3GPP_AN}	Legacy key for existing 3GPP radio network.
$K_{non-3GPP\_AN}$	Legacy key for existing non-3GPP radio network.

This pCR proposes two consolidated key hierarchy options for NextGen networks, incorporating key features of all the current solutions in TR 33.899. Each of the consolidated key hierarchies consists of two variations.

Variation 1: K_{AN} is derived from K_{SEAF}.

Variation 2: K_{AN} is derived from K_{NAS_MM}.

5.1.4.33.2.2.1 Consolidated Key Hierarchy Option 1

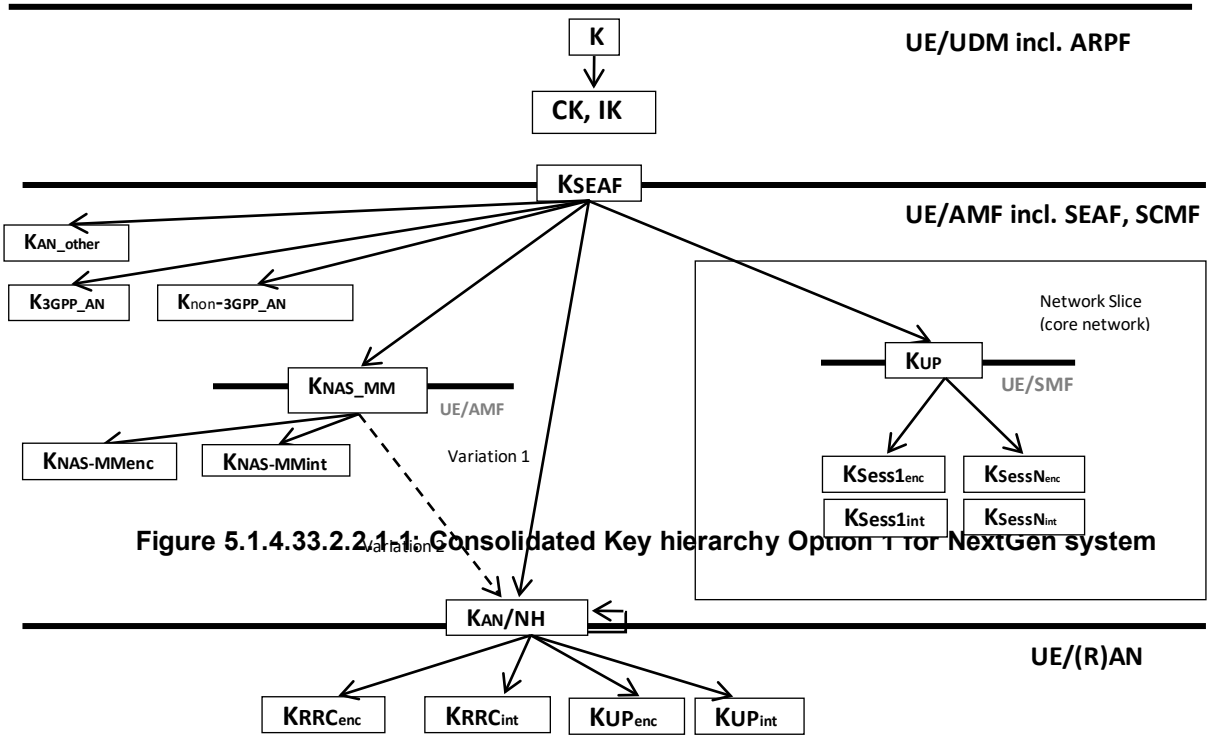


Figure 5.1.4.33.2.2.1-1: Consolidated Key hierarchy Option 1 for NextGen system

Lenovo Ex. 1007
Page 128

5.1.4.33.2.2.2 Consolidated Key Hierarchy Option 2

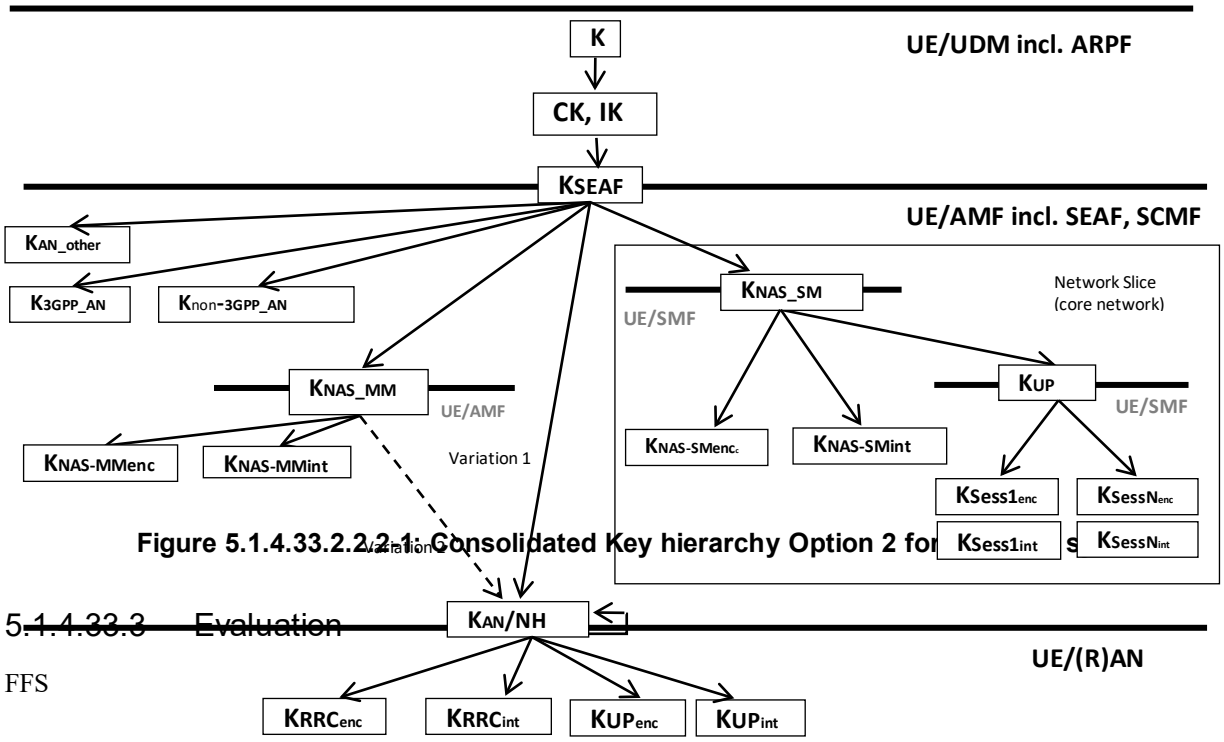


Figure 5.1.4.33.2.2.2-1: Consolidated Key hierarchy Option 2 for s

5.1.4.33.3 Evaluation

FFS

5.1.4.34 Solution #1.34: NextGen USIM

5.1.4.34.1 Introduction

As in previous 3GPP systems, the USIM is a valuable security anchor for security services in the UE. This solution proposes to extend the USIM functionality and platform for NextGen. It can be abbreviated as the "NextGen USIM".

This solution addresses the following key issues: 1.7: Key hierarchy, 1.8: UEs with Asymmetric Keys, 1.17: On-demand security policy, 2.1 Authentication framework, 2.2: Reducing the impact of secret key leakage, 2.3: Authentication identifiers and credentials, 2.5: Non-AKA-based authentication, 2.6: Efficient in energy consuming and reduced signalling for resource constraint environment, 2.8: Authentication of the user, 2.9: Security for service provider connection, 3.2: Refreshing keys, 3.3: Principles of security negotiation, 3.7: The storage of security context, 3.10: Trusted non-3GPP access, 4.1: AS security during RRC idle mode, 5.1: Secure storage and processing of credentials and identities, 6.2: Network authorization, 6.3: Authorization decoupled from authentication, 7.1: Refreshing of temporary subscription identifier, 7.2: Concealing permanent or long-term subscription identifier, 8.1: Security isolation of network slices, 8.3: Security on UEs' access to slices, 9.1: Mutual authentication of remote UE and network over a relay, 9.3: Remote UE session continuity, 11.1: Service-dependent security requirements, 11.3: User control of security, 11.4: On demand security framework, 12.2: Remote credential provisioning for IoT devices, 17.1: Cryptographic algorithms for backward compatibility and 17.2: Quantum safe cryptography.

5.1.4.34.2 Solution details

5.1.4.34.2.1 Overview

For the NextGen USIM, the current USIM functionality should be extended for the following:

- Extension of authentication command to cover new protocols with different size and message flows (such as EAP).
- Addition of the ability to verify the user for UE applications and network applications.
- Addition of mechanisms to allow long term key refresh (such as Ki).
- Addition of support for Asymmetric key cryptography.

Lenovo Ex. 1007
Page 129

5.1.4.34.2.2 Extension of authentication command to cover new protocols

Depending on the end to end authentication solution chosen, the 5G USIM should be updated to accommodate the new procedures and algorithms specified. This clause relates to key issues: 2.1 Authentication framework, 2.3: Authentication identifiers and credentials, 2.5: Non-AKA-based authentication and 5.1: Secure storage and processing of credentials and identities.

The current USIM has an AUTHENTICATE procedure specified in 3GPP TS 31.102[77] that is used by the UE to process authentication requests. This can be extended to include any of currently proposed solutions in the authentication clause of this TR. 3GPP TS 31.102 [77] will need to be updated to accommodate non-AKA authentication methods (if required).

The underlying AUTHENTICATE command is specified by ETSI 102 221 [78] and is extensible to any length of input and output so is still suitable for the new authentication methods chosen.

The new authentication mechanisms may require the use of public key cryptography which may impact the processing power and battery consumption required by the USIM.

5.1.4.34.2.3 Addition of the ability to verify the user for UE applications and network applications.

This clause extends details the extension of the USIM for user verification in NextGen. It relates to Key Issue 2.8: Authentication of the user.

The current USIM can identify a single "level 1" user and a "level 2" user by the correct input of numeric PINs of between 4 and 8 numbers.

The USIM user verification should be extended to enable the following:

- The ability to verify multiple users.
- The specification of additional, secure user verification methods.
- The ability to verify devices and applications to the USIM.

These methods may include:

- Username / password entry for user verification.
- Certificate verification for non-human access verification to the USIM.
- An API on the USIM that allows it to verify a user to a connected device.
- Procedures that allow different content to be made available securely to different users / non humans based on the user verification. ETSI has defined a specification ETSI TS 102 484[79] that could be used with the USIM for this purpose.

5.1.4.34.2.4 Addition of mechanisms to allow long term key refresh (such as Ki).

Solution 2.1 proposes a method that could be used to update the long term secret keys in the USIM. Solution 2.1 is focused on changing the authentication key, however this should also be extended to other key material in the USIM such as the OTA keys.

The USIM may implement this in one of many ways:

- be extended with new commands to achieve this key negotiation,
- use a specific implementation of the existing AUTHENTICATE command to negotiate the new keys,
- be extended with a new remote client to achieve this key negotiation (similar to the RAM in ETSI TS 102 226[76]) that uses the existing OTA protocol specified in ETSI TS 102 225[75].

Due to the improvement in security that this solution achieves, consideration should be given to defining a solution that could be equally usable on LTE and 2G.

Lenovo Ex. 1007
Page 130

5.1.4.34.2.6 Addition of support for Asymmetric key cryptography.

Asymmetric cryptography has been used in SIMs and USIMs for many years for non AKA purposes. This clause proposes that the USIM AUTHENTICATE command be extended to allow Asymmetric cryptography for Authentication and verification purposes as required by the solution choices made for NextGen.

The AUTHENTICATE command as specified in ETSI TS 102 221 [78] is currently suitable for this purpose.

5.1.4.34.3 Evaluation

FFS

5 1.4.35 Solution #1.35: Key management during AMF change

5.1.4.35.1 Introduction

This solution addresses key issues under the security area #1 such as KI #1.7, KI #1.14, as well as under the security area #4, i.e., KI # 4.9. The solution is based on the assumption that the SEAF is collocated with the AMF.

5.1.4.35.2 Solution details

5.1.4.35.2.1 General

The AMF is the termination point for NAS security. It is therefore assumed that AMF shares a key denoted by K_{CN} that is used to derive the NAS protocol keys for integrity and confidentiality protection. In this respect, the K_{CN} in NG Systems would be the equivalent to the K_{ASME} in EPS. It is always the case that following a new authentication procedure, a new K_{CN} is taken into use. Now, how the K_{CN} is derived after authentication is not in scope of this solution. The mechanisms described here work regardless of whether for example the K_{CN} is derived from a higher level key (K_{SEAF}) or directly like the K_{ASME}.

5.1.4.35.2.2 Key derivation

The NAS security context based on the K_{CN} is shared between the serving AMF and the UE. The security context will most likely include parameters similar to those in the legacy context such as the NAS counters, key set identifier. This solution provides a LTE-like horizontal key derivation mechanism to generate a new K_{CN} key during AMF change. The derivation of the new K_{CN} could be solely based on the previous K_{CN}.

From a security perspective, there is no benefit from an additional input in the key derivation step. However for efficiency reasons, there could be scenarios where an AMF needs to prepare in advance keys for more than one potential target AMFs. In that case, such an additional input parameter is needed for cryptographic separation. Depending on the type of this parameter, the UE might need to be provided with the chosen value alongside or as the notification that a key change has taken place. For example in case it is a nonce generated by the target AMF, it needs to be provided to the UE. However this would not be needed for a parameter that is available to the UE by other means such as an AMF public identifier-like parameter.

In this mechanism, it is assumed that such key derivation will rely solely on the old key. The resulting key chaining may go on until a new authentication is performed. In addition, the recommendation here is that it is per operator's policy how to configure the AMF in respect to which security mechanism is selected during an AMF change. Depending on an operator's security requirements, the operator can decide whether to have re-authentication at the target AMF or whether a key change is needed at the source AMF.

5.1.4.35.2.3 AMF change procedure

In the legacy systems, the security context is transferred unaltered to the target MME. In case an algorithm change is required at the NAS level, then the new algorithm is taken into use by a NAS SMC procedure. In fact the rule of thumb in EPS is that new NAS security parameters are always taken into use via an NAS SMC. Changing the used algorithm at the NAS protocol layer does not have any effect on the AN keys. However, changing the main NAS context key render the current AN keys outdated. Therefore, it is proposed that the new K_{CN} key is put into use during the handover such that the target gNB starts using AN keys derived from the new K_{CN}.

Lenovo Ex. 1007
Page 131

Figure 5.1.4.z.2.3-1 illustrates the additional steps based on the S1-handover procedure flow from TS 23.401 clause 5.5.1.2.2. Observe that the original flow was stripped of all irrelevant functions. It is then assumed that the NG2-based handover flow would be similar to the legacy one.

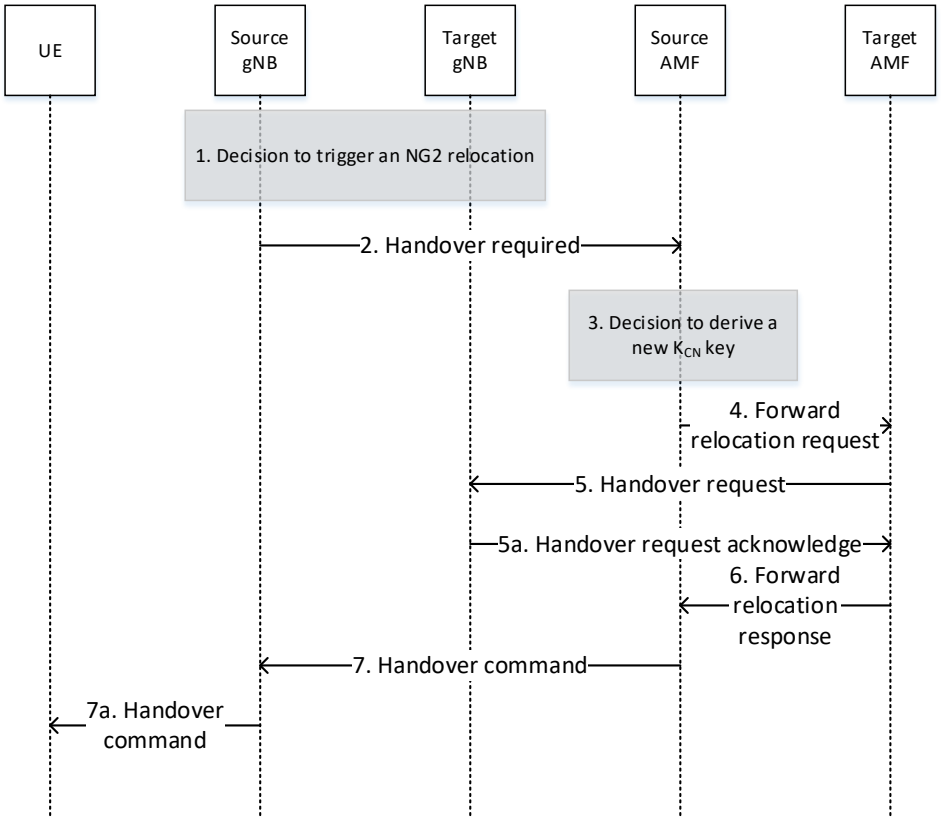


Figure 5.1.4.35.2.3-1: Updated NG2-based handover flow

1. The source gNB decides to intiate an NG2-based handover due to for example no Xn connectivity to the target gNB.

2. The source gNB sends a handover required message to the source AMF. This is the AMF currently serving the UE with which it is sharing a full NAS security context based on a K_{CN} key established possibly following a previous authentication or AMF change procedure.

3. The source AMF selects the target AMF and potentially based on an operator specific security policy decides to derive a new K_{CN} key in order to obtain backward security.

4. The source AMF sends a forward relocation request message including the new K_{CN} key alongside any relvant security parameters such as the UE capabilities. The target AMF uses this new key to set up a new security context and derive an AN key.

5. The target AMF sends a handover requet including the new AN key and all relevant security parameters such as the UE capabilities. This establishes the UE security context at the target gNB.

6. The target AMF sends a forward relocation response including a transparent container.

7. The source AMF sends a handover command message contained the relevant information from the forward relocation message and an indication that a new K_{CN} has been derived.

The UE then acts accordingly on the indication by deriving a new K_{CN} and AN keys.

For idle mobility the key change indication would be then provided to the UE during the NAS SMC procedure. The new AN keys will be derived and put to use when the UE moves to the RRC_CONNECTED like mode, i.e., after the next AS SMC procedure.

Lenovo Ex. 1007
Page 132

5.1.4.35.3 Evaluation

TBD

5 1.4.36 Solution #1.36: Security anchor function via primary AMFs

5.1.4.36.1 Introduction

This solution addresses KI #1.2. The solution is based on the assumption that the SEAF is collocated with the AMF.

5.1.4.36.2 Solution details

5.1.4.36.2.1 General

Editor's Note: A trust model supporting this solution is ffs.

The SEAF shares a key with the UE denoted by K_{SEAF}. This key is the result of the primary authentication procedure for network access between the UE and the AUSF via the SEAF/AMF. The K_{SEAF} is the equivalent of the K_{ASME} in the legacy systems and will serve as the root key for the derivation of the CN and AN keys. Whenever available, the K_{SEAF} could be used to avoid a full re-authentication. It is proposed then that the K_{SEAF} never leaves the AMF where the UE authenticates.

5.1.4.36.2.2 Role assignment

Abusing terminology, the term MMF is used here to refer to the non-SEAF role part of the AMF. Now from the UE perspective, an AMF could endorse the role of the SEAF, the role of the MMF or both. When the UE authenticates first with a particular AMF, that AMF endorses both roles. Such an AMF will be henceforth referred to as the primary AMF (of the UE). When the UE later moves to another target AMF (e.g. in case of a mobility event), the target AMF endorses only the role of the MMF while the primary AMF endorses the role of the SEAF. If a UE is re-authenticated by other than the primary AMF, then the new AMF becomes the primary one and a new K_{SEAF} is taken into use.

The primary AMF will always be in possession of the K_{SEAF} until the UE authenticates somewhere else. The serving AMF will always have the CN key (key used for deriving the NAS keys). Therefore, for any UE, it can be the case that two different AMFs are involved in maintaining and sharing some form of a security context with the same UE. The primary AMF will maintain the SEAF context based on the K_{SEAF} and the serving AMF the CN security context. The UE maintains both contexts. Observe that it is possible that the primary AMF is also the serving AMF in that case it maintains both contexts. In order for this to work, some form of an additional AMF identifier must be included in the CN security context to identify the Primary AMF for example this could be an additional GUTI-like. In the remainder of the description, such an identifier is referred to as the Primary GUTI (PGUTI).

5.1.4.36.2.3 Security context handling during AMF change

An AMF change could occur during mobility events. In legacy systems, the security context is transferred between the MMEs. In NG systems, there will be always some kind of context transfer between the target and source AMF. However, for the security aspect, several scenarios are possible depending on which security parameters are transferred and how they are taken into use. During system operations, which decision the new AMF takes could be based on a security policy for example depending on the location of the old AMF and the primary AMF.

The following clauses show different options to realize the security context handling during AMF change. Mind that the old AMF in the included figures may be the primary AMF or it could be separate one (as shown in the figures) as a result of mobility procedure based on any of the alternatives shown.

5.1.4.36.2.3.1 Scenario #1: Re-authentication

The new AMF decides to run a new authentication as illustrated in Figure 5.1.4.36.2.3.1-1.

Lenovo Ex. 1007
Page 133

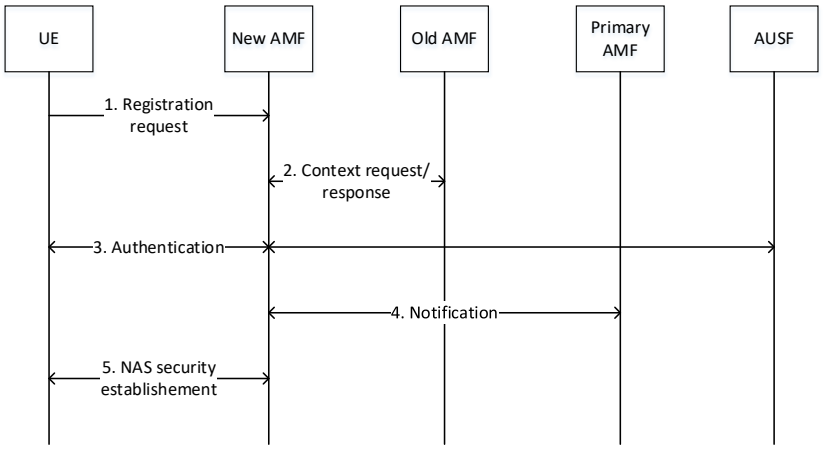


Figure 5.1.4.36.2.3.1-1: re-authentication during an AMF change

1. The UE sends a registration request. The UE registration should include any necessary information from the current NAS security context in order for the new AMF to be able to identify the old serving AMF..

2. The new AMF sends a context request to the old AMF which does reply accordingly. The context includes the additional PGUTI parameter which identifies the Primary AMF.

3. The new AMF decides to run a new authentication leading to the establishment of a new K_{SEAF}. As a consequence, the new AMF becomes the primary AMF for this UE. As a consequence, a new K_{SEAF} is established. The corresponding PGUTI could be for example chosen to be the first GUTI allocated by this new AMF. As the PGUTI is sent over the air and is only passed between AMFs there is no need for dedicated reallocation procedures.

4. The new AMF may optionally notify the primary AMF so that the latter can safely dispose of the old K_{SEAF} and the corresponding security context. In order to avoid such additional signalling, it could the case that a SEAF context is only maintained for a certain period of time once the UE leaves the primary AMF. In this manner, the data will be removed automatically once the defined period elapses.

5. A new CN key is derived and then taken into use via an SMC like procedure between the new AMF and the UE.

5.1.4.36.2.3.2 Scenario #2: Key transfer

The new AMF requests the security context from the old AMF which sends the current CN key. This scenario would not require any interaction with the primary AMF and is similar to the legacy mechanism as illustrated in Figure 5.1.4.36.2.3.2-1.

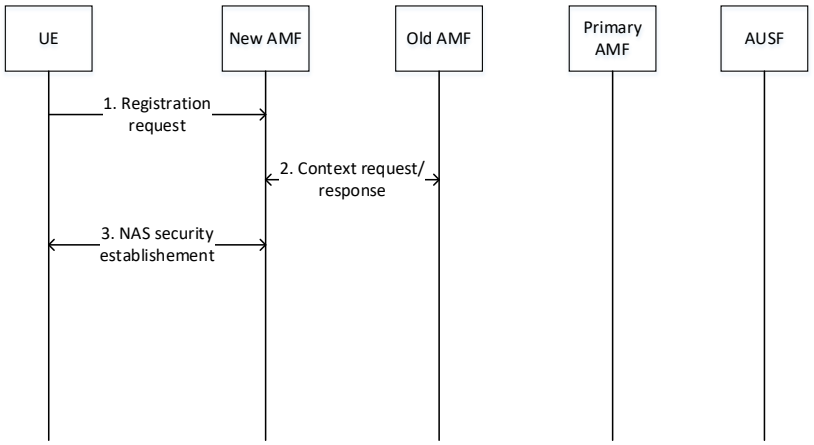


Figure 5.1.4.36.2.3.2-1: CN key transfer during AMF change

1. The UE sends a registration request. The UE registration should include any necessary information from the current NAS security context in order for the new AMF to be able to identify the old serving AMF..

Lenovo Ex. 1007
Page 134

2. The new AMF sends a context request to the old AMF which does reply accordingly. The context includes the additional PGUTI parameter which identifies the Primary AMF.

3. In case an algorithm change is required by the new AMF, then an SMC like procedure is run in order to take the selected algorithms into use.

5.1.4.36.2.3.3 Scenario #3: Horizontal key derivation

The new AMF requests the security context from the old AMF but the old AMF derives a new CN key from the current one and sends that instead as described in solution #1.35.

5.1.4.36.2.3.4 Scenario #4: Vertical key derivation

The new AMF requests a new key from the primary AMF as illustrated in Figure 5.1.4.36.2.3.4-1.

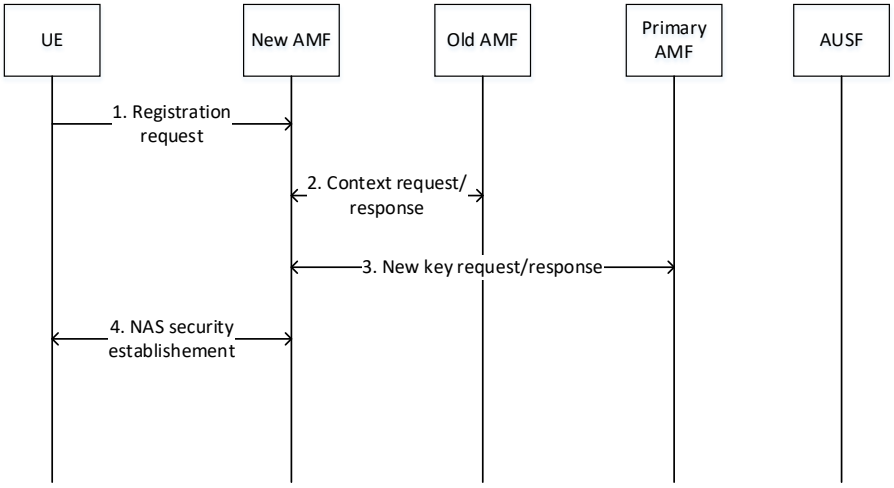


Figure 5.1.4.36.2.3.4-1: vertical key derivation during AMF change

1. The UE sends a registration request. The UE registration should include any necessary information from the current NAS security context in order for the new AMF to be able to identify the old serving AMF..

2. The new AMF sends a context request to the old AMF which does reply accordingly. The context includes the additional PGUTI parameter which identifies the Primary AMF

3. The new AMF sends a key request to the primary AMF identified by the PGUTI and the primary AMF acts accordingly by deriving a new K_{CN} from the current K_{SEAF} and including it in the reply. The derivation of this K_{CN} could be based on a freshness parameter that is included in the reply as well and provisioned to the UE in step 4.

4. The new CN key is taken into use via an SMC like procedure between the new AMF and the UE.

5.1.4.36.3 Evaluation

TBD

5.1.4.37 Solution #1.37: Protecting the initial NAS message

5.1.4.37.1 Introduction

This solution addresses Key Issue #1.5 and #1.6 for initial NAS messages.

5.1.4.37.2 Solution details

If the UE does not have a security context when wanting to send an initial NAS message (that is the first NAS message sent after the NAS connection by a NG-UE leaving Idle), the NG-UE only sends a short message that contains only the information necessary for the network to establish a security context (e.g. UE identifier, UE security capabilities). This

Lenovo Ex. 1007
Page 135

enables the network to establish a secure connection (by authenticating the UE and running the Security Mode procedure) with the NG-UE and then the NG-UE to send the initial message fully protected. To optimise the signalling, the 5G equivalent of the NAS security mode complete message is proposed to carry the fully protected initial message.

If the NG-UE has a security context, the NG-UE sends the same information along with the initial NAS message to the network. All this information is integrity protected with the security context that the NG-UE has but only the initialmessage is confidentiality protected. If the network has the same security context as the NG-UE, then the network can check its integrity protection and retrieve the initial NAS message. If this is successful, the network may responds to the initial NAS message without further security procedures. Of course the network may refresh the NAS security if desired. If the network does not have the security context or the integrity check fails, then the network can use the data that is received in clear to authenticate the UE and establish the security as above, and to get the NG-UE to send the initial NAS message in the 5G equivalent of the NAS security mode complete as above. Figure 5.1.4.37.2-1 describes the flows for this but for simplicity only considers the messages between the NG-UE and AMF.

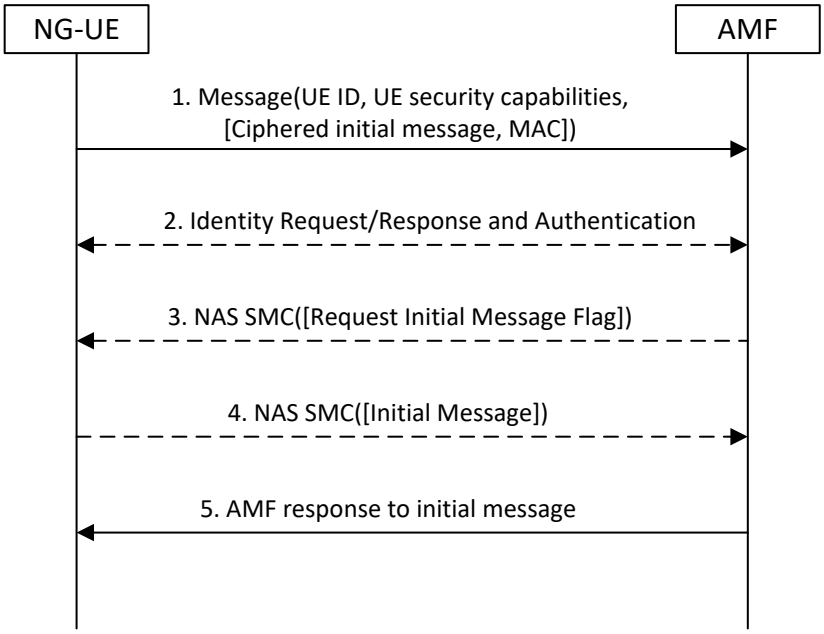


Figure 5.1.4.37.2-1: Protecting initial NAS messages

Step 1: The UE sends the UE ID and UE security capabilities to the AMF. If it has a security context, it in addition sends the initial NAS message ciphered using the security context and integrity protects the whole sent message using the security context.

Step 2: If the AMF does not have the security context or if the integrity check fails, then the AMF initiates an authentication procedure with the UE. This may involve some identity request procedures if the UE gave a temporary identity in the step 1. The AMF may also initiates an authentication procedure with the UE even if the integrity check passed.

Step 3: After a successful authentication of the NG-UE, the AMF sends the NAS security mode command including a request for the initial NAS message, if it was not included in step 1 or the network has failed to verify the integrity of the initial NAS message.

Step 4: The UE sends the NAS security mode complete to the network. This message is ciphered and integrity protected and includes the initial NAS message if requested by the network in the NAS security mode command message.

Step 5: The AMF sends its response to the initial NAS message. This message is ciphered and integrity protected.

5.1.4.37.3 Evaluation

TBD

Lenovo Ex. 1007
Page 136

5.1.4.38 Solution #1.38: Detection and response function for signalling attacks

5.1.4.38.1 Introduction

This solution addresses key issues #1.21, #2.7, #8.1, and #8.3.

The solution proposes to expand the AMF with a signalling attack detection and response function that can detect signalling attacks and send a signalling message to the UE to stop certain actions or to rate limit some types of requests or actions.

5.1.4.38.2 Solution details

The general principle of this solution works as follows. Below is a figure of a UE requesting a service for which the counter / threshold has not yet been met. The service will be granted according to the flow below:

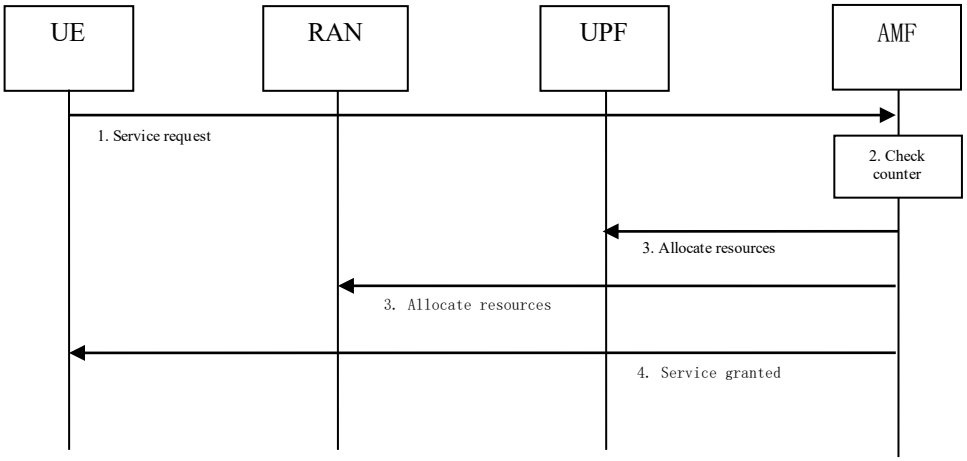


Figure 5.1.4.z.2-1: Service request and grant flow

The steps are as follows:

1. The UE requests a service. This could be a request for a voice call, a new data bearer or access to a new slice or even an attach message

2. The AMF receives the request and checks whether this UE is behaving normally and whether the service can be granted. The AMF also sets a timer and a counter in order to detect the next service request.

3. If the AMF finds no reason to deny the request, the AMF assigns the resources and grants the service to the UE (which is indicated with step 4).

In case that this UE has been requesting and terminating many services in a short period of time, the counter or threshold will be met at some point in time. The AMF will then deny access to the specific service and/or tell the UE to refrain from asking further services for a period of time. The flow will look as follows:

Lenovo Ex. 1007
Page 137

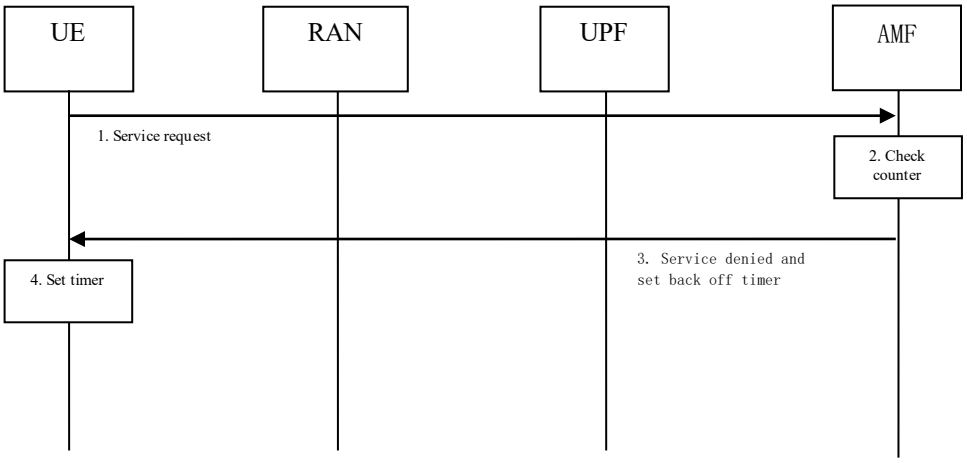


Figure 5.1.4.z.2-2: Service request and deny flow

1. The UE requests a service.

2. The AMF receives the request and finds that the UE is over the threshold for service requests.

3. The AMF sends back a service request denied and instructs the UE to stay away for a certain amount of time. This back off timer could be service type specific so that other services can still be requested.

4. The UE receives the service denied and sets the timer to refrain from further service requests (of that particular type).

The AMF will also set a timer and reset the UE state back to normal whenever that timer has expired.

5.1.4.38.3 Evaluation

This solution has the following merits:

- It solves the key issues #1.y, #2.7, #8.1, and #8.3 by threshold based detection on a per UE bases and extending the LTE back off timer mechanism to be specific for a UE and optionally specific to a service;
- Other UEs, not taking part in a denial of service, will not be affected by this type of selective and discriminatory congestion control measures because only infected UEs will be denied service.
- For authenticated UEs, it allows the AMF to detect which UEs are malbehaving so that selective action can be taken;
- The detection can be relatively simple and yet effective.

This solution has the following drawbacks:

- The AMF will have to keep track of each UEs service requests and timers, possibly organized by service request type which will require storage;
- It is unlikely that UEs of which the baseband processor is infected will comply with the back off timers.

5.1.4.39 Solution #1.39: Flexible UP Termination Point with LTE compatibility

5.1.4.39.1 Introduction

This solution addresses Key Issue#1.15 – Termination point of UP security.

The Next Gen system will co-exist with at least the LTE system for many years. For many network operators, the 5G RAN will be connected to the LTE core network (see 3GPP TR 38.801 [72]). Because of this, any flexible UP security termination point will also need to work with an LTE core.

This solution proposes 2 ways of implementing a flexible Termination point that is LTE core compatible.

Lenovo Ex. 1007
Page 138

5.1.4.39.2 Solution details

5.1.4.39.2.1 Overview

The two solutions described are:

- Flexible UP Security Termination based on Option 3x (in 3GPP TR 38.801 [72]).
- Flexible UP Security Termination based on Option 3a (in 3GPP TR 38.801 [72]).

5.1.4.39.2.2 Flexible UP Security Termination based on Option 3x

Option 3x in 3GPP TR 38.801 [72] clause 10.1.2.4 describes how the PDCP may be moved into a centralised data centre without fundament changes to the RAN protocol stack and in a way that is compatible with LTE. In this solution the PDCP is the security termination point for the User Plane (as it is for LTE).

This solution allows the network operator to either have the PDCP in the RAN site or a secure location near the Core Network. It also allows different network slices to have the PDCP in different locations.

The advantage of 3x over 3a for security is that the data is not tromboned between the master eNB, secondary eNB via the Core network reducing the attack surface for this interface.

5.1.4.39.2.3 Flexible UP Security Termination based on Option 3a

Option 3a in 3GPP TR 38.801 [72] clause 7.2 describes how the PDCP may be moved into a centralised data centre without fundament changes to the RAN protocol stack and in a way that is compatible with LTE. In this solution the PDCP is the security termination point for the User Plane (as it is for LTE).

This solution allows the network operator to either have the PDCP in the RAN site or a secure location near the Core Network. It also allows different network slices to have the PDCP in different locations.

5.1.4.39.3 Evaluation

5.1.4.z Solution #1.z: <solution name>

5.1.4.z.1 Introduction

Editor's note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the security area.

5.1.4.z.2 Solution details

5.1.4.z.3 Evaluation

5.1.5 Conclusions

Editor's note: This clause will contain the evaluation between the solutions, and the conclusions made by SA3.

Lenovo Ex. 1007
Page 139

5.2 Security area #2: Authentication

5.2.1 Introduction

5.2.1.1 General

This security area covers authentication between UE and 3GPP network. Authentication between 3GPP network elements or - as far as applicable - between 3GPP entities and non-3GPP entities are dealt with in other clauses.

NOTE: Examples of authentication between 3GPP network elements are backhaul link security and network domain security between core network elements. Examples of authentication between 3GPP entities and non-3GPP entities covered in 3GPP specifications are the MB2 interface in MBMS or the Tsp interface in MTC.

The support of a novel set of use cases in Next Generation network requires to consider more efficient options for authentication to address all the authentication scenarios.

Some security requirements related to the authentication aspects have been provided in 3GPP as part of the Feasibility Study on New Services and Markets Technology Enablers for Massive Internet of Things [3]. Here the support of a resource efficient mechanism to authenticate a device, when the device is in indirect 3GPP connection mode is required. Also an appropriate and efficient authentication mechanism for groups of IoT devices is requested.

Authentication aspects related to the support of multiple access network by NextGen have been also considered in [6]. In this context it is required that NextGen system is able to support authentication to access NextGen network through a non-3GPP access using 3GPP credentials. Further, the security architecture of Next Generation System needs to provide means to handle authentication and security credentials towards Authentication Framework, supporting multi-RATs including non-3GPP. Signalling overhead and latency for authentication needs to be minimised

This security area includes the study of resilience against single points of major failure in authentication. The LTE security model is strong against what might be called traditional attacks. But a broader set ofattacks can be considered. One example is if the attacker attempts to learn the long term secret key directly, either via an attack on some part of the provisioning flow, or via an attack on the USIM. Another example is if an attacker can observe session keys sent between operator core network nodes. If either of these attacks is successful, they undermine the normal LTE security model. This section deals with ways in which authentication in NextGen systems could be made more robust, so that the impact of some attacks is removed or reduced.

The UE to network perspective can further be characterized as follows:

- Subscription perspective: This is the traditional way of focusing on authenticating the identifier and the related subscription. This study area should clarify how the subscription is authenticated towards to network. Subscription authentication would need to be used over different accesses. TR 23.799 [2] mentions several access types for Next Generation systems which each could be studied from authentication point of view, e.g. authentication over Next Generation RAT(s), eLTE, and non-3GPP access (e.g. WLAN, or fixed access). Furthermore, the efficiency of subscription authentication should be taken into account under this security area (even tough authentication procedure may contribute very little to the total overhead of security signalling). Also, the UE may need to authenticate itself towards several networks as is currently described in TR 23.799 Annex D on Potential solution scenarios for support of multiple slices per UE. Finally, TR 22.891 [7] includes requirements for exchange of frequent and infrequent small bursts of data as well as large amounts of data without a lengthy and signalling intensive bearer establishment and authentication procedure.

Editor's note: Device perspective: TR 22.864 [6] describes scenarios where secure mechanism is needed for unique device identifiers that are stored in a secure and tamper resistant manner on the device. Authentication of the device identifier could be further studied. The network to UE perspective can further be characterized as follows:

- Authentication of the network towards the UE: In the LTE authentication model, the freshness of the authentication challenges are verified (cf. SQN), the network side approves that it knows the long term secret (cf. Ki), and the master key (cf. Kasme) created during the process is cryptographically bind to the identity of the access security management entity. The secondary security association between the UE and the RAN (cf. AS security) is bootstrapped from the primary security association. There is no real authentication between the UE and the RAN. The model has approved to be efficient, and secure, however, the number of security end-points in the network side may change in the Next Generation systems (e.g. UEs accessing multiple core network

Lenovo Ex. 1007
Page 140

instances possibly via a shared RAN as described in TR 23.799 [2]). This security area should clarify which network(s) is (are) authenticated towards the UE and how.

- Equipment perspective: TR 22.864 [6] describes scenarios where secure mechanism is needed for an authorized entity to disable/re-enable from normal operation of a device reported as stolen/found. This clearly implies a need for the device to be able to verify that the disable and re-enable commands come from an authorized party.

The UE to UE perspective and the network to network perspective are covered in different security areas.

This scope of this security area covers the following:

1) Aspects related to the types of credentials, storage, and identifiers

Editor's Note: The aspects of non-3GPP credentials and non-3GPP identifiers need clarification.

- Authentication using 3GPP credentials, storage of those credentials and subscription identifiers: USIM based credentials are currently the only way of authentication in 3GPP systems. There are several reasons for this. Firstly, the USIM provides a secure storage for the permanent identifier and credentials. Secondly, the permanent identities need to be routable to the home network if the UE is roaming in a visited network forming the foundation to the roaming model. Thirdly, the USIM guarantees the international interoperability.

- Authentication using non-3GPP credentials, storage of those credentials and identifiers: TR 22.862 [4] describes a use case in which the network access security (including the identity management and authentication) used in an industrial factory deployment is provided and managed by the factory owner. TR 22.862 states explicitly that "The 3GPP system shall support an authentication process that can handle alternative authentication methods with different types of credentials to allow for different deployment scenarios such as industrial factory automation." This security area should clarify what those non-3GPP credentials could be, how they should be stored, and if there are any requirements for the use of non-3GPP identifiers in Next Generation systems (e.g. related to roaming).

- Credential types related to networks could also be studied. For example, if the subscription is authenticated using non-3GPP credentials, the network would also need alternative credentials towards the UE.

2) Aspects related to the authentication methods and key agreement:

Editor's Note: The aspects of alternative to AKA need clarification.

- Authentication and Key Agreement (AKA), and its potential enhancements: This security area should clarify if it can be expected that the legacy AKA needs to be supported by the Next Generation systems in order to provide backwards compatibility to eLTE. However, this study could potentially also further study enhancements to the legacy AKA, e.g. enhancements to the actual AKA framework implemented in HSS and UICC or enhancements to the protocol exchange between the UE and access security management entity.

- Alternatives to AKA: This security area should study potential alternatives to AKA or its enhancements. This security area could study how the alternative methods could be integrated to 3GPP protocols in an unified way, and clarify what kind of interoperability and roaming requirements are assumed from the alternative authentication methods. For example, it should be clarified if the alternative authentication methods need to have a key generation capability creating a master key (cf. Kasme) to be used to protect the subsequent communication between the parties. Furthermore, if the EUTRA needs to be supported with the alternative authentication methods, the LTE-like interface towards the radio network would need to be supported. These may set requirements to the way alternative authentication methods are integrated to Next Generation system.

5.2.1.2 Authentication-related functions

In the following, four authentication-related functions in the core network are defined:

- Authentication Credential Repository and Processing Function (ARPF)

- Authentication Server Function (AUSF)

- Security Anchor Function (SEAF)

- Security Context Management Function (SCMF)The interaction of all four functions is required to provide authentication between the NG-UE and the NG 3GPP network.

Lenovo Ex. 1007
Page 141

Authentication Credential Repository and Processing Function (ARPF)

This function stores the long-term security credentials used in authentication and executes any cryptographic algorithms that use the long-term security credentials as input. It also stores the (security-related part of the) subscriber profile. The ARPF shall reside in a secure environment in an operator's Home Network or a 3rd party system, which is not exposed to unauthorized physical access. The ARPF interacts with the AUSF.

Examples:

- Long term-security credentials include shared permanent secrets such as the key K in EPS AKA or EAP-AKA.
- In the case of AKA-based authentication (EPS AKA or EAP-AKA or EAP-AKA'), the ARPF generates the authentication vectors. The 4G-equivalent of the reference point between ARPF and AUSF in EPS would be SWx for non-3GPP access to the EPC, while it would be undefined for 3GPP access to the EPC as it would be HSS-internal.

Editor's Note: It is ffs whether authentication methods based on public-key mechanisms will be used in NextGen.

Editor's Note: It is ffs whether the secure environment, in which the ARPF resides, shall be required to be tamper-resistant.

Authentication Server Function (AUSF)

An authentication function that interacts with the ARPF and terminates requests from the SEAF. The AUSF shall reside in a secure environment in an operator's network or a 3rd party system, which is not exposed to unauthorized physical access. In SA2's architecture in TS 23.501, the ARPF is part of the UDM.

An interface between AUSF and UDM, namely N13, is defined in TS 23.501 for retrieving subscriber profile information. Regarding a split for authentication functionality, an interface between AUSF and ARPF shall be defined for the case of EAP-AKA and EAP-AKA'. In this case, the interface description shall be modelled after SWx, the interface between 3GPP AAA server and HSS defined in TS 23.402. For other authentication protocols, no split for authentication functionality will be standardized in 5G phase 1.

NOTE: RFCs for EAP methods generally describe the role of the EAP server, without distinguishing between the roles of AUSF and ARPF as described in the present document.

Examples:

- In the case of EAP-based authentication, the AUSF performs the function of the EAP server. In the case of EPS AKA, the AUSF is part of the functions that today are performed by the HSS; it could be compared to the function of an HSS frontend in 4G; HSS-internal reference points are not standardized today.
- In the case EPS AKA was adopted in NextGen, the comparison of RES and XRES would be done in the SEAF.
- The AUSF may also assume the role of a AAA proxy that forwards authentication messages.

Security Anchor Function (SEAF)

An authentication function in the core network that interacts with the AUSF and the NG-UE and receives from the AUSF the intermediate key that was established as a result of the NG-UE authentication process. The SEAF also interacts with the Mobility Management (MM) function, e.g. during initial Attach, and with the SCMF. The SEAF shall reside in a secure environment in an operator's network, which is not exposed to unauthorized physical access. In the roaming case, an SEAF resides in the visited network. The intermediate key sent to the SEAF in the visited network shall be specific to the visited network.

Examples:

- In the case of EPS AKA, the SEAF receives the intermediate key KASME from the AUSF. In the case of EAP-based authentication, the SEAF takes the authenticator role from the point of view of the UE and the AUSF (*) and receives the intermediate key MSK from the AUSF. The 4G-equivalent of the SEAF for non-3GPP access to the EPC resides in the ePDG for untrusted access, while the TWAN provides an example for trusted access.

Lenovo Ex. 1007
Page 142

- (*) This formulation has been chosen deliberately: It is conceivable that a function between the NG-UE and the SEAF, e.g. a WLAN access point, believes to play the role of EAP authenticator and receive the MSK, while in fact it receives a key from the SEAF or SCMF derived from the MSK. This possibility is ffs.

Editor's Note: It is ffs whether the SEAF can only reside in the visited network, or whether in addition, there may be scenarios where an SEAF resides in the visited network and another SEAF in the home network in case of roaming. A potential advantage of having the SEAF in the home network in the roaming case could be avoiding full re-authentication when the UE moves and the serving network changes; but this aspect is also ffs. This editor's note will be resolved once the question in Annex E.2.0.1.1 is answered.

NOTE: The key K_{ASME} in EPS AKA and the key MSK in EAP-AKA' are specific to the network, to which they are delivered.

Security Context Management Function (SCMF)

The SCMF receives a key from the SEAF that it uses to derive further (e.g., access-network specific) keys. The SCMF shall reside in a secure environment in an operator's network, which is not exposed to unauthorized physical access. In the roaming case, the SCMF resides in the visited network.

Editor's Note: It is ffs whether the SCMF is needed as a separate function or whether it can always be co-located with the SEAF.

Editor's Note: It is ffs whether an additional function needs to be defined that reflects the role of an ERP server in EAP.

NOTE: Nothing in the above definitions is meant to limit the deployments of these functions in a virtualised environment. The term "secure environment" does not necessarily imply tamper-resistance.

Security policy control function (SPCF)

The SPCF provides the security policy based on service application applicable to security policy negotiation e.g. UP protection negotiation. Security policy negotiation may be based on the following information: security capabilities of UE, security capabilities of network/network slice and security policy based on service application. SPCF may distribute the security policy based on service application to the network entities (e.g. SMF, AMF) and/or to the UE. The SPCF shall reside in a secure environment in an operator's network, which is not exposed to unauthorized physical access. The SPCF could be standalone or co-located with PCF, if the SPCF is co-located with PCF, the security policy based on service application can be retrieved via NG5 interface between the PCF and AF.

Security policy based on service application may include as follows:

- AUSF selection
- Confidentiality protection algorithm
- Integrity protection algorithm
- Key length
- Key lifecycle

Examples:

- In the case of UP protection and NAS Signalling protection negotiation, SPCF acts as security algorithm determination function.

NOTE: From the security point of view, the security requirements from services would be different, for example, the security requirement from the critical communication could be different from video streaming. Editor's note: It is FFS whether the SPCF should be standardized and needed to be centralized position.

5.2.2 Security assumptions

Authentication may involve at least one cryptographic key, for each subscription, that needs to remain secret. (This may be a shared secret key for use in symmetric cryptography, or a private key used in asymmetric cryptography.)

Lenovo Ex. 1007
Page 143

5.2.3 Key issues

5.2.3.1 Key Issue #2.1 Authentication framework

5.2.3.1.1 Key issue details

Editor's note: There are various citations of requirements in SA1 TRs. As SA1 is currently working on TS 22.261 [80] to capture the normative 5G requirements it needs to be checked whether the cited requirements in SA1 TRs are carried over to TS 22.261.

The next generation system is expected to accommodate various services defined in the 3GPP TRs 22.861 [3], 22.891 [7], 22.862 [4]. 22.863 [13]. In order to guarantee better support operator or 3rd party services, the 3GPP network should support a flexible authentication framework for network and service access.

The purpose of this key issue is to identify how the authentication framework could efficiently and adequately support different kinds of scenarios and applications.

This key issue addresses the following general aspects:

- provision of a common framework for mandatory-to-use primary authentication between the UE and the network defined in 3GPP specifications (3GPP network for short)

- provision of a common framework for optional-to-use secondary authentication between the UE and an external data network (DN) possibly run by a 3rd party.

NOTE: An interface between the 3GPP network and the DN is defined in 3GPP specifications, but the DN itself is not.

NOTE: SA2's TS 23.501 [74], v011, clause 5.6.6 contains the following: "The user may be authenticated by the DN... Such DN authentication and/or authorization takes place for the purpose of PDU session authorization in addition to: - The 5GC access authentication handled by AMF and described in clause 5.2.1… The UE provides over NAS SM information required to support user authentication by the DN."

NOTE: A form of secondary authentication between the UE and an external DN has already been defined for previous generations of mobile networks for the purpose of providing access control to the DNs, cf. 3GPP TS 29.061 [81].

NOTE: The authentication framework is to enable a secure secondary authentication, but it should be noted that the security for the secondary authentication also depends on the choice of the authentication method by the external DN. The establishment of mutual trust between a 3GPP network operator and a 3rd party running an external Data Network is outside the scope of 5G security specifications, in line with the handling of trust establishment in specifications for earlier generations of mobile networks.

Since NexGen network is supposed to meet different use cases such as broadband access, massive IoT, mission critical tasks, an authentication framework is highly desired to satisfy different authentication requirements in a fine-grained manner.

The present key issue is assumed to start from the observations in TR 23.799 [2] and TR 22.864 [6]. But it is meant to go further in defining methods how this support for a variety of access networks and authentication mechanisms can be achieved. It appears that NextGen system intends to minimize the dependencies between access and core networks allowing more flexible evolvement of both. Even though the CN needs to be aware of different characteristics, and security properties of the ANs, the goal is to develop the AN-CN interface towards more unified handling of different accesses. This is reflected in the conclusions of TR 23.799:

"Minimize access and core network dependencies by specifying a converged access-agnostic core with a common AN - CN interface which integrates different 3GPP and non-3GPP access types." [2, clause 8.12.1]

In the first normative release of NextGen, the untrusted non-3GPP access will not have an independent AAA infrastructure as it has in EPC. In particular, there is no direct Diameter based connection from the non-3GPP access site to the 3GPP AAA server but instead, the authentication messages are carried over the NAS protocol [2, clause 8.8.2]. Furthermore, UE connected to the core network over 3GPP access and non-3GPP access is served by a single AMF [2, clause 8.4]. Figure 5.2.3.1.1-1 demonstrates the architectural assumption. It seems that there will be two instances of NG1. However, it does not necessarily mean that the SEAF serving these two instances of NG1 could not

Lenovo Ex. 1007
Page 144

use a single master key as demonstrated e.g. in solution #3.4. The master key created over 3GPP access could be used to derivate keys for non-3GPP access, and vice versa.

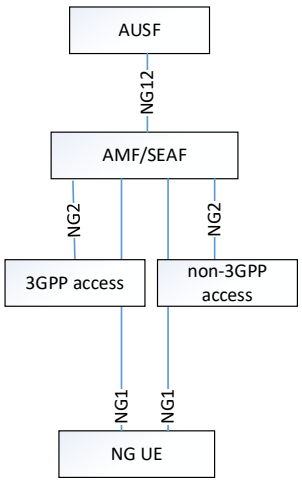


Figure 5.2.3.1.1-1: Simplified NextGen architecture for control plane over 3GPP access and standalone untrusted non-3GPP access

The evaluation of solutions for the authentication framework should take into account the following criteria

- Security:
- Possibility of a common transport for a variety of authentication methods:
- Efficiency:
- Interworking:

  Ease of handovers and idle mode mobility within NextGen and with other RATs
- Migration

  Backward compatibility to LTE:
- 3GPP control over possible enhancements of authentication method used over 3GPP-defined access network

5.2.3.1.2 Security threats

Weak authentication could cause the resource of operators to be misused or overloaded.

5.2.3.1.3 Potential security requirements

- The authentication framework shall be protected against misuse and overload.
- The authentication framework shall support use primary authentication between the UE and the 3GPP network.
- The authentication framework shall support optional-to-use secondary authentication between the UE and an external data network. The choice of the secondary authentication method shall be transparent to the 3GPP network and shall not weaken the security of the 3GPP network. If used the secondary authentication shall be run independently of the primary authentication, but after the completion of primary authentication.
- The authentication framework shall support authentication for communication over a variety of access networks providing access to the 5G core, including access networks not defined by 3GPP, e.g. fixed or WLAN access networks.

Editor's Note: It is ffs whether the authentication framework shall support alternative authentication methods with different types of credentials. The types of credentials and how to use these credentials are ffs.

Lenovo Ex. 1007
Page 145

- EPS AKA shall be supported for accessing to LTE network either during initial access or via mobility events.
- The system shall support enhanced authentication mechanism while maintaining backward compatibility.

A NextGen authentication framework should take into account the following potential requirements from TR 22.864 [6]:

"The 3GPP network shall be able to integrate fixed and wireless access management and provide an efficient provision of services over 3GPP and non-3GPP accesses."

NOTE: SA2 has decided to consider only 3GPP-defined access and untrusted non-3GPP access in 5G phase 1.

"The NextGen system shall be able to support:

- Authentication to access NextGen network through a non-3GPP access using 3GPP credentials."

A NextGen authentication framework should take into account the following potential requirements from TR 23.799 [2]:

"Support authentication of UE connecting to the NextGen CN via different access network, including 3GPP technologies, non-3GPP wireless technologies, fixed broadband access, secure and unsecure Non-3GPP accesses."

"Authentication mechanism include 3GPP authentication mechanisms for the NextGen RAT and for evolved LTE, 3GPP authentication mechanisms for non-3GPP access networks (e.g. 3GPP mechanisms for trusted Wi-Fi scenarios), and possibly mechanisms for other access technologies that may not be defined by 3GPP. As an example, depending on the specific authentication mechanisms to be supported, the common authentication transport may be AAA to support authentication mechanisms based on EAP."

- The authentication framework shall support EAP framework for non-3GPP accesses.

Editor's Note: EAP methods are FFS.

5.2.3.2 Key Issue #2.2: Reducing the impact of secret key leakage

5.2.3.2.1 Key issue details

The current mobile security architectures – GSM / GPRS, UMTS and LTE – rely almost entirely on the secrecy of the long term secret key (called Ki in GSM / GPRS, or K in UMTS/LTE – we will call it Ki here).

The fundamental security assumption is that the attacker does not know Ki. But if this security assumption fails, the loss of security is catastrophic.

Ki might leak to an attacker for a number of reasons, e.g.:

a. hacking at the factory (SIM vendor or subscription manager) where Ki is generated
b. hacking of the communication channel over which Ki is transported from SIM vendor or subscription manager to mobile operator
c. hacking into the mobile operators
d. insider attack at a mobile operator or SIM vendor
e. local attack (e.g. side channel) on the SIM card in the supply chain
f. local attack (e.g. side channel) on the SIM card while temporarily "borrowed" from the customer

Operators and vendors should of course try to prevent any of (a) – (f) from happening.

5.2.3.2.2 Security threats

Consider an attacker who wants to listen to a target user's phone calls. Assume that this attacker knows the authentication algorithm on the target user's USIM; some operators have proprietary algorithms, and some algorithms use additional secret constants, but these are all global secrets, and (following Kerckhoff's principle) we must assume

Lenovo Ex. 1007
Page 146

that they will not remain secret from a determined attacker. (They may add extra security, and make the attacker's life harder, but the security of the NextGen system cannot rely on that.)

If the attacker also knows the target user's Ki, then intercepting and decrypting the target's calls becomes easy for the attacker, and completely passive. The attacker does not need to set up a false base station, or man-in-the-middle, or anything like that. The attacker simply listens out for the authentication challenge sent from the network to the target device, and extracts RAND; he/she feeds RAND and Ki into the algorithm, and can compute the same radio interface encryption key (session key) that the target device has.

By such straightforward, passive means the attacker can:

- decrypt user plane traffic (uplink or downlink);
- decrypt user plane traffic from any sessions that he recorded before learning the target user's Ki (assuming that the recording includes the authentication challenge);
- decrypt control plane messages, which may also include sensitive information (such as the assignment of new temporary identifiers).

Extending to a more active attack, the attacker can also:

- pose as a serving network, and trick the target user into attaching to that false network, with all the further attack opportunities that this implies (e.g. phishing, or delivering malware to the target);
- pose as the target user, to carry out fraud.
- launch an active man-in-the-middle attack to tamper with data being transferred between UE and the network.

5.2.3.2.3 Potential security requirements

It will be very difficult to achieve really robust security against an attacker who knows all of the secret keys and algorithms that a subscription is using. But we can make sure that the attacks would be much harder in practice. Realistic requirements are thus:

- An attacker, even if he/she knows the secret key and Authentication and Key Agreement algorithm (including any global constants) that a subscription is using, would have to carry out a long-term active man-in-the-middle attack in order to eavesdrop on that subscription. That is, anti-passive attack capabilities shall be provided if the pre-shared root key Ki is stolen.
- Likewise, an attacker, even if he/she knows the secret key and Authentication and Key Agreement algorithm (including any global constants) that a subscription is using, would have to carry out an active man-in-the-middle attack in order to spoof uplink or downlink traffic from/to that subscriber.
- The system provides forward secrecy, in the sense that an attacker learning Ki at any time should not be able to decrypt earlier encrypted radio interface traffic that that they may have recorded.

More ambitious goals are:

- An attacker who knows the secret key and Authentication and Key Agreement algorithm (including any global constants) that a subscriber is using cannot eavesdrop on that subscriber or tamper with data being transferred between UE and the network even by means of an active (e.g. man-in-the-middle) attack.
- An attacker who knows the secret key and Authentication and Key Agreement algorithm (including any global constants) that a subscriber is using can still not carry out a false base station attack against that subscriber.

5.2.3.3 Key issue #2.3: Authentication identifiers and credentials

5.2.3.3.1 Key issue details

a) Subscription identifiers and credentials

In UMTS and LTE, the IMSI uniquely identifies a mobile subscription globally. The IMSI is stored in the USIM application on the UICC issued by the MNO. In other words, the identifier of the subscription belongs to, and is completely under the control of, the MNO.

Lenovo Ex. 1007
Page 147

TR 22.862 has the following requirement that calls for the network access to equipment owned and managed by a 3rd party such as a factory owner.

"The 3GPP system shall support industrial factory deployment where network access security is provided and managed by the factory owner with its ID management, authentication, confidentiality and integrity."

This key issue deals with the types of subscription credentials and identifiers that are used to access Next Generation system. Equipment related credentials and identifiers are dealt with in a separate key issue (Key Issue # 2.4). Solutions may describe how the credentials could be stored, as well as how the interoperability and roaming (if supported) related to credentials could be implemented. Figure 5.2.3.3.1-1 demonstrates the types of subscription credentials that are under discussion, and how the identifiers, and long term security keys are related to each other. The intention is to define a flexible system that allows also alternative access authentication methods with different types of credentials other than the legacy methods currently supported in 3GPP for machine type devices. This is both for locally deployed industry automation systems and large scale MNO networks for non-human IoT deployments (i.e., where the devices are not used by humans, e.g., excludes smart phones and wearables).

Editor's note: Word "non-3GPP" should be replaced by another word because the "non-3GPP" credentials and "non-3GPP" identifiers are being described in 3GPP specifications.

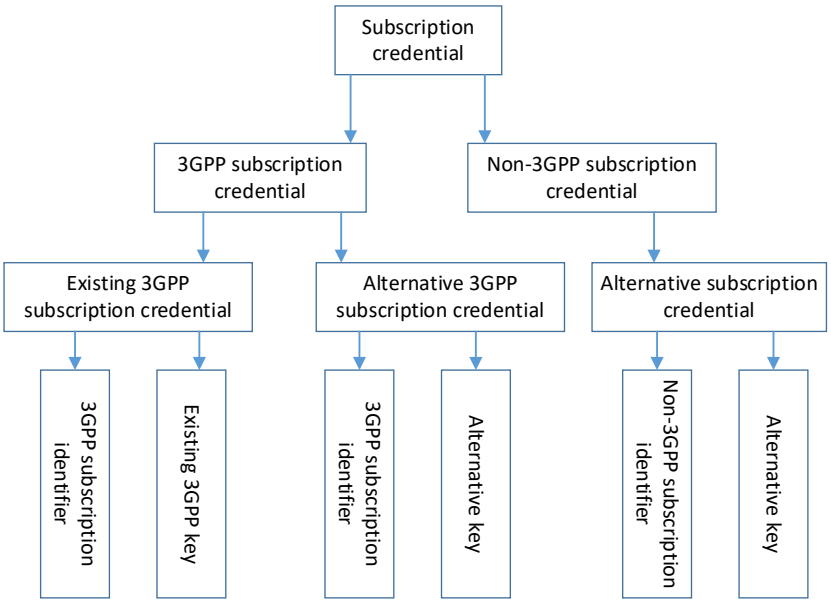


Figure 5.2.3.3.1-1: Different variants of subscription credentials

Three types of credentials could be relevant for this key issue:

- Existing 3GPP subscription credential: This is a credential similar to (or exactly the same as) the legacy credential that has a 3GPP subscription identifier and a long-term shared key. There are no limitatinos in the usage of this type of credentials in the NextGen system.

- Alternative 3GPP subscription credential: This is a new type of credential that is based on something else than the legacy credential. It includes an alternative key (e.g. shared, private, or public), however, it still has a 3GPP subscription identifier. These credentials can be used for large scale MNO networks deploying alternative credentials for non-human IoT devices.

- Alternative subscription credential: This is a second type of new credential that is also based on something else than the legacy credential. It includes an alternative key (e.g. shared, private, or public), however, it does not have a 3GPP subscription identifier. These credentials can be used for locally deployed, non-human machine type communication systems, e.g. industrial automation systems.

Lenovo Ex. 1007
Page 148

NOTE: The use of any alternative credential has many business aspects that are out of the scope of this TR. This key issue will focus on technical side of the problem, and it is motivated by TR 22.862's [4] service requirement related to the 3GPP system supporting authentication process that can handle alternative authentication methods with different types of credentials. The service requirements in TR 22.862 [4] refer to the use of alternative credentials in factory context e.g. with robots, sensors and actuators over both licensed and unlicensed spectrum.

The subscription identifiers in 3GPP-based systems are used for several purposes. They globally and uniquely identify the subscription; however, they are also used for identifying the home network and for routing the authentication vector request to the home network when the UE is roaming. Therefore when the use of an alternative subscription credential requires the support for roaming, a 3GPP subscription identifier shall also be associated with the alternative credential, and used for routing the authentication request to the home 3GPP network. It is understood that a non-3GPP subscription identifier is not routable to the home 3GPP network if the UE is roaming.

NOTE: The use of alternative keys and the non-3GPP subscription identifiers may be subject to regional regulatory requirements. However, it is assumed as a general principle that if the Mobile Operator has not provided the alternative key for security, the Mobile Operator would not be responsible for providing the session key material to Lawful Interception. The regional regulation is assumed to be dependent on different network deployment scenarios and the services provided, e.g. different network slices may have different regulatory requirements. For example, a dedicated network slice for factory where the subscribers are not humans but robots, sensors and actuators or networks operated only over unlicensed spectrum may have different Lawful Interception requirements than the more traditional network deployment scenario.

The acceptance of any type of alternative credentials (i.e. 3GPP or non-3GPP) is a local decision of the serving access network, and consequently can be limited in terms of global roaming. In other words, alternative credentials are sometimes limited to local usage in one access network, and are not accepted by other access networks. Furthermore, the use of different types of alternative credentials can be limited to certain services or for dedicated network slices that are isolated from other slices within the same PLMN.

In addition there are other requirements that relate to identifiers and possibly could be covered under the present key issue:

Separation of equipment identifier from subscription (TR 22.864)

"The 3GPP system shall be able to support identification of subscriptions independently of identification of devices."

Two different types of identifiers are referred to in the above requirement – identifier of the device and identifier of the subscription. The TR is unclear on what these identifiers really mean. For the purposes of the present TR, the definitions of identifiers in clause 3.1 apply.

b) Group identifiers and credentials

Need for group identifier (TR 22.861)

"The 3GPP System shall support a mechanism which provides an appropriate and efficient authentication mechanism for groups of IoT devices."

One implicit requirement coming out of the above statement is the need to uniquely identify and manage identifiers of the group.

It is ffs how group identifiers are assigned and managed in Next Generation system, and which credentials are used for authentication.

5.2.3.3.2 Security threats

a) Subscription identifiers and credentials

One motivation for allowing the use of alternative credentials in the Next Generation system is to re-use already existing identity management infrastructures (e.g. in a factory), and their credentials for network access security. It is also possible that the MNO provides IoT services based on alternative credentials within it's own identity management infrastructure. However, this must not lead to the fragmentation of the market or to complexity in the UE and network side for supporting tens or hundreds of authentication methods.

Lenovo Ex. 1007
Page 149

If the authentication end-point is located outside a 3GPP network, the interface between the 3GPP network and the external entity performing the authentication needs to be secured. Otherwise there is a risk for false charging and unauthorized access to network resources.

The alternative credentials could be compromised in the UE side if they are not stored in secure way. Compromised credentials may lead to false charging, impersonation and unauthorized access to network resources, and false identification for the purpose of Lawful Interception.

If the long-term key is not stored securely, there might be risks for the subscription or the home operator being liable for unauthorized use. For this reason, it could be beneficial if the use of the credentials could be limited, e.g. to certain networks, or services, or limitations of usage could be given in the mutual agreements between two roaming partners. For example, if the alternative credentials were used for sponsored subscriptions where the sponsor is providing the credential and is paying the bill, the usage should be limited to sponsored services only. Or if some visited network does not provide dedicated network slice for IoT devices with alternative credentials, such limitations would need to be agreed beforehand in the roaming agreement.

There could be baseline security requirements for the lengths of the permanent keys and/or the related authentication methods. Otherwise, the use of potentially weaker credentials could potentially impact negatively to the services offered by stronger credentials, e.g. indirectly if all credential types are used within a single network slice, and the slice becomes a victim of denial of service attack because of the weaker credentials. On the one hand, the use of the potentially weaker keys and authentication methods could be isolated in dedicated network slice in order to avoid attacks towards the network slices using stronger keys and authentication methods.

b) Group identifiers and credentials

5.2.3.3.3 Potential security requirements

a) Subscription identifiers and credentials

The following potential security requirements apply to any type of alternative credentials:

- The NG shall support alternative credentials that should be able to be used to authenticate the machine-type NG-UE to the 3GPP network access.
- The system shall provide means for the MNO to allow or prevent the usage of alternative credentials.
- Alternative credentials shall only be used with non-human machine type devices (IoT).
- Alternative credentials that are linked to non-3GPP subscription identifiers shall only be used locally in the home network. Roaming to visited networks is not possible.
- Alternative credentials that are linked to 3GPP subscription identifiers may be used globally, however, the visited network shall make a policy decision if the alterantive credentials are allowed locally or not.

5.2.3.4 Key issue #2.4: Equipment identifier authentication

5.2.3.4.1 Key issue details

In existing 3GPP systems, the UE has two permanent identifiers, namely, the IMSI for identifying the subscription associated with the UE, and the IMEI for identifying the Mobile Equipment (or the equipment identifier) that is using the subscription associated with the IMSI. The network authenticates the IMSI using AKA (subscription authentication). Therefore, the network can trust the IMSI reported by the UE. However, the IMEI reported by the UE to network is not authenticated. Therefore, the network cannot place any trust on the reported IMEI of the UE.

IMEI is being used as a key identifier for blocking stolen MEs, to identify Emergency Calling originators when IMSI is not present or cannot be authenticated, and as one of the target identities for LI. In all of the above use cases, trust in the equipment identifier is of a great importance.

The NextGen systems will not only need to authenticate the subscription of the device based on the subscription identifier associated with the device but also may need to authenticate the identifier of the device (i.e., equipment identifier) that is using the subscription associated with the subscription identifier.

In addition, there are other requirements that relate to equipment identifiers and possibly could be covered under the present key issue:

Lenovo Ex. 1007
Page 150

Separation of equipment identifier from subscription (TR 22.864)

"The 3GPP system shall be able to support identification of subscriptions independently of identification of devices."

Two different types of identifiers are referred to in the above requirement – identifier of the device and identifier of the subscription. The TR is unclear on what these identifiers really mean. In LTE and earlier generations, equipment identifier referred to the IMEI of the device whereas subscription identifier refers to the IMSI stored in the UICC.

The TR 22.864 section 5.8.1.1 "Device Theft Prevention", is the driving factor behind this requirement. It states the following:

"Smartphones and other high value devices such as drones and unmanned aerial vehicles potentially lead to increased numbers of devices with communications capability being stolen and modified to prevent tracing and recovery by civil authorities. This use case applies to devices that law enforcement requires to be traceable."

It further goes on to say:

"There are two facets employed for reducing device theft rates: theft prevention and stolen device recovery. Theft prevention involves disabling normal smartphone operation, preventing its illegal reuse, repurpose or resale, and deleting user sensitive data. Stolen device recovery involves identifying a recovered smartphone (by the user or civil authorities), verifying that it is stolen, and potentially restoring the smartphone to normal operation.

Unique equipment identifiers in the Next Generation system are needed that are stored in a secure and tamper resistant manner on the device. When a stolen device is recovered, the civil authority has a need to retrieve the equipment identifier but may not have sufficiently detailed knowledge of the specifics of the device's user interface. These protected equipment identifiers can then be used to reliably identify a recovered smartphone as stolen as well as support the tracing of illegal reuse, repurpose or resale of stolen smartphones."

Secure storage of equipment identifiers (TR 22.864)

This suggests a need for having a piece of equipment identifier that is "securely" associated with a device and can be obtained independent of the user of the device.

It should be noted that in LTE and earlier generations, the equipment identifier, i.e. the IMEI, was not considered an identifier that could be used in authenticating the equipment to the network. However, there is a requirement from GSMA that IMEI be securely implemented in the terminal. Furthermore, the IMEI is used for tracking stolen phones in the Equipment Identity Register (EIR) operated by the GSMA.

There are currently mechanisms to cryptographically associate an identifier to equipment, for example, based on the 802.1AR DevID manufacturing certificates or TPM generated cryptographic identifiers.

It is proposed to be ffs to determine the use cases where device identification based on secure equipment identifiers apply and evaluate its implication on the overall security architecture of Next Generation.

5.2.3.4.2 Security threats

NextGen systems are expected to support a large number of devices that are many orders of magnitude greater than today. These devices may also have varying levels of capabilities, including varying levels of security capabilities. In addition to the authorization based on subscription authentication, the network may additionally need to perform further authorization checks for access to different services based on the reported equipment identifier (e.g., based on the capabilities associated with the equipment identifier). In such cases, it should be possible for the network to authenticate the equipment identifier before authorizing services that are tied to equipment identifier. Otherwise, an attacker may be able to use victim equipment identifier to bypass the network authorization checks.

Furthermore, in case a security vulnerability (e.g., implementation or design vulnerability) is found with a class of devices with a certain set of capabilities (e.g., devices with the same model number), in order to protect the network from potential attacks, it is desirable that these devices are blocked or restricted from accessing certain networks or services, at least temporarily until their security vulnerability is remediated (e.g., through OTA security firmware/software update). Otherwise, an attacker may be able to exploit the vulnerability of these compromised devices in order to launch attack on those networks or services. In order to identify and block or restrict access to such devices, it should be possible for the network to identify these devices in an authenticated manner. If the network is not able to verify the claimed identifier of the device, the attacker may simply modify the equipment identifier reported to the network, thus bypassing any restriction that are enforced by the network. Furthermore, if unauthorised modification or spoofing of a equipment identifier is possible, then the NextGen System will not be able to distinguish spoofed

Lenovo Ex. 1007
Page 151

devices from genuine ones. Therefore, it is desirable that NextGen systems are capable of authenticating the reported equipment identifier. Storage and processing of equipment identifier and associated credentials outside of a secure entity on the NG-UE could lead to unauthorised access, modification, and cloning of the equipment identifier and associated credentials.

5.2.3.4.3 Potential security requirements

- Based on the use case, it should be possible for the network to authenticate the reported identifier of the device (i.e., equipment identifier).

Editor's Note: It is FFS whether the above requirement needs to be modified or new requirement(s) added in order to take into account the necessity for the operator to not be dependent on a 3rd party for the authentication of the reported equipment identifier (e.g., the operator doesn't need to make use of any entities outside of operator's network).

NOTE: Secure storage and processing requirements for device credentials and identities is covered in Security area #5: Security within NG-UE.

5.2.3.5 Key issue #2.5: Non-AKA-based authentication

Editor's Note: This key issue may have to be significantly revised depending on the reply to S3-160821 from SA1.

5.2.3.5.1 Key issue details

While AKA-based authentication has been a cornerstone for the success of UMTS and LTE security, there are service requirements that suggest that non-AKA-based methods need to be considered in NextGen as well. They can be found in TR 22.862 " Feasibility Study on New Services and Markets Technology Enablers - Critical Communications ", clause 5.1.3, as follows:

"The 3GPP system shall support industrial factory deployment where network access security is provided and managed by the factory owner with its ID management, authentication, confidentiality and integrity." and

"The 3GPP system shall support an authentication process that can handle alternative authentication methods with different types of credentials to allow for different deployment scenarios such as industrial factory automation".

However, it is not clear from these requirements what it actually means for NextGen security to support these alternative authentication methods. E.g., it is not clear whether 3GPP AAA servers would support alternative authentication methods, or rather whether 3GPP serving networks would be required to interact with 3rd party AAA servers.

What seems clear, however, is that it would not be appropriate to mandate the support for alternative authentication methods in all 3GPP AAA servers or in all NG UEs. There are likely to be operators wishing to support only traditional 3GPP credentials, i.e. USIM-based credentials, and there are likely to be NG UEs designed to support only enhanced Mobile Broadband using only traditional 3GPP credentials.

It is obvious that there is a relationship with the key issue "Authentication Framework". Such an authentication framework would be one way to make the use of alternative authentication methods transparent to the 3GPP NextGen serving network.

Possible EAP methods to study are EAP-TLS and EAP-TTLS, cf. e.g. Hotspot 2.0 that mandates their support. As explained above, mandating support of particular EAP methods in 3GPP AAA servers or in NG UEs seems not appropriate, but 3GPP could think about recommending a (quite limited) number of methods. Providing a security review of all available EAP methods by 3GPP seems out of the question.

A review of non-3GPP access to the EPC, as defined in TS 33.402, with respect to its relevance for NextGen is likely to be needed:

- In trusted non-3GPP access to the EPC, the authenticator resides in the trusted access network; would the authenticator in NextGen rather reside in the core network?

- It is ffs whether the analogy of the case of untrusted non-3GPP access to the EPC, using an ePDG, needs to be supported in NextGen.

Lenovo Ex. 1007
Page 152

It is further not clear where credentials are stored and processed on the terminal side when alternative authentication methods with different types of credentials are used. It is ffs whether 3GPP would have to define any requirements on credential storage and processing on the terminal side.

5.2.3.5.2 Security threats

- Weak alternative authentication methods could lead to security breaches.
- Weak credential storage and processing on the terminal side could lead to security breaches.
- The reliance on third parties for security of the NextGen network could make it difficult or impossible for 3GPP operators to vouch for the security of their networks.

5.2.3.5.3 Potential security requirements

- The NextGen system needs to support an authentication process that can handle alternative authentication methods with different types of credentials.
- Impact of potential security breaches resulting from weaknesses in alternative authentication methods or in credential storage on the NextGen system as a whole has to be minimized. One possibility to consider is separation of the uses of different authentication methods into different network slices so that any negative effects of potential breaches are limited to one network slice.
- If, based on architectural decisions, 3GPP serving networks are to interact with security entities, e.g. AAA servers, of third party then the impact on the trust model needs to be studied.

5.2.3.6 Key Issue #2.6: Efficient in energy consuming and reduced signalling for resource constraint environment

5.2.3.6.1 Key issue details

The Massive Internet of Things introduces new operational considerations to a 3GPP system. While some support for IoT will be provided by current systems, there is a room for improvement in the operational aspects that can be designed into a NexGen system whereas they are not easily retrofitted into an existing system.

Especially for the energy consumption sensitive devices, the objective is to keep operation for years, the authentication scheme should be designed to save computation cost and signalling overhead as efficient as possible.

5.2.3.6.2 Security threats

Editor's note: Security threats need to be further clarified.

5.2.3.6.3 Potential security requirements

Editor's note: potential security requirements should be derived from security threats.

- The lightweight but secure enough authentication scheme for energy consuming sensitive devices is required in NexGen network.

5.2.3.7 Key Issue #2.7: Reduced signalling overload for massive number of UEs activating at the same time

5.2.3.7.1 Key issue details

There is a scenario that many IoT devices (e.g. meter devices) which are located in a given deployment need to access to operator's network. Then, the authentication for these IoT devices will be addressed by the network. It will bring a significant signalling overhead to the operator's network and even signalling storm may happen.

Efficient authentication for a group of IoT devices to reduce the signalling overhead is required in NexGen network to lighten the impact on the network, and more importantly, to decrease the chance of signalling storm.

Lenovo Ex. 1007
Page 153

5.2.3.7.2 Security threats

The attacker may control a number of IoT devices by compromising the IoT server (e.g. through intrude attacks). The attacker could invoke the authentication process between IoT UEs and network repeatedly. The amount of signalling overhead will occur when the authentication for these IoT devices are addressed by the operator's network. The network resource will be maliciously occupied. Even there is no an attacker, a large amount of signalling overhead may also occur when authenticating a great number of IoT devices.

Furthermore, it is envisioned that a large number of devices (e.g. IoT devices) are expected to be supported and serviced by NextGen networks. Each of these devices may perform a full authentication procedure (e.g., EAP-AKA') each time they connect or re-connect using different access network (e.g., non-3GPP). Such a volume of authentication requests / responses that may traverse back-and-forth between the UE and the network may cause the resources of the NextGen HSS / AuC to be exhausted thus causing a DoS scenario.

5.2.3.7.3 Potential security requirements

The 3GPP system shall support an authentication method which is resilient to DoS attacks caused by massive number of UEs authenticating at the same time.

Editor's Note: The below requirement assumes that the UE is capable of triggering the authentication procedure. This requirement needs to be revisited if a UE triggered authentication mechanism is considered for NextGen.

The 3GPP system should support an authentication method which is resilient to DoS attack caused by an abnormal UE that repeatedly initiates authentication procedure in a short period.

5.2.3.8 Key Issue #2.8: Authentication of the user

5.2.3.8.1 Key issue details

The following requirement is stated in clause 5.1.3.5 of [3]:

"Enhanced authentication mechanism shall enable an operator to provide efficient means to authenticate a user and a device (e.g., using biometric information)."

This could mean one or both of the following and it is not clear in [3] which is intended:

- the operator needs to be able to determine and verify the identifier of a user already associated with that device; or
- the operator needs to be able to determine and verify the identifier of a user, even if that user is using the device for the first time.

There may be some overlap here with the "identifications of subscriptions" issue discussed in clause 5.2.3.3.1.

5.2.3.8.2 Security threats

A device may be used by an attacker other than an intended user, compromising privacy of user data and/or integrity of data reported by the device (e.g. the user's medical information may be contaminated with data pertaining to the attacker). If the same device has multiple users, then these users may be able to compromise each other's privacy and/or the integrity of each other's data. If actions are billed on a per-user basis, then fraudulent usage may occur (by pretending to be a different user of the device, the fraudulent user transfers the bill to that other user).

An attacker may learn or compromise user authentication information (PINs, biometrics etc.) from a device or from a server. This may lead to loss of user privacy and authentication fraud. Use of a central server may lead to a mass compromise of multiple users' information at once.

User privacy may be compromised if the user is authenticated using the same credentials toward multiple services and relying parties. Use of a common credential may allow the user's actions across services to be linked together, and so create pervasive tracking of the user beyond the user's awareness and consent.

Lenovo Ex. 1007
Page 154

Where IoT devices are authenticated as a group, an attacker may get his own IoT device registered as part of another user's group, or may take control of a device which is part of some other user's group. The actions of the attacker would then be attributed (e.g. billed) to the victim user.

5.2.3.8.3 Potential security requirements

It shall be possible for devices to securely authenticate a single registered user, or any one of a set of registered users.

For any given device, it shall be possible for a mobile network and/or an IoT service to determine: whether a registered user has been authenticated; which user has been authenticated (if there are several registered users); the means that were used to authenticate the user (e.g. was it PIN, password or biometric); and/or other factors related to the reliability of authentication (e.g. how recently was this done, were there retries?)

It shall be possible for devices to register new users, in such a way that an operator and/or IoT service can associate the newly-registered user with an already-known party (e.g. the known user of another device).

Sensitive user authentication data (especially biometric information) shall be stored in a way which makes compromise very difficult. Mass compromise of many users' data shall be prevented. Tracking of a user across different services without the user's consent shall be prevented.

Where devices are joined into a group, for purposes of authentication of a user to a network and/or IoT service, each group shall have a designated owner who is recognized by the network and/or IoT service (for purposes of responsibility, billing etc). A device shall not join or leave a group without this action being confirmed by the owner of that group. For any given group-joined device, the owner shall be able to determine if a new user registers to the device, or if the user of the device otherwise changes; the owner shall then be able to decide whether the device remains part of the group.

A device that asserts that a user is authentic shall be suitably trustable by the operator and/or the IoT service.

5.2.3.9 Key issue #2.9: Security for service provider connection

5.2.3.9.1 Key issue details

NOTE: In this key issue, when it is said that service provider or manufacture pays for the network connection, service provider or manufacturer means a 3rd party in general.

Next generation network will be designed to serve not only new functions for mobile handset, but also to connect industries (such as manufacturing and processing, intelligent transport, remote health care). Since next generation network is aimed at supporting new business models, such as "connection support by service provider" scenario in TR22.861, security needs to be taken in into account to enable the new business model.

In the traditional mobile system, the authentication model evolves a subscription (UE) and the operator network, so the authentication mechanism is established between the subscription/UE and the operator network. This authentication model doesn't wholly capture the evolved business and new services of next generation network.

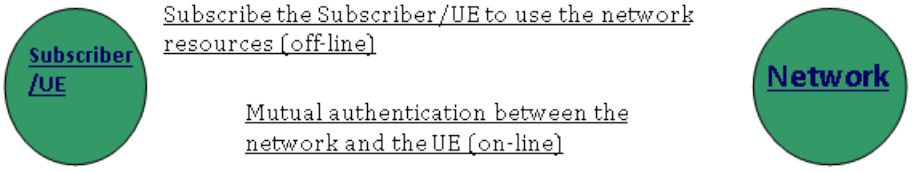


Figure 5.2.3.9.1-1: Legacy two-party authentication model for UMTS/LTE

For next generation network, the business model may further include the network, service provider/ device manufacturer, user of the service, and device, according to the "connection support by service provider" scenario.

TR 22.861 ve00 has the following requirements:

- [PR.5.1.3.5-002] The 3GPP system shall be able to support enhanced authentication, authorization and charging mechanisms to support various types of connectivity (e.g., subscribed, OTB or content-aware connectivity), with or without the presence of operator credentials in the device.

Lenovo Ex. 1007
Page 155

Based on the scenario and requirement, it's necessary to consider security and trust issues for these roles in the new business model:

- The service and network need to trust each other.
- The service needs to authorise device/user to get access to the network.
- It is necessary to prevent fraudulent use of the provided connectivity, which means network access authentication and/or authorization is necessary.
- When the user buy a device in order to access to the service cennectivity, user should trust the device with it's service information, and device should serve the user exclusively, so there should be mutual trust between user and device (e.g. passcode).

For the connection support by service provider, the business model may further include the network, service provider/ device manufacturer, user of the service, and device, as shown in the following figure.

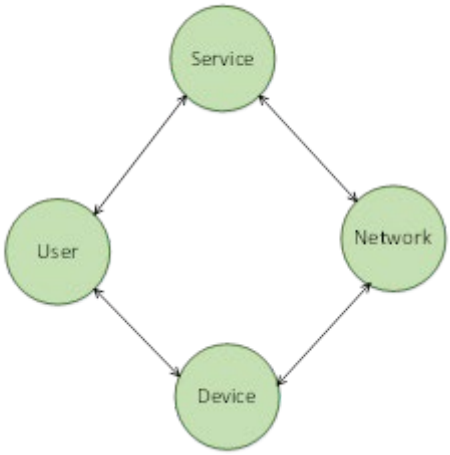


Figure 5.2.3.9.1-2: Four-party model for the connection support by service provider

5.2.3.9.2 Security threats

Next generation systems are expected to support a large number of devices that can be used by different service, as described in the "connection support by service provider" scenario. The following threats to the network and device/user needs to be taken into account

If there is no mutual trust between service provider and the network, there is a risk for manipulating the network connection and tampering the service data, which may cause fake service billing information to the network.

If the device/user isn't authorized or authenticated by the service, an attacker may be able to impersonate a legitimate device of the service, thus the service and its network resource could be misused.

If the device/user isn't authenticated or authorised for the network access, the network resources (e.g., network spectrum) would be misused.

If the device/user does not authenticate the network, malicious network attack could happen e.g. false base station.

5.2.3.9.3 Potential security requirements

TR 22.861 ve00 has the following requirements:

- [PR.5.1.3.5-002] The 3GPP system shall be able to support enhanced authentication, authorization and charging mechanisms to support various types of connectivity (e.g., subscribed, OTB or content-aware connectivity), with or without the presence of operator credentials in the device.

Based on the above requirement, the security requirements are the following:

Lenovo Ex. 1007
Page 156

- Mutual trust should be established between the 3GPP network and the service provider.
- Device/user should be authenticated and authorised to access to the network.
- The 3GPP network should be able to mitigate malicious access.
- The device should be able to authenticate the network to mitigate malicious network attacks, such as false base station attacks.

5.2.3.10 Key issue #2.10: Secondary authentication for network slice access by 3rd party service

5.2.3.10.1 Key issue details

In the next generation system, 3rd party services are hosted in a network slice, which is a dedicated logical network operating within the MNO owned infrastructure and configured to provide optimized solution for a particular 3rd party service.

The Key issue #2.1, discusses the need for a flexible authentication framework for operator and 3rd party services. One of the identified goals of the authentication framework is to provide authentication services for UE access to a 3rd party service in a one or more network slices.

Editor's Note: This is marked as ffs in clause 2.1 and above text is dependent on the resolution of that EN.

The 3GPP TR 22.862 observes that NextGen networks are supposed to provide authentication capability based on identities, credentials and AAA servers that is provided and managed by a 3rd party.

Editor's Note: There is an EN that these requirements from TR 22.862 require further clarification.

The purpose of this key issue is to identify specific issues when access authentication to a network slice is based on authentication by 3rd party AAA servers. This key issue looks at the scenario where the network access to a subscription is granted based on default MNO based authentication of the subscription, followed by a scenario/use-case specific 3rd party authentication of the subscription in a network slice. The case where the access to the network – or a particular network slice – rests entirely on authentication by 3rd party AAA servers without any MNO based authentication of the subscription, is not considered in this key issue.

For the purpose of this key issue, we call MNO based network access authentication as "Primary" authentication, and 3rd party based authentication authentication as "Secondary authentication".

This key issue would address the following security aspects when secondary authentication is used for access to a network slice:

- The subscription identifier used for secondary authentication may or may not be the same as the MNO provided identifier.
- Credential provided to the subscription may or may not be provided by the MNO.
- Changes, if any, that are required in 3GPP defined Authentication function (CP-AU, as currently defined in TR 23.799) to accommodate 3rd party AAA servers.

  Note: The goal is to specify a unified authentication framework for next generation systems, with the expectation of a common authentication mechanism for both primary and secondary authentication. In a unified framework, Authentication function (CP-AU) would be standardized for both primary and secondary authentication.
- Need for a standardized secure interface between the 3GPP defined Authentication function, CP-AU and the 3rd party AAA server

  Note: This aspect ties into the aim of coming up with a unified authentication framework, which should define a unified interface between CP-AU and any AAA server.
- Is there a need to define a "minimum" level of security requirements for secondary authentication methods? If so, how could 3GPP achieve this? Or should the MNO be content with the primary authentication the MNO performs and leave it to the third party to perform whatever authentication they prefer as it does not affect the security of the MNO network?

Lenovo Ex. 1007
Page 157

- Impact on Charging needs to be studied.

  Note: Charging is expected to be based on MNO records following a successful MNO authentication of the subscription, and may not depend on secondary authentication.

- LI aspects when 3rd party identifier is used in a network slice to identify subscriptions. Existing 3GPP LI mechanism is based on the following target identities - IMSI, MSISDN and IMEI. This aspect will study impact to LI when non-MNO identities are used to identify subscriptions in a network slice.

NOTE: This aspect also depends on the key management hierarchy for network slice. For example, which keys are used for protecting signaling and user plane – ones from primary authentication or secondary authentication?

5.2.3.10.2 Security threats

Access of UEs to network slice unauthorized by the third party.

5.2.3.10.3 Potential security requirements

Editor's note: It is FFS under what circumstances authorization of access to 3rd party slices that is not based on secondary authentication would be a viable alternative.

5.2.3.11 Key issue #2.11: Increasing home control in roaming situations

5.2.3.11.1 Key issue details

Roaming relations between operators are currently based on trust. However, some home operators may want to reduce the degree of trust they have to place in some operators of networks their subscribers visit as the trust may be abused by some visited network operators, e.g. for claiming false charges. The choice of authentication methods may help here, while Network Domain does probably not help (see next subclause), which is why the key issue is placed in this security area.

5.2.3.11.2 Security threats

- A fraudulent visited network that has a valid roaming relationship with the home operator may request authentication vectors from the home network and subsequently send an (Next Generation version of an) Update Location request for subscribers that are not actually present in the visited network. They may hope to be able to obtain additional revenue by claiming charges for the allegedly visiting subscriber.

NOTE: The threat may exist even when the origin of the Update Location request message can be verified by the home network through appropriate security measures in the interconnection network (e.g. Network Domain Security) as the visited network is an authorised participant in the interconnection network that, however, abuses the roaming relationship.

- Another variant of this type of fraud consists in the visited network authenticating a visiting subscriber correctly, but then claiming charges for traffic allegedly incurred by this subscriber even when the subscriber has already left, or was never attached to, the visited network. E.g. a visited network could properly authenticate the subscriber, but then not even bother sending the Attach Accept message.

5.2.3.11.3 Potential security requirements

- The home network shall have a means to ascertain that a subscriber whose location is updated to a new visited NG network has actually been authenticated involving this visited NG network.

The home network shall have a means to ascertain that a subscriber whose location is updated to a new visited NG network has actually been authenticated involving this visited NG network.

NOTE1: This requirement helps against the first threat above, but not the second one.

- The home network shall have a means to mitigate the second threat above, e.g by ascertaining a minimum authentication frequency for his roaming subscribers.

Lenovo Ex. 1007
Page 158

NOTE2: This requirement, in conjunction with the first requirement, helps mitigating the second threat above, although it cannot completely prevent it.

5.2.3.y Key issue #2.y: <key issue name>

5.2.3.y.1 Key issue details

5.2.3.y.2 Security threats

5.2.3.y.3 Potential security requirements

5.2.4 Solutions

5.2.4.1 Solution #2.1: Updating the long term secret key, in such a way that the new key is less exposed to potential attack than the original one was

5.2.4.1.1 Introduction

This solution addresses key issue #2.2.

It will be very difficult to achieve really robust security against an attacker who knows all of the algorithms and long term secret keys that a subscription is using. But we can make sure that the attacks would be much harder in practice. A realistic objective is that an attacker, even if she knows the long term secret key and Authentication and Key Agreement algorithm (including any global constants) that a subscription is using, would have to carry out a long-term active man-in-the-middle attack in order to eavesdrop on that subscription.

5.2.4.1.2 Solution details

NOTE1: In this clause the terms "UICC" and the "HSS" are referred to. These should be understood as shorthand, referring respectively to the "device's UICC / secure element (or wherever the long term key is stored)" and the "HSS (or its Next Generation Systems equivalent)".

NOTE2: In this clause, the GSM term "Ki" to refers to the long-term shared secret key stored in the UICC and the HSS – assuming that NextGen security remains largely based on such a shared secret key. The UMTS or LTE equivalent would be K. The terminology for NextGen is not yet decided.

Clause 5.2.3.2.1 lists a number of ways in which the original shared secret key might leak to an attacker. Many of the possible leakage points (points a – e) arise from the initial provisioning process. This solution involves a key exchange protocol being run between the UICC and the home network HSS, in order to create a newly agreed Ki value to replace the existing one. Elliptic Curve Diffie Hellman would be a suitable key exchange algorithm.

Exposing the HSS to update may in itself introduce new risks, and so should be handled with great care. One might consider running the key exchange protocol with a proxy for the HSS rather than with the HSS directly. However, the benefits of doing this are not entirely clear. Below, it is recommended that the update protocol take place over 3GPP-standardised signalling, rather than over the internet; and it is also recommend that the HSS, rather than the UICC, be the entity to trigger the update protocol. With these two points in mind, it is recommend for simplicity that the update protocol be carried out by the HSS directly, rather than by a proxy.

The key exchange protocol should be authenticated using the pre-existing shared secret, so that an attacker who does not already know the secret cannot act as man-in-the-middle at all. An attacker who does already know the secret may be able to act as man-in-the-middle during the key exchange protocol; however, a good protocol design can ensure that this attacker will have to remain as an active man-in-the-middle, essentially forever, in order to exploit that.

Editor's note: It is ffs whether the risk described in the above paragraph is acceptable.

Editor's note: The protocol design needs further details. This includes how this protocol fits the NextGen architecture.

Using a key exchange protocol raises a risk that this protocol itself might be compromised over the lifetime of Next Generation Systems (perhaps using quantum computers), and allow newly-exchanged keys to be recovered by an

Lenovo Ex. 1007
Page 159

attacker. One counter-measure is that where parties to the protocol already have a shared secret (e.g. the UICC and HSS already share Ki), then this existing shared secret should be fed into the new key derivation function, together with the output from the key exchange protocol. That way, an attacker would have to know the existing shared secret and compromise the key exchange to learn the newly derived secret. A suitable key derivation algorithm can use HMAC-SHA256, as defined in 3GPP TS 33.220 [27], as follows:

new Ki = KDF (key exchange protocol output, initial Ki)

where "key exchange protocol output" refers to the shared secret resulting from the key exchange protocol, and "initial Ki" refers to the Ki value that was shared between the UICC and the HSS before the protocol was run, and that was used to authenticate the key exchange.

There are two alternative ways to carry the key exchange protocol messages:

1. Over signalling messages. In this case, signalling messages will have to be defined to carry the protocol messages between UICC / secure element (or wherever the long term key is stored) and the home network HSS (or its Next Generation Systems equivalent), across core and (potentially roamed-to) radio network.

2. Over the user plane and the internet.

The recommended option is to carry the key exchange protocol messages over signalling messages. This is the safer option

There are two alternative entities that could initiate the key exchange protocol:

1. The UICC.

2. The HSS.

To maintain operator control, and mitigate possible DoS risks, the recommended option is to have the HSS trigger the key exchange protocol. Either way, the key exchange protocol should be run, and the long term key replaced, at the earliest feasible opportunity after the subscription is activated. It is not necessary, though, to do this before any user traffic is allowed.

5.2.4.1.3 Notes on statefulness at the HSS

Editor's note: This clause needs to be revised once the editor's notes in the previous clause are resolved.

Using something like Elliptic Curve Diffie Hellman for key agreement might suggest that the HSS would need to maintain state during the key agreement session – whereas HSS/AuCs today are generally stateless, not running multi-pass communication sessions.

If this is a concern, then there are a number of ways to mitigate it:

Editor's note: The way to mitigate the risk is ffs. It also depends on the details on the protocol design that are ffs.

1. It was already noted that it might be better to run the key exchange protocol with a proxy for the HSS, rather than with the HSS directly. In that case the proxy would be new, and there would be less reason to avoid it being stateful.

2. The "statefulness" could be managed by using the database that the HLR maintains with information for each subscription.

3. If the UICC sends the first message in the two-pass ECDH key exchange then it's the UICC, not the HSS, that needs to remember a secret ECDH parameter. (The HSS could still initiate the overall protocol by first sending a trigger message to the UICC.)

4. The HSS need not store its secret ECDH parameter at all, but instead can send it to the UICC – encrypted under an HSS public key, and signed under an HSS private key. The UICC then simply sends this back to the HSS in the return message. Neither the UICC nor any eavesdropper can read the secret parameter (because of the encryption), nor can they modify it without the HSS detecting that (because of the signature).

5. The above mechanism could work in reverse, with the UICC sending its secret ECDH parameter to the HSS encrypted and signed, and the HSS returning it.

Lenovo Ex. 1007
Page 160

5.2.4.1.4 Evaluation

An attacker who does not know the original Ki at the time that the key exchange protocol is run will not be able to carry out a man in the middle attack on it (because it is authenticated with the original Ki).

An attacker who does know the original Ki may be able to carry out an active man in the middle attack on the key exchange protocol. (This is likely to be easier if the protocol runs over the internet, harder if it runs over inter-operator signalling.) By doing this, the attacker can trick the HSS and UICC into thinking that they are sharing a new key, whereas in fact one key is shared between HSS and attacker, and another key between attacker and UICC.

What the attacker cannot do, though, is to trick the HSS and UICC into agreeing a new Ki that the attacker also knows. To exploit the man in the middle attack, therefore, the attacker will have to remain as an active man in the middle on all subsequent exchanges that use, or depend on, the new Ki value. This is a much harder attack in practice than the passive eavesdropping described in clause 5.2.3.2.2.

Clause 5.2.3.2.1 lists six possible ways (labelled a – f) in which a long term secret key might leak to an attacker. This solution fully addresses points a, b and e, and reduces the exposure to points c and d. It does not address point f.

The recommended approach is to carry the key update protocol messages over signalling, rather than over the user plane and the internet. This requires less exposure of the HSS to possible malicious attack. Based on this recommended approach, it is also recommended that the key update protocol be carried out with the HSS directly, rather than in a proxy "in front of" the HSS. While a proxy would in some sense shield the HSS from attacks attempting to exploit the key update mechanism, it also complicates the picture, and the extent to which it would reduce risks in practice is not very clear. Another recommendation made for this solution, which is to have the HSS rather than the UICC trigger the key update protocol, also reduces the exposure of the HSS.

It's interesting to note that this mechanism could also address some concerns with embedded SIM. In the embedded SIM world, operators may have to accept UICC hardware and IMSI/Ki credentials from a much wider set of suppliers than before, with less confidence about their quality. Supplier accreditation schemes can give some reassurance here; and if "profile interoperability" is supported – allowing profiles from any subscription manager to work on any UICC hardware – then operators will be able to work with their favourite subscription managers irrespective of the UICC hardware manufacturer. But the Ki replacement mechanism described above gives another way to reduce risk: the operator can accept initial Ki's from vendors they may not entirely trust, but then replace those Ki's with new ones created directly between the AuC and the UICC, with no involvement from the subscription manager at all.

5.2.4.2 Solution #2.2: Including a key exchange protocol into the derivation of the radio interface session keys

5.2.4.2.1 Introduction

This solution is identical to solution #3.1. Please see the text there.

5.2.4.2.2 Solution details

This solution is identical to solution #3.1. Please see the text there.

5.2.4.2.3 Evaluation

With a well-chosen key exchange protocol, a would-be eavesdropper who somehow (Key Issue #2.2) knows a subscriber's long term secret key will still not learn the keys used for radio interface security, unless they:

- act as man-in-the-middle during the key exchange, and
- remain as active man-in-the-middle during the subsequent radio communication on which they want to eavesdrop

… all of which is significantly harder in practice, and more likely to be detected, than a passive eavesdropping attack.

This solution therefore satisfies the first potential security requirement identified in section 5.2.3.2.3. It also satisfies the second requirement identified there: an attacker learning Ki at some time cannot retrospectively determine any session keys used previously, even if she has recorded all of the key exchange messages used to establish those session keys.

Lenovo Ex. 1007
Page 161

All of the above refers to confidentiality attacks. In terms of integrity attacks, where a single spoofed message may cause damage, the increase in difficulty and detectability is not quite so pronounced, but still present to some degree. In any case, confidentiality attacks are probably more of a risk in practice.

The main downside of Solution #2.2 is latency. A key exchange protocol such as Elliptic Curve Diffie Hellman takes noticeably longer than the type of key derivation used in 4G. Rather than imposing this solution on all connections, therefore, it may be best only to use it for connections that can "afford" the latency impact.

5.2.4.3 Solution #2.3: Device reporting on local user authentication

5.2.4.3.1 Introduction

This solution addresses the first part of key issue 5.2.3.8:

- the operator needs to be able to determine and verify the identifier of a user already associated with that device;

The associated security requirements are achieved by avoiding central storage of user authentication information (PINs, biometric data etc.). Rather, such data is stored locally on the device: the device authenticates the user locally, and then securely reports (to the mobile network, service provider etc.) which user has been authenticated and how it was done.

5.2.4.3.2 Solution details

Several specifications for this solution have been developed by the FIDO Alliance [19]. Some key points are as follows:

- For each user authentication method ("Authenticator") supported by the device ("FIDO client"), there is a preloaded attestation key. This enables the service ("FIDO server") to be sure that the device is compliant to the FIDO specifications.
- When registering a user of the device towards a service, the device generates a unique cryptographic key-pair for that (user, service) pairing; and then proves the public key belongs to the device using the attestation key
- The (user, service)-specific key is then used to sign reports to the service, indicating whether the user has been authenticated, how recently this was done etc.

These mechanisms protect user privacy: as well as preventing the central storage of biometric data, keys used with different relying parties will not allow any such party to link all the actions to the same user.

As the FIDO mechanism allows reporting to several different parties, it can address the requirements for a group owner and/or IoT service provide to be able to tell who is using which devices, as well as for the operator to learn this info.

5.2.4.3.3 Evaluation

The solution meets the following requirements listed in 5.2.3.8.3:

"It shall be possible for devices to securely authenticate a single registered user, or any one of a set of registered users."

"For any given device, it shall be possible for a mobile network and/or an IoT service to determine: whether a registered user has been authenticated; which user has been authenticated (if there are several registered users); the means that were used to authenticate the user (e.g. was it PIN, password or biometric); and/or other factors related to the reliability of authentication (e.g. how recently was this done, were there retries?)"

"Mass compromise of many users' data shall be prevented."

"Tracking of a user across different services without the user's consent shall be prevented."

In addition provided that a secure component not removable from the UE (as suggested in Key Issue #1.13) is used to store biometric data for registered users, then the solution will meet the following requirement:

"Sensitive user authentication data (especially biometric information) shall be stored in a way which makes compromise very difficult."

And provided a secure component that is not removable from the UE (as suggested in Key Issue #1.13) is used to generate and register FIDO asymmetric key-pairs, then the solution will also meet the following requirements:

Lenovo Ex. 1007
Page 162

"A device that asserts that a user is authentic shall be suitably trustable by the operator and/or the IoT service."

5.2.4.4 Solution #2.4: Authenticating a new user for a device using a known device

5.2.4.4.1 Introduction

This solution addresses the second part of key issue 5.2.3.8:

- the operator needs to be able to determine and verify the identifier of a user, even if that user is using the device for the first time.

The proposed solution is to verify the new user by messaging a device and subscription that is already associated with that same user (e.g. a personal smartphone that the user already possesses). Provided that the new user has already registered such a "master" device with the operator, then the operator is able to identify the same user when he or she attempts to register to additional devices.

5.2.4.4.2 Solution details

Several specifications for this solution have been developed by the GSMA, called "Mobile Connect" [20].

In brief, an online service captures the user's (claimed) MSISDN, and then a challenge message is sent to the "master" device associated with that MSISDN, asking the user to confirm his identifier (and actions) within that service. The specific service here would be the act of registering to a new device i.e. using that device for the first time.

Several different levels of authentication are available on the master device, ranging from simple SMS and pushed USSD to SIM applets. These can be used for single factor authentication (proof of possession of the master device) or two factor authentication (proof of possession + PIN etc.) GSMA has defined four Levels of Assurance (LoA) in total.

5.2.4.4.3 Evaluation

The solution meets the following requirements listed in 5.2.3.8.3:

"It shall be possible for devices to register new users, in such a way that an operator and/or IoT service can associate the newly-registered user with an already-known party (e.g. the known user of another device)."

If the user who is messaged on the "master" device is designated as an owner of a group of IoT devices, then the Mobile Connect solution can also meet this requirement:

"Where devices are joined into a group, for purposes of authentication of a user to a network and/or IoT service, each group shall have a designated owner who is recognized by the network and/or IoT service (for purposes of responsibility, billing etc). A device shall not join or leave a group without this action being confirmed by the owner of that group. For any given group-joined device, the owner shall be able to determine if a new user registers to the device, or if the user of the device otherwise changes; the owner shall then be able to decide whether the device remains part of the group."

5.2.4.5 Solution #2.5: Timed attach for UEs

5.2.4.5.1 Introduction

This solution addresses key issue 5.2.3.7 of overload of network signalling. In particular, it addresses the issue where a large number of UEs try to access the network at the same time.

5.2.4.5.2 Solution details

In order for this solution to work, the network should monitor related signalling messages, such as attach messages. In case the number of signalling messages reach beyond a certain threshold (or the network detects otherwise that an overload situation occurs), the network may instruct the UE to 'back off' for a time X. A UE receiving such a message should refrain from sending signalling messages until the time X has passed.

Lenovo Ex. 1007
Page 163

The network may decide to grant the UE a time interval during which the UE is allowed to send signalling messages. In that case the network provides the UE with a time X and a time Y and asks the UE to send signalling messages between time X and time Y. The UE can randomly decide when to send signalling messages within this time interval.

NOTE: The back-off timer in the UE should be protected against tampering.

5.2.4.5.3 Evaluation

This solution is effective only against signalling measures due to massive attaches.

This solution is not effective against UEs of which the baseband processor is not complying with the networks request.

Note: This solution is a congestion control like measure that is to be specified by SA2.

5.2.4.6 Solution #2.6: Binding a serving network public key into the derivation of the radio interface session keys

5.2.4.6.1 Introduction

This solution addresses key issues 2.2 and 3.1. It is an enhancement to Solution #2.2 in that it achieves the same prevention against purely passive attacks, and also makes active attacks harder.

In particular, the solution ensures that an attacker who:

a) either knows the long term secret key and Authentication and Key Agreement algorithm, including any global constants, that a subscription is using (Key Issue 2.2),

b) or is able to observe or request keys sent between network nodes (Key Issue 3.1),

can still not abuse radio interface confidentiality in a purely passive attack, or abuse radio interface integrity by simple injection of a single spoofed message, but will instead have to carry out an ongoing active man-in-the-middle attack – which is harder, and more likely to be detected.

Further, by using a serving network public key N_{PUB} to authenticate the key exchange, we can ensure that an attacker of type b) is unable to act as a full man-in-the-middle, but is only able to unilaterally impersonate the UE towards the serving network. This will prevent an eavesdropping attack on the genuine UE. And since the genuine UE will fail the connection and attempt to re-authenticate, the attack is very likely to be detected.

5.2.4.6.2 Solution details

The key exchange proceeds much as described in Solution #2.2 but with some additions to steps 1,2, 4 and 5. These additions are shown below in bold:

1. UE and CP-AU perform mutual authentication. The authentication vector received from the AAA is a function of a serving network id, and a serving network public key N_{PUB}.

    a. Each CP-AU may generate a separate key-pair (N_{PRIV}, N_{PUB}). Or a single CP-AU may generate multiple key-pairs (e.g. it may refresh the key-pair regularly).

    b. If the AAA does not already have the intended N_{PUB} then the CP-AU must provide this to the AAA. The communication of a new N_{PUB} to the AAA must be integrity-protected.

    c. Using a USIM, the authentication vector might include a key K_N = KDF(CK||IK, Network Id, N_{PUB}) binding the authentication vector to the specific serving network, like the K_{ASME} in LTE.

2. UE and CP-AU derive K_1 after mutual authentication. K_1 is a function of the serving network id and of N_{PUB}. If the UE does not already have the intended N_{PUB}, then the CP-AU must provide this to the UE. But the UE should always use a known NPUB in preference to accepting a previously unknown NPUB; for example if surrounding cells present different NPUBs then the UE should prefer to select a cell using a known value.

    a. Using a USIM, K_1 may be derived from, the above key K_N.

Lenovo Ex. 1007
Page 164

3. CP-AU generates a private Diffie-Hellman key A_{PRIV} and a corresponding public key A_{PUB}.

4. CP-AU sends message 1 to UE, which contains A_{PUB}, a MAC computed using K_1 and a signature computed using the serving network private key N_{PRIV}.

5. UE verifies the MAC, verifies the signature using N_{PUB}, decodes A_{PUB}, and further generates a Diffie-Hellman private key B_{PRIV} and corresponding public key B_{PUB}. UE also derives a symmetric key K_{DH} from B_{PRIV} and A_{PUB} with Diffie-Hellman procedure. UE derives a session key $K_{session}$ from K_{DH} and K_1.

6. UE sends message 2 to CP-AU, which contains B_{PUB} and a MAC computed using K_1.

7. CP-AU verifies the MAC, decodes B_{PUB}, and derives the same symmetric key K_{DH} from A_{PRIV} and B_{PUB} with Diffie-Hellman procedure. CP-AU derives the same session key $K_{session}$ from K_{DH} and K_1.

Both UE and CP-AU now own the same shared session key $K_{session}$. They use $K_{session}$ to derive other keys for encryption and integrity protection. The Diffie-Hellman technique used in this authentication protocol can also be Elliptic Curve Diffie-Hellman.

Editor's note: The next paragraph should move to the Evaluation section when this is added. It is included here to demonstrate the security advantages of this proposal.

Observe that the only ways an attacker can become a full man-in-the-middle are: determine N_{PRIV} or A_{PRIV}; make the AAA use the attacker's own N_{PUB}; or make the serving network private key sign the attacker's own A_{PUB}. If the attacker is able to create **both** a spoof serving network **and** a spoof AAA (e.g. because the attacker knows the long-term secret K and the AKA algorithm) then this is possible. Otherwise, in the absence of such a powerful capability, even an active attacker will not be able to impersonate the network towards the UE; the attacker can only unilaterally impersonate the UE towards the network.

Further, even a powerful attacker who knows the K value and AKA algorithm must ultimately reveal his hand by generating a new N_{PUB} value. As noted above, the UE should prefer to cells which are presenting a known N_{PUB} value rather than an unknown one, which would require the active attacker to drown out all genuine surrounding cells. And if the UE finds that the **only** available cells have high power, and are presenting unknown N_{PUB} values, then this may itself be considered suspicious, and several responses are possible including: selecting a different network or protocol, switching on an additional security layer (e.g. VPN), showing a user warning, or sending the unknown N_{PUB} over https to a repository for suspicious keys. (Such a repository will collect evidence of false networks using hacked K values.)

5.2.4.6.3 Evaluation

Evaluation#1

Editor's Note: This section was updated in TR 33.899 v0.6.0 by two overlapping and conflicting pCRs, S3-162029 and S3-161890. Implementation was done by merging the content when possible. Text that was updated by one but removed by the other was kept in the TR.

Solution #2.6 is an enhancement to solution #2.2 as stated in clause 5.2.4.6. Solution #2.2 helps against purely passive attacks when the permanent key K has leaked to an attacker, as described in key issue 2.2, while solution #2.6 also helps against active attacks when the permanent key K has leaked to an attacker. In addition, like solution #2.2, solution #2.6 addresses key issue #3.1, but protects against more of the threats listed in 5.3.3.1.2.

It should also be noted that there are solutions for addressing key issue #2.2 that do not affect the establishment of air interface keys at all, e.g. solution 2.1. However, solution 2.1 does not also address key issue #3.1

It is assumed for solution #2.6 that the serving network possesses a private-public key pair, and the home network knows the public key.

Under these assumptions, also solution #2.24 applies. Solution #2.24 has the same effect as solution #2.6 in that it mitigates also active attacks.

The advantage of solution #2.24 over solution #2.6 is that the UE need not know the public key of the serving network, only the home network would need to know it. This makes distribution of the public key easier. Furthermore, there are fewer public-key operations on the air interface.

It should also be noted that there are solutions for addressing key issue 2.2 that do not affect the establishment of air interface keys at all, e.g. solution 2.1.

Lenovo Ex. 1007
Page 165

Solution #2.6 is compared against the combination of solution #2.2 and solution #10.2 as described in 2.24, noting that both solutions assume that the serving network has a public key-pair. In solution #2.6, the UE needs to know the public key of the serving network, whereas in solution #10.2 only the home network needs to know this public key. However, the cost of solution #2.6 here is minor, since a public key can be communicated in a single short message, and may be broadcast to all UEs in a cell at once to save radio resource. Further, there is no real risk of public key spoofing here: if a UE uses a false public key, it will derive an incorrect $\mathbf{K_N}$ and the authentication of the network will fail. (Also note that a number of other solutions e.g. #7.2 assume that the UE knows a public key for the serving network).

Solution #2.6 requires two more public key operations on the air interface than solution #2.2 (one signature operation, and one signature verification option), whereas solution #10.2 requires two more public key operations on the inter-operator network (one encryption and one decryption).

An ecosystem issue with Solution #10.2 is that it is only optional for the visited network to have a private/public keypair, which means that in practice many may well neglect to implement it initially (and then home networks will have to live with that, creating a dynamic where there is little or no pressure to ever implement it). Compare the situation here with that of Diameter security in LTE. Whereas solution #2.6 mandates each visited network to use a public key-pair from the start, otherwise UEs can't authenticate the network and won't attach. This mandatory use of an NPRIV/NPUB will tend to raise security of the whole NextGen ecosystem.

Editors Note: It is ffs whether the possession of a private/public keypair can be mandated for all NextGen serving networks. If so, this would be equally possible for solutions# 2.6 and 10.2. If not, then migration strategies would need to be studied; an example of migration is provided in solution #10.2

Evaluation#2

Solution 2.6 states at the beginning:

> "This solution addresses key issues 2.2 [long-term secret key leakage] and 3.1 [Interception of radio interface keys sent between operator entities]. It is an enhancement to Solution #2.2 in that it achieves the same prevention against purely passive attacks, and also makes active attacks harder."

But solution 2.6 does not achieve these goals. Any fixes to 2.6 would likely be so significant that they would rather constitute a new solution.

In more detail:

Key Issue 2.2

How does solution 2.6 try to address key issue 2.2 [long-term secret key leakage] in the presence of an active attacker?

By assumption of key issue 2.2, the attacker knows long-term secret key K used in AKA.

In solution 2.6, "CP-AU sends message 1 to UE, which contains APUB, a MAC computed using K1 and a signature computed using the serving network private key NPRIV." Here, "K1 may be derived from, the above key KN = KDF(CK||IK, Network Id, NPUB)"

As already mentioned in the penultimate paragraph of 5.2.4.6.2, nothing in this prevents an attacker from selecting a public-private key pair NPUB, NPRIV, creating the above message and sending it to the UE. There are no provisions in the protocol that would allow the UE to tell a genuine NPUB from one generated by an attacker. Likewise, the attacker can replicate the action of replacing KASME by a key KN generated by the HSS, with NPUB bound in. Hence, the attacker can mount a false network attack on the UE. The reasons is that the HSS now also binds NPUB into KN. But this does not help as the binding is done using the long-term secret key K, which, by assumption, is known by the attacker.

However, a pre-condition for this attack to succeed would be that the attacker must also drown out all surrounding cells broadcasting a genuine serving network NPUB, which may itself count as suspicious and trigger a UE response.

Also, one could try to add further provisions so that the UE can tell a genuine NPUB from a false one. Simple key continuity solutions could be enhanced further by things like serving network certificates, id-based schemes, digital signatures applied to NPUB by the home network, lists in the USIM managed by OTA etc. (Any such proposal should, of course, come with an evaluation of the system implications of using these provisions.) Any complex proposals here should be regarded as a new solution rather than an enhancement of 2.6.

Key Issue 3.1

Lenovo Ex. 1007
Page 166

How does solution 2.6 try to address key issue 3.1 [Interception of radio interface keys sent between operator entities] in the presence of an active attacker?

The network impersonation attack described above (under 'key issue 2.2) works also here unless the home network (called AAA here) has a means to authenticate the CP-AU so that the AAA knows which key to bind the authentication vectors to. (This is considered in solution 2.6 by stating that the message from CP-AU to AAA needs to 'integrity-protected' if the AAA does not already have the NPUB value. Alternatively, one way of ensuring that the AAA already knows the NPUB value would be communicating it as part of an out-of-band process at the set up or periodic refresh of a roaming agreement; this would not require any form of inter-operator PKI, whereas an in-band exchange of NPUB values probably would require such a PKI.)

Under this assumption that integrity protection can be provided between CP-AU and AAA (or under the assumption of an out-of-band key exchange), one can assume the existence of a security association between AAA and CP-AU that also allows encrypting the authentication vectors so that interception of the keys in the authentication vectors becomes no longer possible. Hence the tehnical pre-conditions to achieve solution 2.6 would also permit solution 2.10.

It is worth noting that operators would have a very strong incentive to communicate NPUB values correctly under solution 2.6, since a mistake here will lead to an incorrect NPUB being bound into authentication vectors, and a large scale failure of 5G roaming traffic between the networks. It is not at all clear that operators would have any similarly strong incentive to deploy solution 2.10, since roaming would continue to work with the encryption of AVs switched off, whereas switching encryption on might create interoperability issues. Another difference is that solution 2.6 would not be vulnerable to an active MITM on the interface between network operators, unless such a MITM also knew the K values for all roaming subscribers from the home to visited network. Solution 2.10 is potentially more vulnerable to an active MITM if the networks do not authenticate each other thoroughly when exchanging keys; in such a case, the MITM would **not** need to know any subscribers' K values to intercept the AVs.

This analysis does not affect solution 2.2, which is meant to prevent passive attacks.

5.2.4.7 Solution #2.7: Authentication framework

5.2.4.7.1 Introduction

This solution addresses key issue #2.1 Authentication framework. It is a framework for subscription authentication (as opposed to equipment authentication or (human) user authentication). It covers access to the NextGen Core via 3GPP-defined access networks, in particular E-UTRAN and NextGen-NewRadio, as well as via trusted non-3GPP access networks.

Editor's Note: Solution 3.4 shows how access via untrusted non-3GPP access networks can be included in this authentication framework in principle. However, some modification of the text and of figure 5.2.4.7.2.4-1 below are required to reflect the role of the NG-PDG.

All UEs considered here are NG-UEs, i.e. UEs that are able to communicate with a NextGen Core over the NextGen NG1 interface, cf. TR 23.799. LTE UEs are not considered here.

Editor's Note: It is ffs whether LTE UEs need to be considered.

5.2.4.7.2 Solution details

5.2.4.7.2.1 Candidate authentication methods

The present solution shows how support for

- EPS AKA
- EPS AKA* (as defined in solution #2.22)
- Any EAP method

can be provided in a uniform way.

Editor's Note: It is for further study in SA1, SA2, and SA3 whether authentication not based on AKA-credentials should be allowed in NextGen, and, if so, whether it should be allowed over 3GPP-defined access networks.

Lenovo Ex. 1007
Page 167

If authentication methods not based on AKA-credentials are admissible in NextGen then the present solution envisages that only support for such methods that are EAP methods needs to be provided, irrespective of the type of access network. Examples of EAP methods not based on AKA-credentials are EAP-TLS and EAP-TTLS.

Non-3GPP access networks:

For non-3GPP access networks attached to a NextGen core network, the present solution envisages that only support for EAP authentication methods needs to be provided, irrespective of the type of credentials used. This applies to both trusted and untrusted access.

When AKA-credentials are available in the UE then the present solution proposes to use EAP-AKA' for access over trusted non-3GPP access networks.

3GPP access networks:

The present solution describes several alternatives for authentication over 3GPP-defined access networks for the case when AKA-based credentials are used (more details in 5.2.4.7.2.5 below):

1a) EPS AKA is always used for AKA-based authentication over 3GPP-defined access networks or

1b) EPS AKA* is always used for AKA-based authentication over 3GPP-defined access networks or

2) EAP-AKA' is always used for AKA-based authentication over 3GPP-defined access networks or

3) the choice among EPS AKA, EPS AKA* and EAP-AKA' for AKA-based authentication over 3GPP-defined access networks is taken by the AUSF.

Only one of these alternatives should be standardized. If alternative 3) was selected the choice among EPS AKA, EPS AKA* and EAP-AKA' could be further narrowed down, cf. clause 5.2.4.7.2.5.

Editor's Note: If authentication methods with non-AKA credentials over 3GPP access networks are admissible in NextGen then text further above states that these methods will be EAP methods in the context of the present solution. It is expected that the suppport for any EAP method over 3GPP-defined access networks would be very similar to the support for EAP-AKA' envisaged in alternatives 2 and 3 above and detailed in 5.2.4.7.2.5.

NOTE1: The issue of EAP-AKA vs UMTS AKA has already been discussed for EPS in Rel-8, cf. TR 33.821, clause 7.2.2, and, as a result, UMTS AKA was selected, which was later enhanced to become EPS AKA. (EAP-AKA' was not available at the time when TR 33.821, clause 7.2.2, was written as EAP-AKA' was motivated by EPS AKA.) This does not imply, of course, that the outcome of this discussion should be the same for NextGen. Note also that the independence of the authentication framework from the access network was already required for EPS in Rel-8, cf. TR 23.882, clause 5, bullet 19.

NOTE2: The UE needs to support both, EPS AKA and EAP-AKA‘ anyhow: EPS AKA for legacy LTE access to the EPC (backward compatibility); EAP-AKA‘ for legacy non-3GPP access to the EPC. For the UE, there is no difference between EPS AKA and EPS AKA*.

5.2.4.7.2.2 Transport considerations

It is assumed that, for this solution, authentication messages need to be transported over three interfaces:

- UE to SEAF (Security Anchor Function; for the present solution the SEAF resides in the serving network. The EPS-equivalent of this interface is realized by the NAS protocol.)
- SEAF to AUSF (where AUSF is assumed to be in the home network.)
- AUSF to ARPF (The ARPF is always in the home network, according to clause 5.2.1.2.)

Over all three interfaces, authentication messages can be transported in a uniform fashion, independent of the particular authentication method, in the following way:

UE to SEAF:

Transport for EAP messages is provided already today over a variety of access network types, e.g. WLAN, Ethernet, and WiMAX. Transport for EAP messages is currently not defined for 3GPP-access networks, but no obstacle is seen

Lenovo Ex. 1007
Page 168

for this in principle. E.g. EAP messages and EPS AKA message could be transported over a NextGen-version of the NAS protocol in a uniform way. The messages between UE and SEAF are quite similar for EAP-AKA' and EPS AKA. The messages between UE and SEAF are identical for EPS AKA and EPS AKA*.

SEAF to AUSF:

It is envisaged that this interface is DIAMETER-based. Authentication messages relating to different authentication methods may be carried in the same or different DIAMETER AVPs.

AUSF to ARPF:

As AUSF is in the home network this interface may be identical to SWx today.

Editor's Note: The final decision over the format of the transport for authentication messages will be taken by CT1 and CT4 respectively. If EAP is carried over RRC then also RAN is to be included in the decision process.

5.2.4.7.2.3 Efficiency considerations

Identity exchanges

The EAP frameworkin RFC 3748 describes an optional EAP-method-independent identity exchange initiated by the authenticator that may be followed by an EAP-method-specific identity exchange initiated by the EAP server. These exchanges introduce additional roundtrips and conflict with the NextGen objective of increased efficiency of security procedures.

The present solution avoids the need for identity exchanges between the UE and the SEAF by including the needed identity in the Attach request sent from the UE to the MM (Mobility Management function in the serving NextGen core network).

- The subscription identifier included in the Attach request may have the form of an IMSI or a NAI, or a concealed version of an IMSI or NAI (e.g. temporary identifier or pseudonym or encrypted identifier used for enhancing user identity confidentiality). Any concealed version of an IMSI that cannot be mapped to an IMSI by the MMF is assumed to leave the MCC and MNC parts in the clear. Any concealed version of a NAI is assumed to have the information used for routing in the clear.
- The MMF forwards the identifier to the SEAF.
- If the identifier is a (concealed) IMSI then the SEAF canonically transforms it into a NAI. If the identifier is a NAI then the SEAF does not transform it.
- Then the SEAF sends a message containing the NAI obtained in the previous step to the AUSF. This message starts the authentication procedure. This message may be of the form of an EAP identity response for all authentication methods.

Editor's Note: The final definition of the Attach procedure is within the remit of SA2.

Editor's Note: Enhanced forms of subscriber identity confidentiality are still under study.

Roundtrips between serving network and home network

In general, EAP methods may have many roundtrips between authenticator (SEAF in a NextGen setting) and AUSF. In a NextGen setting, EAP-AKA' would have two roundtrips between SEAF and AUSF, while EPS AKA would have one. EPS AKA* would necessitate one additional Authentication Confirmation message to the AUSF, but the SEAF could proceed with its interaction with the UE as it would not have to wait for a response. The performance impact of the additional roundtrips for EAP methods could be reduced by

- placing a AUSF in the serving network; this would, at least for EAP-AKA', but potentially many other cases, necessitate a roaming interface between AUSF and ARPF, or between AUSF and some other form of authentication centre holding the long-term secrets. The exchange between AUSF and ARPF would consist in only one roundtrip; additional roundtrips would occur inside the serving network, which would reduce delay. This would also negatively impact the uniformity of the authentication framework as the interface between the AUSF and the ARPF will become dependent on the authentication method.

Lenovo Ex. 1007
Page 169

- using the concept of EAP Re-authentication Protocol (ERP) as in RFC 6696. With ERP, the initial authentication would necessitate the full number of roundtrips between serving and home network, as required by the EAP method; but subsequent authentications could be run between the UE and ERP server in the serving network.

Statelessness of AUSF

- For EAP methods and EPS AKA*, the AUSF needs to keep state until receiving confirmation of successful UE authentication. If statelessness is considered a performance advantage then EPS AKA may be used. For EPS AKA, strictly speaking no AUSF would be needed. If there is a AUSF for the sake of the uniformity of the authentication framework then the AUSF can simply act as a pass-through function (or rather a front-end to the ARPF), and keeping state in the AUSF would be avoided. In neither case would the ARPF have to keep state.

Computation effort

- The computation effort for EPS AKA and EPS AKA* is lower than that for EAP-AKA' for both UE and server. It is ffs whether this would be a decision criterion, e.g. for low-power UEs with very limited capabilities.

Length of messages

Editor's Note: text tba

5.2.4.7.2.4 General information flow

The following figure (5.2.4.7.2.4-1) depicts the general information flow for the present solution. The flow applies to all candidate authentication methods described in 5.2.4.7.2.1, i.e. to any EAP method used over 3GPP- or non-3GPP access networks as well as EPS AKA and EPS AKA* over 3GPP-access networks.

The information flow for the authentication procedure is described as follows:

- The flow starts with an Attach request from UE to MMF
- MMF extracts the identifier and forwards it to SEAF
- SEAF transforms identifier into NAI (if needed, cf. clause 5.2.4.7.2.3).
- SEAF and AUSF exchange one round of authentication request / response message.
    - Depending on the authentication method, AUSF requests authentication vectors or other authentication material from the ARPF, before sending the response to SEAF

Editor's Note: it is ffs whether 3rd-party authentication centres will be available in NextGen, based on service requirements.

- SEAF and UE exchange one round of authentication request / response message.
- If the authentication method is EPS AKA, the authentication procedure stops here. (In the figure below, n=1 for EPS AKA.)
- If the authentication method is EPS AKA*, the SEAF sends an Authentication Confirmation message to the AUSF, then the authentication procedure stops. (In the figure below, n=1 for EPS AKA*.)
- If the authentication method is an EAP method, SEAF and AUSF exchange further rounds of authentication request / response messages as required by the EAP method. Each such round is followed by either a Success message from SEAF to UE or a further round of authentication request / response messages between SEAF and UE. (In the figure below, n>1 for EAP methods; n=2 for EAP-AKA'.) The authentication procedure stops when the UE receives an EAP Success message.

After the completion of the authentication procedure SEAF has an intermediate key available. This intermediate key is called MSK in the case of EAP methods and K_{ASME} in the cases of EPS AKA and EPS AKA* (but the name does not matter, it is just a key). It will be used by the SCMF for deriving further keys.

The further steps in the figure are not part of the authentication procedure any more. They show for informational purposes what happens after the end of the authentication procedure (based on the corresponding steps in EPS; these steps are not known for NextGen yet).

Lenovo Ex. 1007
Page 170

- SCMF derives keys for protection of NAS signalling and forwards them to MMF via the SEAF.
- MMF runs Security Mode procedure with UE.
- MMF sends Attach Accept protected with NAS keys.

Note that neither the SEAF nor the MMF need to obtain any knowledge about the type of the access network. The choice of the authentication method is implied in the subscription identifier. So, this information flow realizes an access network-agnostic framework. More on this can be found in the next subclause 5.2.4.7.2.5.

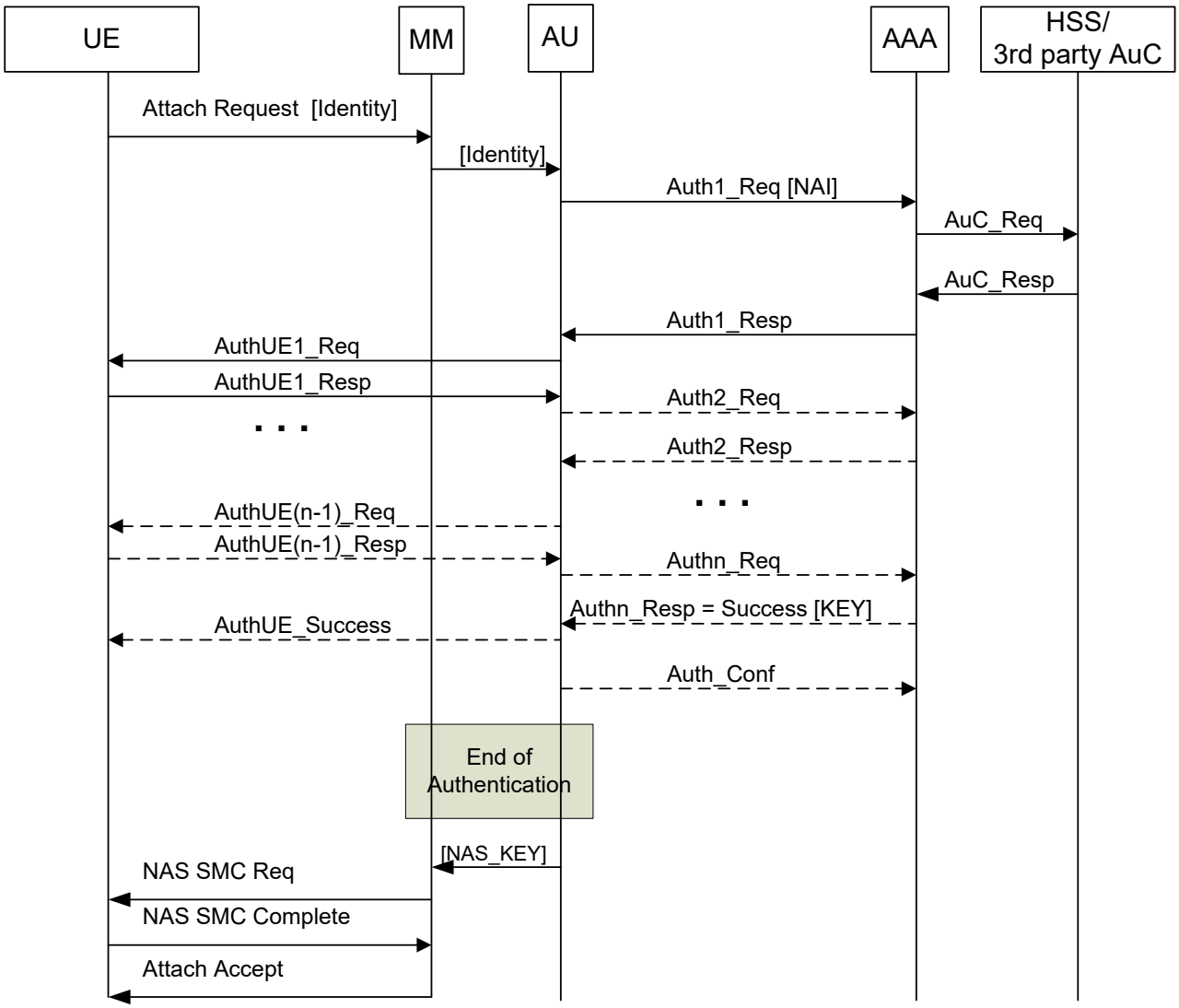


Figure 5.2.4.7.2.4-1

5.2.4.7.2.5 Alternatives for AKA-based authentication over 3GPP-defined access networks

NOTE: Depending on the alternative, the form of NAI should allow the AUSF to distinguish between protocols. An approach similar to the one for root NAIs in TS 23.003, 19.3.2, that allows distinguishing between EPS AKA and EAP-AKA', could be taken (use of different leading digits).

Alternative 1a: EPS AKA is always used for AKA-based authentication over 3GPP-defined access networks

A UE using a 3GPP-defined access network always includes IMSI in Attach request, and SEAF transforms it canonically into NAI. This transformed NAI must be of a type different from any NAI received by the AU directly from the UE. AUSF determines, based on type of NAI, that authentication method of choice is EPS AKA. From that point onwards, DIAMETER AVPs as in S6a could used between AU and AAA (but this is within the remit of CT4). SEAF

Lenovo Ex. 1007
Page 171

determines, based on received DIAMETER AVP, that this is the case of EPS AKA, i.e. it runs one authentication request /response roundtrip with the UE, which completes the authentication.

If the AUSF determines, based on the NAI, that the authentication method is an EAP method, it acts as an EAP server. The SEAF recognises from the response from the AUSF that this is the case of an EAP method and SEAF acts according to the EAP framework. (This then implies, according to the assumption for Alternative 1, that the access network is non-3GPP, but the AUSF server need not know this.)

Alternative 1b: EPS AKA is always used for AKA-based authentication over 3GPP-defined access networks*

A UE using a 3GPP-defined access network always includes IMSI in Attach request, and SEAF transforms it canonically into NAI. This transformed NAI must be of a type different from any NAI received by the AU directly from the UE. AUSF determines, based on type of NAI, that authentication method of choice is EPS AKA*. From that point onwards, DIAMETER AVPs as in S6a could used between AU and AAA (but this is within the remit of stage 3). SEAF determines, based on received DIAMETER AVP, that this is the case of EPS AKA*, i.e. it runs one authentication request /response roundtrip with the UE and sends an Authentication Confirmation message back to the AUSF, which completes the authentication.

If the AUSF determines, based on the NAI, that the authentication method is an EAP method, it acts as an EAP server. The SEAF recognises from the response from the AUSF that this is the case of an EAP method and SEAF acts according to the EAP framework. (This then implies, according to the assumption for Alternative 1b, that the access network is non-3GPP, but the AUSF server need not know this.)

Alternative 2: EAP-AKA' is always used for AKA-based authentication over 3GPP-defined access networks

A UE using a 3GPP-defined access network always includes NAI in Attach request, as used in EAP. SEAF forwards NAI unchanged. (Variant: UE includes IMSI and SEAF transforms it canonically into NAI. Note that the latter would have the advantage of making the Attach request shorter as an IMSI is typically shorter than NAI.) AUSF decides, based on NAI, that EAP method of choice is EAP-AKA‘. EPS AKA does not occur at all in this alternative, so SEAF acts according to the EAP framework.

Alternative 3: The choice between EPS AKA, EPS AKA and EAP-AKA' for AKA-based authentication over 3GPP-defined access networks is made by the AUSF*

A UE using a 3GPP-defined access network always includes IMSI and SEAF transforms it canonically into NAI. This transformed NAI must be of a type different from any NAI received by the SEAF directly from the UE. AUSF determines, based on type of NAI, that either some sort of EAP method shall be used or a choice has to be made between EPS AKA, EPS AKA*, and EAP-AKA'. In the latter case, AUSF decides (presumably based on overall policy and not on a per-UE basis) whether to use EPS AKA, EPS AKA*, or EAP-AKA‘. SEAF acts depending on the DIAMETER AVP(s) in the received response.

Editor's Note: In case alternative 3 is selected, it is ffs whether the AUSF should have the choice among the three protocol variants EPS AKA, EPS AKA*, and EAP-AKA', or whether the standard should rule out one of EPS AKA and EPS AKA*.

Editor's Note: For all three alternatives in this subclause, compliant UE behaviour is assumed. It is ffs whether network-side policing for non-compliant UEs trying to use a different authentication method (e.g. non-AKA-based EAP method) would be required.

5.2.4.7.3 Evaluation

Security:

- No attacks on EAP-AKA' nor on EPS AKA are known that would speak against the use of these protocols in NextGen. EPS AKA* is a new proposal, but it is believed that it is at least as strong as EPS AKA; more can be found in the evaluation section of solution #2.22.
- EAP-AKA' and EPS AKA* offers some additional security compared to EPS AKA in that it provides proof to the home network that the subscriber was actually present in the authentication whereas in EPS AKA the home network has to trust the visited network in this respect. However, this proof provided by EAP-AKA' and EPS AKA* cannot guarantee the subscriber's continued involvement in any communication following the completion of the authentication procedure. The relevance of this security property for NextGen is ffs.

Handovers and idle mode mobility within NextGen and with other RATs:

Lenovo Ex. 1007
Page 172

- It should be studied whether there are any advantages associated with the use of EAP-AKA' or EPS AKA or EPS AKA* in this respect.

Backward compatibility to LTE:

- For services like wireless broadband access and VoLTE, AKA has been proved to be an applicable way for authentication and key distribution and negotiation. It may be necessary to reuse the mechanism since it's widely supported in core network, terminal and proved to be effective in previous communication systems. If EPS authentication is not supported, users who are only allowed to access a fully next generation network and may not be able to roam back to an LTE network or may not be able to access the next generation network that is tunnelled via LTE network. It is expected that the initial deployments of next generation systems will be an overlay system.

Possibility of enhancements and 3GPP control:

- It should be also borne in mind that EPS AKA and EPS AKA* are under complete control of 3GPP, which may facilitate future enhancements if needed. On the other hand, EAP methods are under the control of the IETF, and the IETF WG "EAP Method Update" has the status "concluded".

Editor's Note: This solution shall be evaluated against the new key issue #2.11.

5.2.4.8 Solution #2.8: Authentication Framework based on EAP

5.2.4.8.1 Introduction

This solution addresses key issue # 2.1.

When considering EAP for NextGen System (based on unified authentication framework under consideration in the TR 23.799 [2]), it is essential to consider the location of the authentication entities (for example, authenticator) and the encapsulation protocol for EAP transportation.

5.2.4.8.2 Solution details

5.2.4.8.2.1 Authentication Entities and their location in the Next Generation System

5.2.4.8.2.1.1 Alternative 1: Authentication using direct interface between the UE and the SEAF

Based on the potential security requirement in clause 5.1.3.2.3 of this TR, the EAP authenticator functionality specified in the RFC 3748 [21], needs to be in the core network (in an operator's network, which is not exposed to unauthorized physical access) and not at the edge of the network (exposed locations). The authenticator functionalities are performed by the SEAF. The EAP server is the AUSF (backend authentication server). The SEAF operates as a "pass-through authenticator" and forwards the EAP messages from the NextGen UE to the AUSF and vice versa. The New Radio (NR) access technology relays the EAP messages from the NextGen UE to the SEAF and vice versa. The SEAF decides to allow access to the NextGen UE.

Lenovo Ex. 1007
Page 173

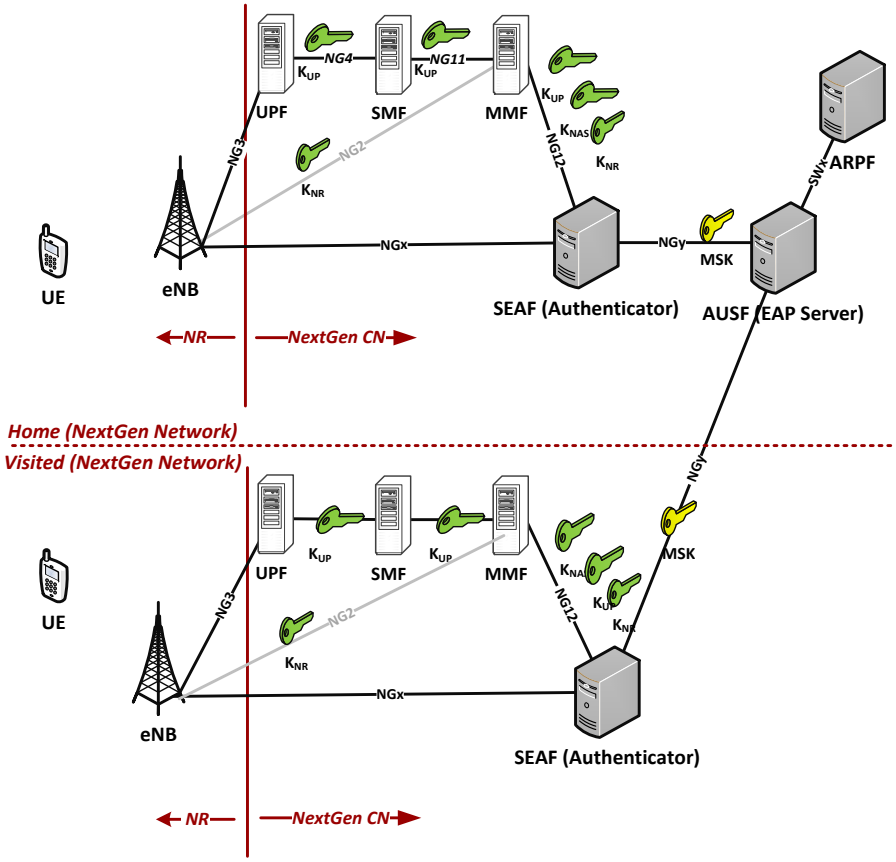


Figure 5.2.4.8.2.1.1-1: EAP based Authentication Framework for Next Generation System

Figure 5.2.4.8.2.1.1-1 depicts the authentication framework for the NextGen System. The mutual authentication is performed between the NextGen UE and the AUSF via the SEAF. The SEAF interfaces with the AUSF for carrying out the authentication. The SEAF is configured with the relevant information for routing of the authentication request to the appropriate AUSF. The AUSF interfaces with the ARPF to retrieve the authentication information and subscription details. The authentication signalling may pass through AUSF proxies in the visited network. The NextGen UE interfaces with the SEAF via the NR, for authentication procedures.

Unlike the existing mechanisms in 3GPP system, the NextGen System authentication procedure is separated from mobility management and session management procedures. Performing authentication procedure independently allows decoupling and independent evolution of CN/AN and also supports decoupling of authentication server functionality from MM and SM functionality in the network, so that if required the MM and SM functionality can be moved towards the NR.

After the successful mutual authentication, the SEAF obtains the keying material from the AUSF and provides the security context to the NR entity(s) and other core network entities for communication protection. The NextGen UE performs the mobility management and session management procedures, after successful authentication and security association establishment procedure.

EAP encapsulation protocol

FIG. 5.2.4.8.2.1.1-2 shows the authentication encapsulation protocol for NextGen system. RRC and NG2 signalling protocol encapsulates the EAP payloads between the UE and the SEAF. The NR access network performs relay functionality for the EAP payloads. The NR takes care of filtering of packets from the non-authenticated NextGen UEs. The NR allows only the EAP messages to pass through until it receives the security context from the core network.

Lenovo Ex. 1007
Page 174

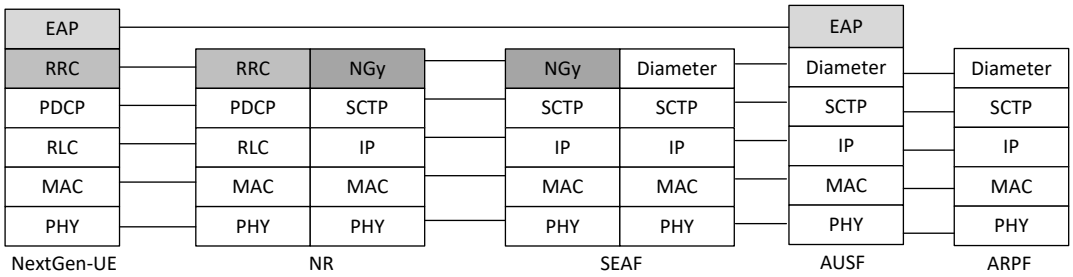


Figure 5.2.4.8.2.1.1-2: EAP based Authentication Framework for Next Generation System

Editor's note: The protocol stack needs to be revisited based on the progress in other working groups.

Editor's note: Currently this solution assumes NGy is similar to S1-AP. Needs to be revisited based on the progress in other working groups.

Editor's note: Interface NGx needs to be defined

Message Flow

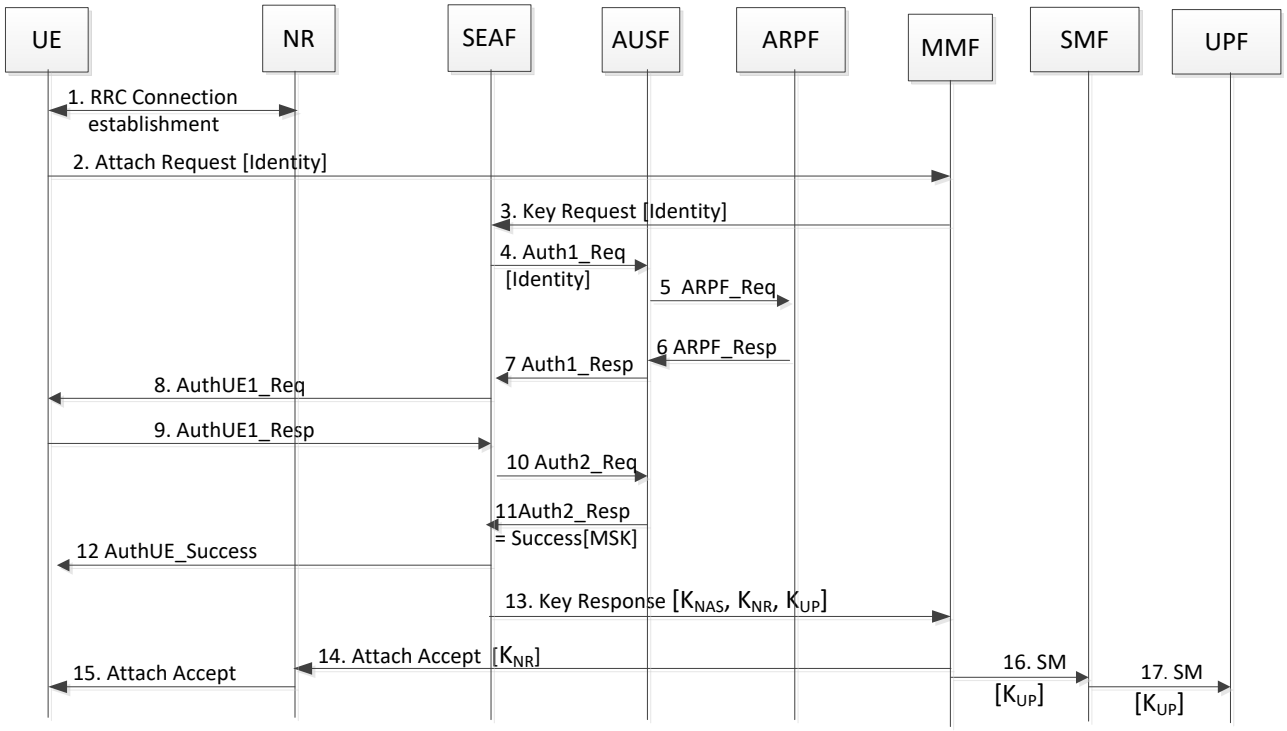


Figure 5.2.4.8.2.1.1-3: Authentication procedure during Initial Attach

The message flow for the authentication procedure is as follows:

1. The NextGen UE performs the RRC connection establishment procedure with the NR.

2. After RRC connection establishment, the NextGen UE initiates the Attach procedure with the MMF by sending the Attach request message. The NextGen UE includes the identity with the Attach request message.

3. On receiving the Attach request message from the NextGen UE, the MMF sends the key request message to the SEAF (as there is no security context available with the MMF).

4-12. The SEAF initiates the EAP authentication procedure by requesting the authentication credentials from the ARPF. The EAP Authentication is performed between the UE and the AUSF. The number of EAP message exchanges between the UE and the AUSF and AUSF and the ARPF, depends upon the EAP Method. At the end of the successful authentication procedure, the SEAF obtains intermediate key (MSK) from the AUSF.

Lenovo Ex. 1007
Page 175

If the NextGen UE is already authenticated with the SEAF and if the intermediate key is valid, then the SEAF provides the Keys (Step 13), without performing the authentication (Steps 4-12).

13. The SEAF derives further keys [K_{NAS}, K_{NR}, K_{UP}] and provide these derived keys to the MMF in Key response message. SCMF is always co-located with the SEAF.

14-15. The MMF provides the key [K_{NR}] to the NR. The NR further derives the request key to protect the AS messages and also UP packets, based on configuration.

16-17. If the UP security terminates at the UPF, then the MMF provides the key [K_{UP}] to the UPF via the SMF during session establishment procedure.

Illustrative example on performing EAP-TLS by non-human IoT deployments

This illustrative example details the alternative authentication methods with certificate as credentials, under operator control, for 3GPP network access for machine type devices used for non-human IoT deployments.

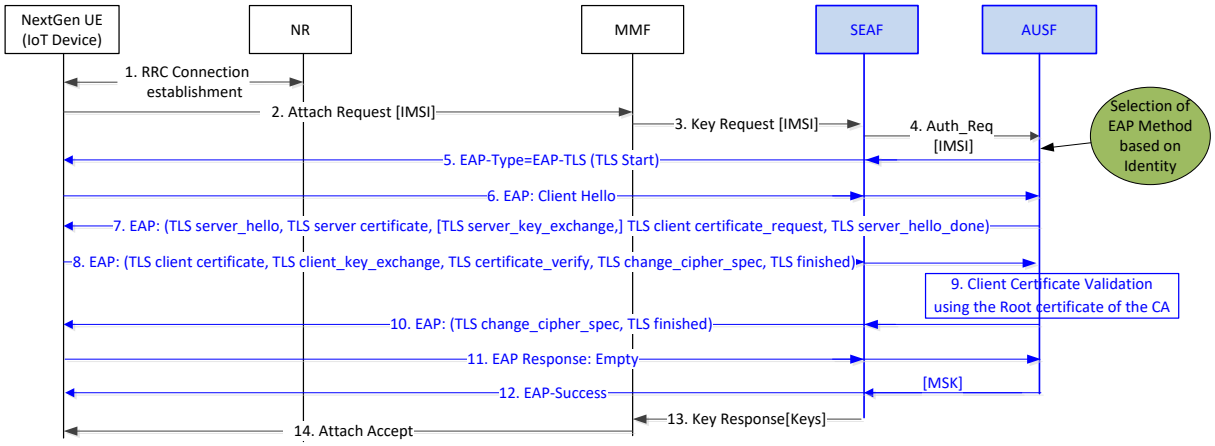


Figure 5.2.4.8.2.1.1-4:

Steps 5 to 12 details the EAP-TLS as described in RFC 5216 [23]. The authentication is performed using the subscription certificate in the UE and the server certificate issued by Certificate Authority (may be owned by the operator or trused by the operator). The private key corresponding to the subscription certificate is securely stored in the UE (may be using the solution agreed for Security area #5: Security within NG-UE). At step 9, the AUSF can validate the subscription certificate using the Root Certificate of the CA. The need for ARPF for the EAP-TLS to validate the subscription certificate is implementation specific.

Editor's note: In this example, at what step authorization is performed by the network is FFS.

5.2.4.8.2.1.2 Alternative 2: Authentication using NG1 interface

Based on the potential security requirement in clause 5.1.3.2.3 of this TR, the EAP authenticator functionality specified in the RFC 3748 [21], needs to be in the core network (in an operator's network, which is not exposed to unauthorized physical access.) and not at the edge of the network (exposed locations). The authenticator functionalities are performed by the SEAF. The EAP server is the AUSF (backend authentication server). The SEAF operates as a "pass-through authenticator" and forwards the EAP messages from the NextGen UE to the AUSF and vice versa. The New Radio (NR) access technology relays the EAP messages from the NextGen UE to the SEAF and vice versa. The SEAF decides to allow access to the NextGen UE. In roaming scenario, the visited SEAF directly interface with the home AUSF.

Lenovo Ex. 1007
Page 176

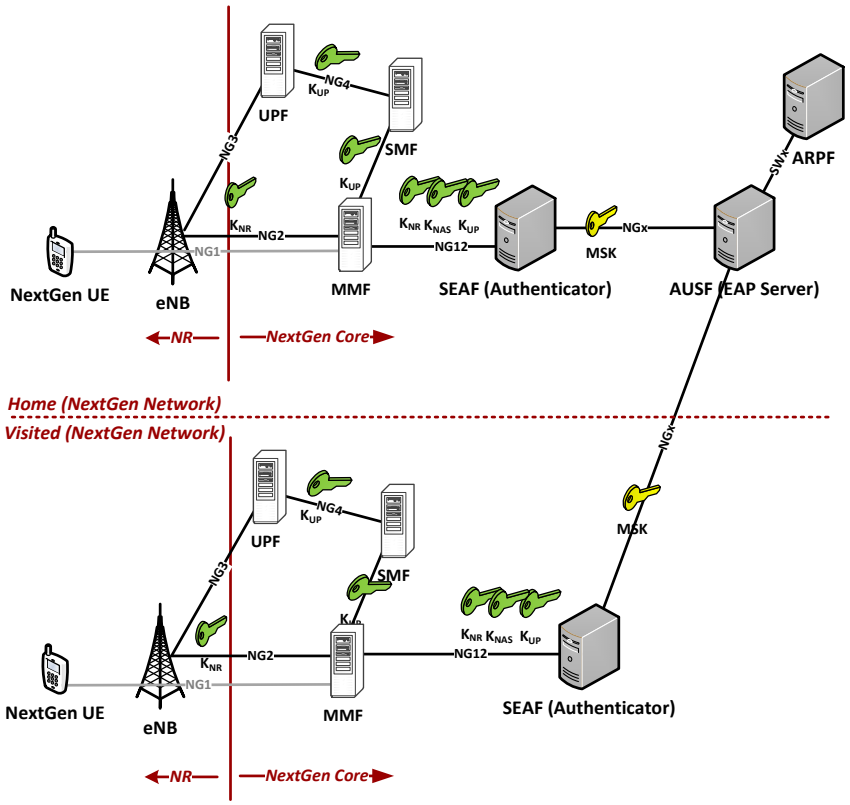


Figure 5.2.4.8.2.1.2-1: EAP based Authentication Framework for Next Generation System

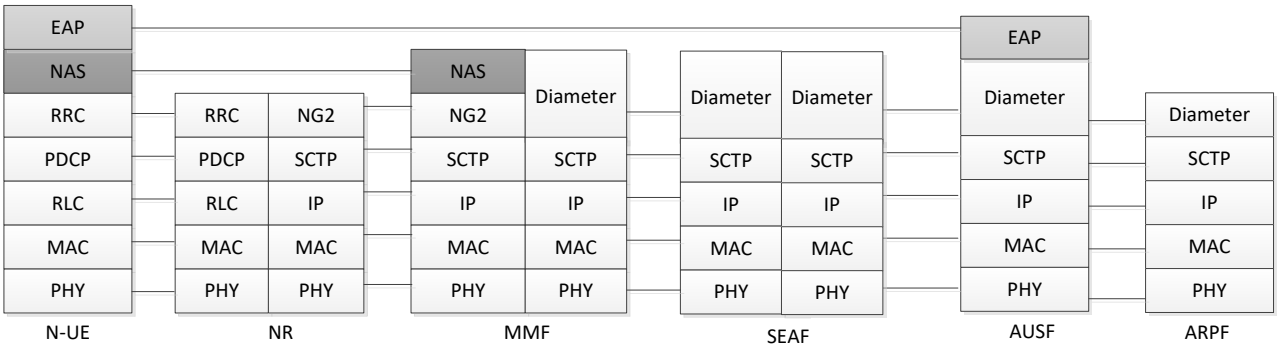
Editor's note: Interface NGx needs to be defined.

Figure 5.2.4.8.2.1.2-1 depicts the authentication framework for the NextGen System. The mutual authentication is performed between the NextGen UE and the AUSF via the MMF and the SEAF. The SEAF interfaces with the AUSF for carrying out the authentication. The SEAF is configured with the relevant information for routing of the authentication request to the appropriate AUSF. The AUSF interfaces with the ARPF to retrieve the authentication information and subscription details.

Alike the existing mechanisms in 3GPP system, the NextGen System authentication procedure is performed along with the mobility management procedures during initial attach procedure. After the successful mutual authentication, the SEAF obtains the keying material from the AUSF and provides the security context to the NR entity(s) and other core network entities for communication protection. If the UP security is terminated between the UE and the UPF, then the key K_{UP} for protecting the UP is provided to the UPF by the MMF via the SMF.

EAP encapsulation protocol

FIG. 5.2.4.8.2.1.2-2 shows the authentication encapsulation protocol for NextGen system. NAS signalling protocol (over the NG1) encapsulates the EAP payloads between the UE and the SEA. The NR access network performs relay functionality for the EAP payloads. The NR takes care of filtering of packets from the non-authenticated NextGen UEs. The NR allows only the EAP messages to pass through until it receives the security context from the core network.



Lenovo Ex. 1007
Page 177

Figure 5.2.4.8.2.1.2-2: Protocol stack for EAP based Authentication Framework for Next Generation System

Message Sequence

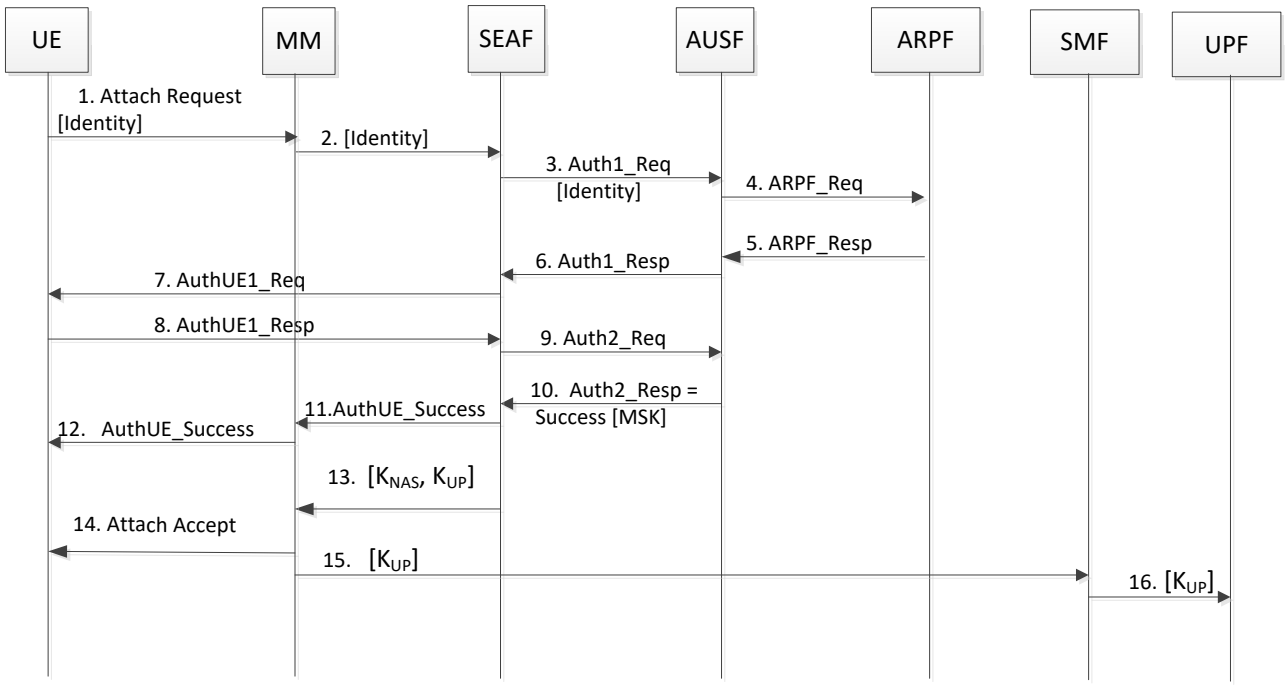


Figure 5.2.4.8.2.1.2-3: Authentication procedure during Initial Attach

The message flow for the authentication procedure is identical to the flow detailed in 5.2.4.8.2.1.1-3, except the EAP Messages (Step 7, 8 and 12) are via MMF in this alternative, whereas in 5.2.4.8.2.1.1-3, EAP Messages (Step 8, 9 and 12) are between the UE and the SEAF directly.

Illustrative example on performing EAP-TLS by non-human IoT deployments

This illustratiove example details the alternative authentication methods with certificate as credentials, under operator control, for 3GPP network access for machine type devices used for non-human IoT deployments.

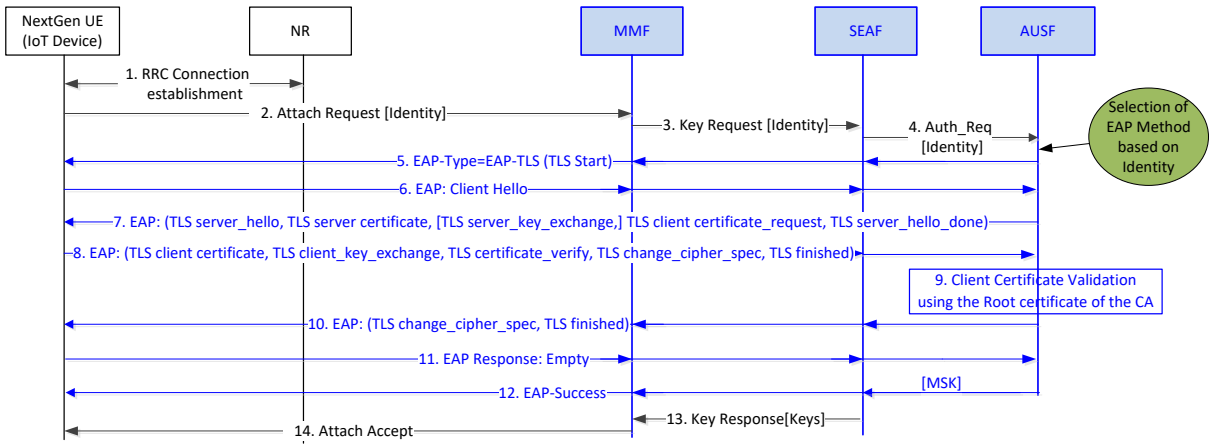


Figure 5.2.4.8.2.1.2-4:

Steps 5 to 12 details the EAP-TLS as described in RFC 5216 [23]. The authentication is performed using the subscription certificate in the UE and the server certificate issued by Certificate Authority (may be owned by the operator or trused by the operator). The private key corresponding to the subscription certificate is securely stored in the UE (may be using the solution agreed for Security area #5: Security within NG-UE). At step 9, the AUSF can validate the subscription certificate using the Root Certificate of the CA. The need for ARPF for the EAP-TLS to validate the subscription certificate is implementation specific.

Lenovo Ex. 1007
Page 178

Editor's note: In this example, at what step authorization is performed by the network is FFS.

5.2.4.8.3 Evaluation

5.2.4.9 Solution #2.9: EAP authentication framework

5.2.4.9.1 Introduction

This solution addresses key issues #2.1 Authentication framework, #2.3: Authentication identifiers and credentials, #2.5: Non-AKA-based authentication and #2.11: Increasing home control in roaming situations.

Editor's note: The use of this solution with network slicing is FFS.

This solution assumes that the NextGen system requires an authentication framework that is capable of delivering more than one authentication mechanism in a uniform way. The purpose is to further explore how the Extensible Authentication Protocol (EAP) [21] could be deployed in NextGen system.

Some reasons for making the EAP framework appealing for NextGen system are:

- EAP would make the integration of non-3GPP and 3GPP accesses easier by introducing a uniform framework for all accesses.

- EAP would facilitate new use cases, and business opportunities for Mobile Operators. EAP would make it easier to integrate various authentication methods into the system. Such methods may be needed to support use cases related to new types of actors, such as factories or corporations, using their own identity management, credentials and authentication methods in the authentication process to access the 3GPP network.

Editor's note: Interworking with and migration from earlier 3GPP network(s) is FFS.

5.2.4.9.2 Solution details

5.2.4.9.2.1 Introduction

NOTE: In order to make the solution more readable to people familiar with earlier 3GPP protocols, this solution refers to NAS protocol and messages in order to demonstrate the principles of the solution. These messages should be taken examples.

This solution assumes the presence of the following functions involved in the authentication:

- Authentication Credential Repository and Processing Function (ARPF)
- Authentication Server Function (AUSF)
- Security Anchor Function (SEAF)
- Security Context Management Function (SCMF)

The EAP authentication framework is presented as a collection of generalized phases that can be referred to and discussed separately in the solution. There are several ways to deploy the EAP framework for authentication, and some deployments and network configurations may be more optimized than others. This solution analyses different options of deploying EAP into the NextGen.

The generalized phases are:

1. Identity exchange
2. Optional EAP method specific identity exchange
3. Rest of EAP method specific signalling (including the signalling with the potential back-end server)
4. EAP Success/Failure and exchange of the Authentication Root Security Key (ARSK) over AU-SCKM interface.

The connection establishment (phase 0 in Figure 5.2.4.9.2-1) or how the ARSK is used between the UE and the CN are out of the scope of the solution.

Lenovo Ex. 1007
Page 179

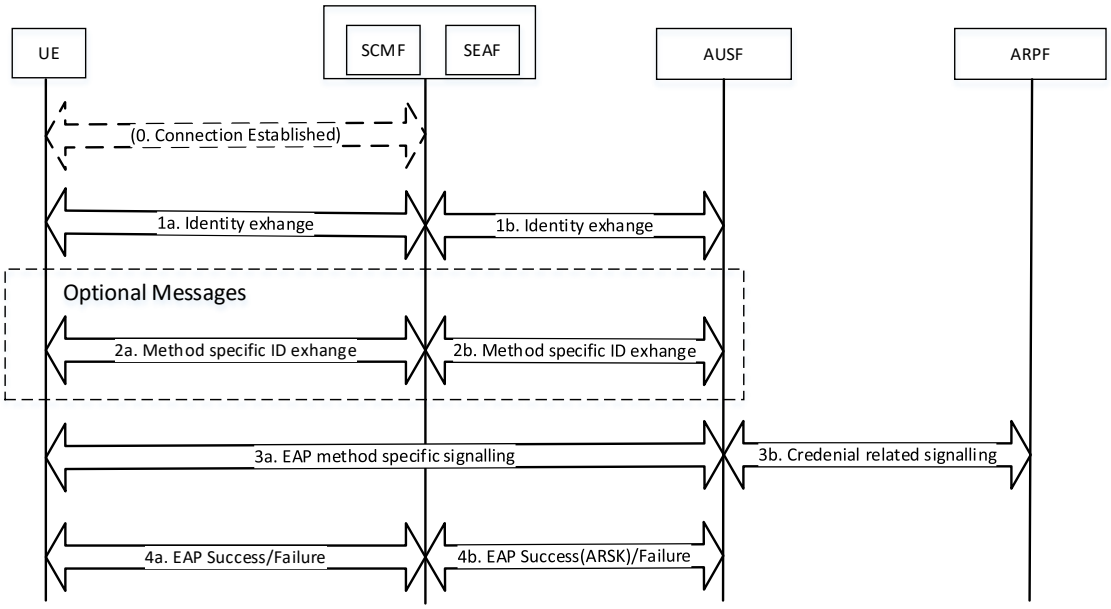


Figure 5.2.4.9.2-1: Generalized EAP framework

NOTE: EAP assumes unreliable transport. This means that the authenticator may retransmit Requests that have not yet received Responses. Since EAP defines its own retransmission behavior, it is possible for the retransmission to occur both in the lower layer (e.g. NG "enhanced NAS" or equivalent) and the EAP layer. However, this aspect is out of the scope of the present document. 5.2.4.9.2.2 Phase 1: Identity exchange

EAP framework provides an initial set of EAP Types used in Requests/Responses exchanges. Identity is one of EAP Types, and it is mandatory in all EAP implementations. However, it is optional to use within the EAP conversation. The identity information can be sent by using means outside EAP.

The purpose of the (initial) EAP identity exchange is mainly to locate the right AAA server that is able to authenticate the UE, and to choose the correct EAP method. In theory, the first identity presented by the UE could be abbreviated or encrypted identity as long as it identifies the AAA Server. The exact content of the identity response may depend on EAP method or deployment.

Variant p1-1: Front-end identity exchange within EAP conversation

In this variant, illustrated in Figure 5.2.4.9.2.2-1, the identity exchange is done within the EAP conversation. More precisely, after the connection establishment, the SCMF/SEAF sends the EAP Identity Request to the UE (Figure 5.2.4.9.2.2-1 assumes that an enhanced NAS protocol (eNAS) is used to carry EAP packets). The UE responds with its identity in the EAP response. Afterwards, the SCMF/SEAF initiates the Diameter EAP application with the AUSF.

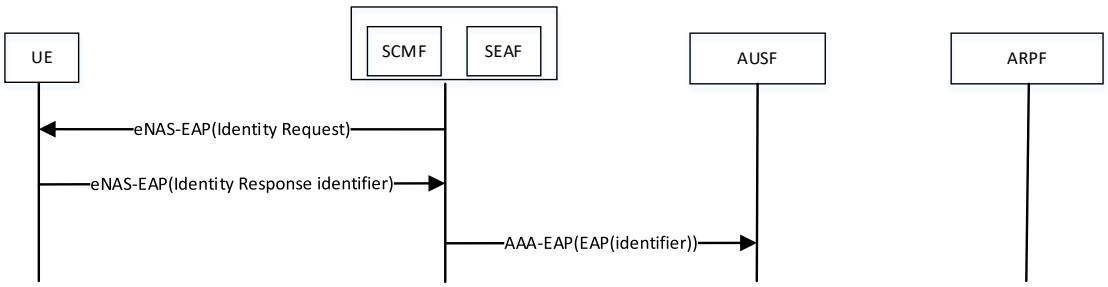


Figure 5.2.4.9.2.2-1: EAP identifier carried within EAP conversation

Lenovo Ex. 1007
Page 180

Variant p1.2: Identity exchange in eNAS Attach

In variant p1.2 shown in Figure 5.2.4.9.2.2-2, the identity exchange is done outside EAP conversation. The UE sends an Attach (or an equivalent) with the identity, and the SCMF/SEAF initiates the EAP conversation with the AUSF.

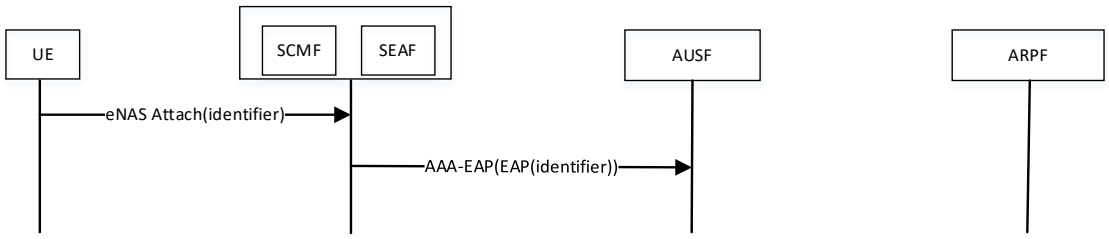


Figure 5.2.4.9.2.2-2: EAP identifier carried outside EAP conversation

5.2.4.9.2.3 Phase 2: Optional EAP method specific identity exchange

The AUSF may send another Identity Request to the UE in case it is not able to choose the appropriate EAP authentication method, or identify the UE if required before proceeding with the authentication. The identifier used in the initial identity response may be different than the one used for authentication within the EAP method (e.g. for privacy reasons). The optional identity exchange is demonstrated in Figure 5.2.4.9.2.3-1.

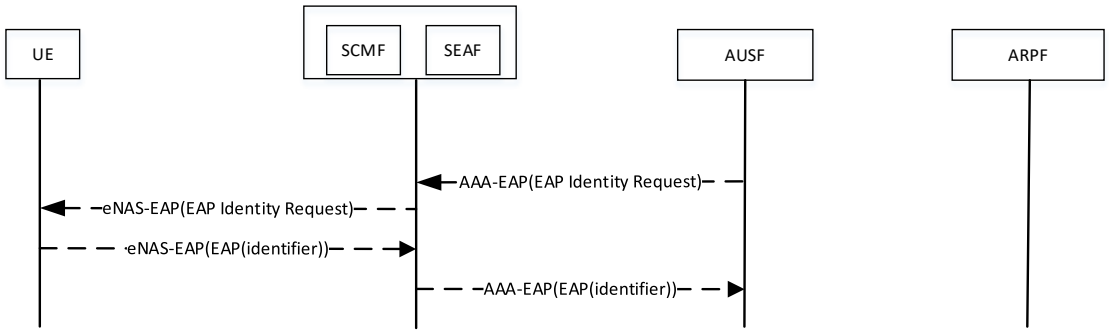


Figure 5.2.4.9.2.3-1: Optional EAP method specific identity exchange

5.2.4.9.2.4 Phase 3: Rest of EAP method specific signalling

The EAP authentication methods have different number of round-trips but they all run end-to-end authentication between the UE and the AUSF. The intermediate nodes are typically just pass-through entities. Nevertheless, it is also possible that the intermediate nodes implement some EAP methods locally, and that the authentication is terminated closer to the serving network.

NOTE: It is often assumed that the home control of authentication is an inseparable characteristic of the EAP-architecture i.e. the AAA-server (AUSF) always resides in the Home Network. However, more flexibility on the termination of EAP methods could be possible if EAP methods were implemented in the Visited Network, and the Home Network acted as a back-end server (cf. LTE). Similar deployment model in which EAP was terminated in MME was considered in TR 33.821.

Variant p3.1: EAP-AKA'

This solution assumes that it would be beneficial to specify only one AKA variant for Next Generation. The proposal is that this would be EAP-AKA'. There might be backwards compatibility reasons for the UE to support both EAP-AKA' and EPS AKA. However, support of both is not necessary for the Next Generation CN.

Lenovo Ex. 1007
Page 181

EAP-AKA' is already used in TS 33.402 [22] for non-3GPP accesses. In figure 5.2.4.9.2.4-1, the AUSF is terminating the EAP-AKA' conversation and requesting AKA AVs from the ARPF. EAP-AKA' Request and Response messages are exchanged between AUSF and UE.

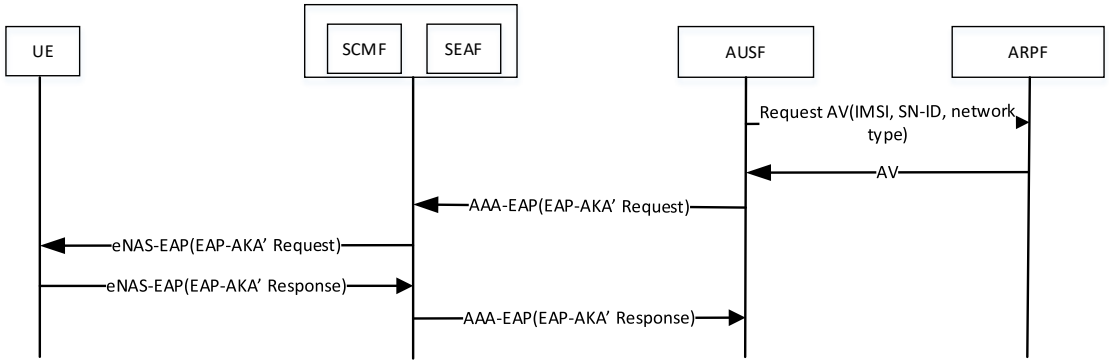


Figure 5.2.4.9.2.4-1: EAP method specific signalling – EAP-AKA'

Variant p3.2: EAP-TLS

Alternative authentication methods are being discussed in the co-called "Factory" use case [4]. It is assumed that the NextGen system is owned by a third party, and that third party would need to use alternative authentication methods with different types of credentials. The EAP framework provides means to use alternative methods with different types of credentials.

This variant assumes that the authentication is done using existing third party credentials and identity management system. In other words, the AUSF function performing the authentication may be owned and managed by a third party (the Factory owner). The exact details of the authentication method are transparent to the SCMF/SEAF, and any other EAP method (than EAP-TLS) could be used if agreed between the Factory and the mobile operator.

EAP-TLS described in RFC 5216 [23] is based on TLS 1.1. The protocol itself includes the TLS version number, so in theory any TLS version above 1.1 could be used. TLS version is important because modern TLS variants are secure and more optimized than the older variants. The IETF TLS working group is currently working to finalize TLS version 1.3 [aa] with the target to published as RFC during the beginning of 2017. TLS version 1.3 significantly reduces that number of roundtrips.

Figure 5.2.4.9.2.4-2 demonstrates the initial EAP-TLS handshake done between UE and AUSF. Authentication is done by using both server and client certificates, and requires a root of trust (i.e. certificate authority, CA). After the initial handshake, EAP-TLS session can be "resumed" making the handshake more efficient.

Lenovo Ex. 1007
Page 182

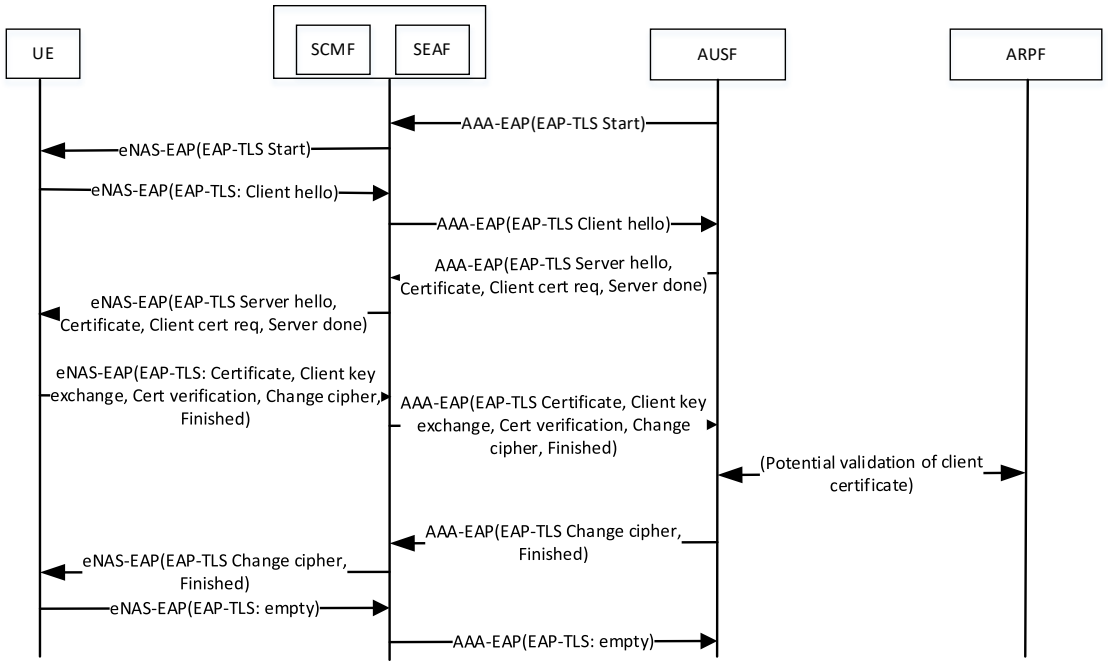


Figure 5.2.4.9.2.4-2: EAP method specific signalling – EAP-TLS

Variant p3.3: EAP-TTLS

Another alternative authentication method is EAP-TTLS. EAP-TTLS is an EAP type that utilizes TLS to establish a secure connection between a client and server, through which additional information may be exchanged. There are two versions of EAP-TTLS: EAP-TTLSv0 and EAP-TTLSv1. EAP-TTLSv0 is described in RFC 5281 [58] and EAP-TTLSv1 is described in an Internet draft [59]. Note that the use of TLS 1.3 [57] would also significantly reduce the number of roundtrips.

Figure 5.2.4.9.2.4-3 demonstrates the EAP-TTLS handshake done between UE and AUSF. During the handshake phase the server is authenticated to the client using server certificate, and requires a root of trust (i.e. certificate authority, CA). In version 1, an extension to TLS, called TLS/IA [60], is utilized. TLS/IA provides an extended handshake which guarantees that the TLS handshake endpoint and the authentication endpoint are one and the same. This eliminates attacks against tunnelled protocols for inner authentication that generates session keys. During the data phase, the client is authenticated to the server using an authentication method encapsulated within the secure tunnel. EAP-TTLS allows legacy password-based authentication protocols to be used against existing authentication databases. The encapsulated authentication mechanism may itself be EAP, PAP, CHAP, MS-CHAP or MS-CHAP-v2.

Lenovo Ex. 1007
Page 183

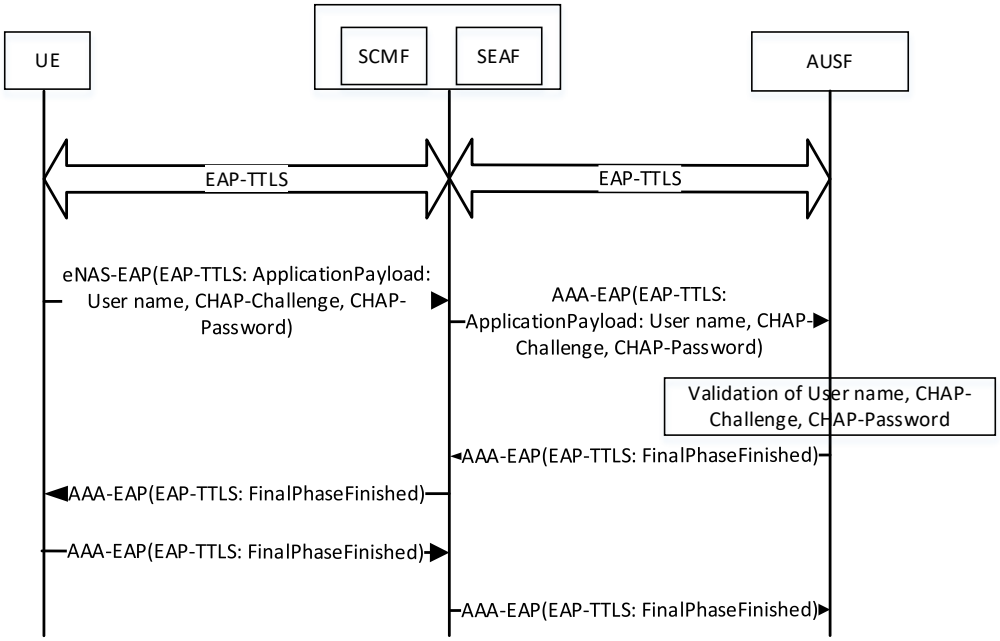


Figure 5.2.4.9.2.4-3: EAP method specific signalling – EAP-TTLS

5.2.4.9.2.5 Phase 4: EAP Success/Failure and exchange of the ARSK

The EAP Success/Failure messages are part of the EAP authentication layer. These messages are not delivered to the EAP method. It is important that these messages are sent over reliable transport because they are not retransmitted by the authenticator. It is also important that the SCMF/SEAF understands the semantics of these messages because the EAP Success message carries the master security key ARSK, and the EAP Failure means unsuccessful authentication, and potentially an unauthorized UE.

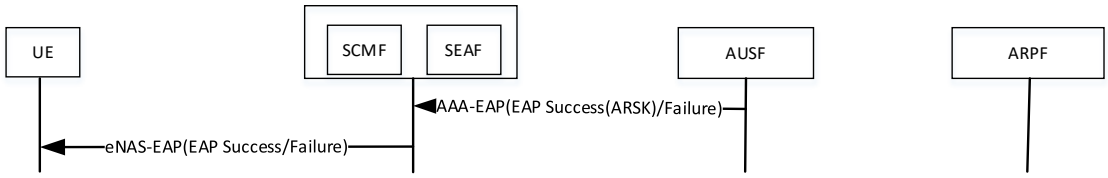


Figure 5.2.4.9.2.5-1: EAP Success or EAP Failure

5.2.4.9.2.6 Fast re-authentication with ERP

Editor's note: It is FFS if ERP is needed in addition to security anchor function. A separate evaluation for 3gpp and non-3gpp accesses would be needed.

TR 33.821 [24] focused on evaluating EAP-AKA only, and considered the method specific fast re-authentication as one option to optimize the procedure. There has been further progress in IETF on a EAP method independent framework for re-authentication that should be further analysed from Next Generation point of view. RFC 6696 [25] specifies the EAP extension for EAP re-authentication protocol (ERP). ERP is common for all EAP based authentication methods and can be used for efficient re-authentication between the peer and EAP re-authentication server. The re-authentication server may locate in the visited network.

Figure 5.2.4.9.2.6-1 assumes local ERP server in the visited network. In this scenario, the SCMF and SEAF are co-located in CN-CP (cf. MME), and a new node AUSF-VN (cf. AAA proxy) has been added to the VN. As a result of EAP/ERP run, there will be two keys in the visited network, the Domain-Specific Root Key (DSRK) in the AUSF-VN,

Lenovo Ex. 1007
Page 184

and the Master Session Key (MSK1) in the SEAF (i.e. EAP authenticator). The domain specific Master Session key is taken into usage by making a EAP-Initiate exchange between the UE and the AUSF-VN (not shown in the figure). The separate ERP run serves the purpose of NG-UE and the ERP server (i.e. typically a AAA proxy) to proof the possession of the DSRK, and the delivery of domain specific master key rMSK1 to EAP/ERP authenticator.

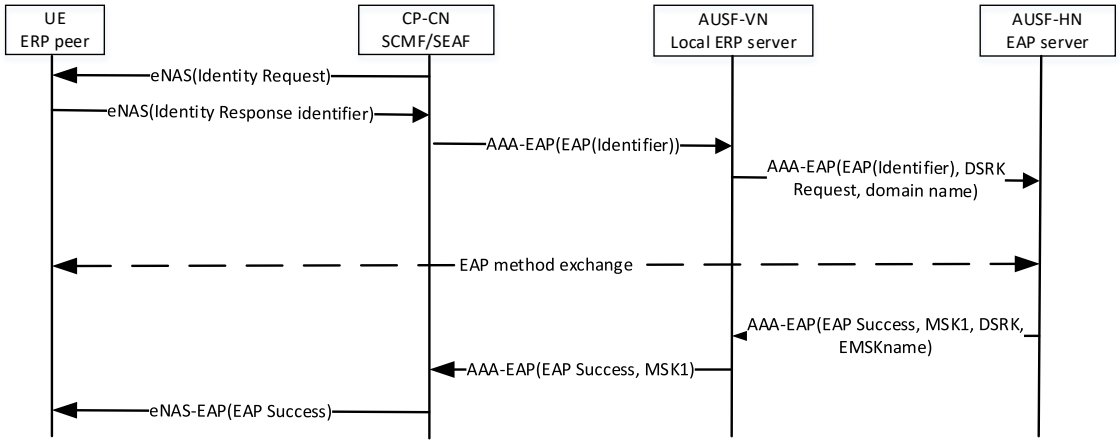


Figure 5.2.4.9.2.6-1: Implicit bootstrapping of local ERP server between SEAF and AUSF-HN

After the bootstrapping phase, ERP could be used in NextGen system to provide faster re-authentication, for example if/when the security end-point (i.e. CP-CN) in the network side is changing. In figure 5.2.4.9.2.6-2, the new CP-CN. is fetching new master key (rMSK2) from AUSF-VN. Note that the old CP-CN may also forward keying material to new CP-CN, and re-authentication may not be needed.

It is assumed that UE is in possession of the domain name of AUSF-VN/Local ERP Server before triggering the ERP exchange with the new CP-CN. The UE learns the presence of a local ER Server and its domain either as specified in RFC 6696 or through some other means outside ERP.

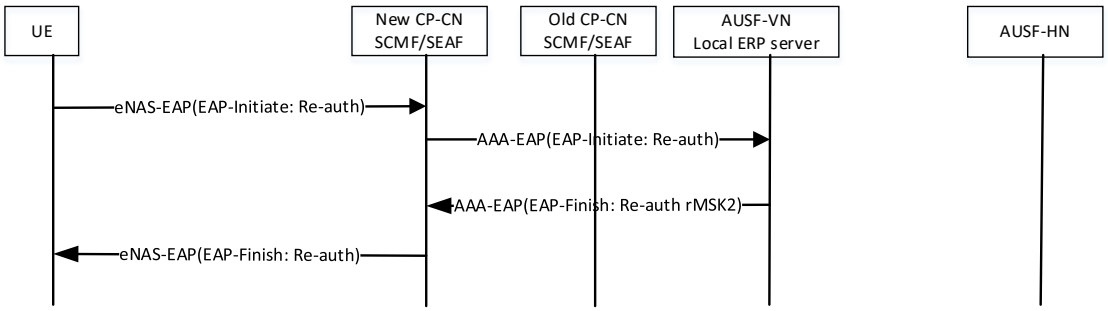


Figure 5.2.4.9.2.6-2: Re-authentication using ERP

5.2.4.9.3 Migration and interworking with LTE/eLTE

The NG-UE supporting interworking with EPC would need to support EPS AKA, and EAP-AKA or EAP-AKA' if access via non-3GPP accesses are also supported.

It seems that AUSF needs to implement EAP-AKA or EAP-AKA' anyway for non-3GPP accesses, support of EPS AKA would not provide any benefit for migration for operators that integrate non-3GPP accesses to NextGen CN.

The legacy interface between HSS and AAA server from EPC could probably be re-used or enhanced for NextGen.

Lenovo Ex. 1007
Page 185

5.2.4.9.4 Optimization considerations: termination of EAP method in the VPLMN

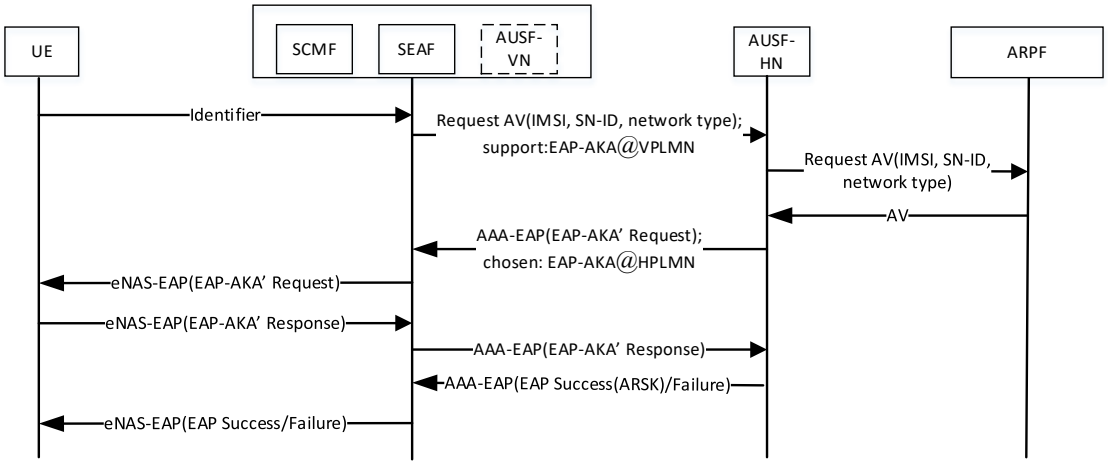
Variant 1:

One of the concerns related to the usage of EAP in the 3GPP network (also documented in TR 33.821 [24]) is related to the termination of authentication in the home network. This could be problem for efficiency by comparison to EPC AKA where authentication is done in the visited network. Essentially, the home network termination of authentication adds delay to the authentication process because some additional messages must be sent between the visited and home networks. On the other hand, this is also a way to make the overall system design more secure because the home network would not give out security related keying material out unless the authentication of the UE is successful.

In the EAP framework, the authenticator may act as a "pass-through authenticator" allowing the back-end authentication server to perform the actual authentication. However, it is also possible that the "pass-through authenticator" implements locally some of the EAP methods. The same entity may behave differently depending on the EAP method used. Currently, there is no standard mechanism for the EAP entities that would allow them to share the information about the locally implemented EAP methods or negotiate if the authenticator should act as a "pass-through authenticator" or as a "full authenticator".

One possibility would be to develop a 3GPP extension for the AAA protocol that would allow NG entities to share information about locally implemented EAP methods and negotiate where the authentication end-point is located. Figures 5.2.4.9.4-1 and 5.2.4.9.4-2 demonstate a potential realization of the extension. If the visted network had a local implementation of the EAP method (e.g. EAP-AKA), it could inform the home network about this. Based on this information, and a local policy, the home network would be able to decide, based on trust in VPLMN's supported security capabilities, wether it would choose the HPLMN terminated authentication (figure 5.2.4.9.4-1) or the VPLMN terminated authentication (figure 5.2.4.9.4-2). An indication (through the content in the response from the HPLMN) of the home network's choice would be made available to the VPLMN whereas the UE would not need to know where exactly the authentication is terminated.

NOTE: Placing the EAP server in the visited network has the disadvantage of the HPLMN not knowing the result of authentication.



Lenovo Ex. 1007
Page 186

Figure 5.2.4.9.4-1: HPLMN terminated EAP-AKA

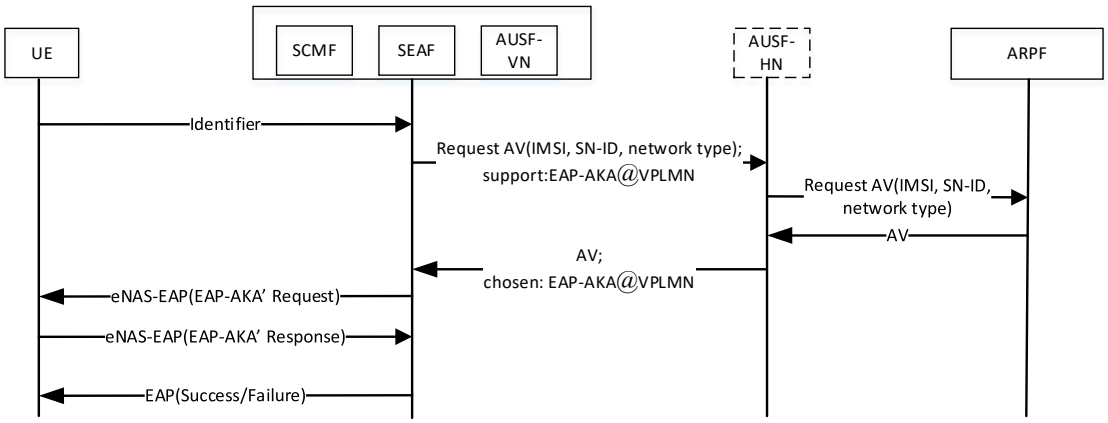


Figure 5.2.4.9.4-2: VPLMN terminated EAP-AKA

Variant 2:

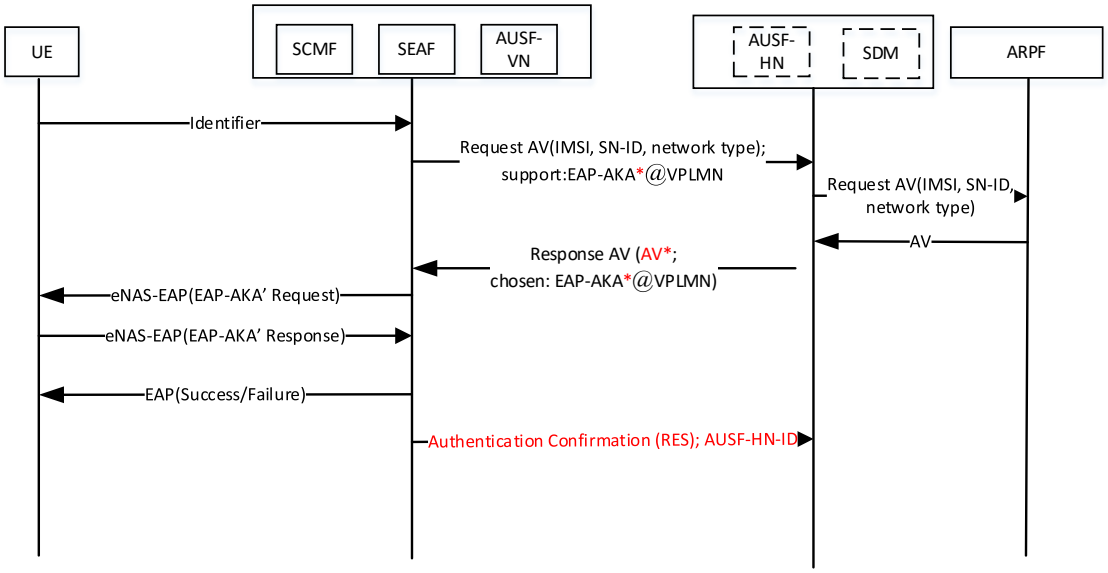


Figure 5.2.4.9.4-3: EAP AKA' with UE authentication confirmation

This new variant solution enhances EAP AKA' in a similar way as described for EPS AKA* in solution #2.22, with providing an Authentication Confirmation message from the visited network to the home network that confirms successful authentication of the UE such that the message cannot be spoofed by the visited network with a reasonable probability.

This new variant solution is called EAP-AKA*.

This new solution leaves the authentication exchange between the UE and the visited network unchanged, compared to using EAP AKA' in 5G, as e.g. described for VPLMN terminated EAP-AKA in variant 1 in this same clause above (solution #2.9. In particular, the solution does not affect the authentication behaviour of the UE, compared to EAP AKA'.

EAP AKA* works as follows:

Lenovo Ex. 1007
Page 187

The SEAF in the visited network requests a new authentication vector by sending a Request AV message to the AUSF-HN in the home network. The SEAF informs the AUSF-HN that it has a local EAP server (AUSF-VN) supporting EAP-AKA*.

NOTE: AUSF-VN is a function implemented in SEAF rather than a separate node.

The AUSF_HN translates the Request AV message into a request to the ARPF. The ARPF generates the authentication vector in the same way as for EAP AKA' in TS 33.402 and returns it to the AUSF-HN. Only one authentication vector shall be returned in response to a Request AV message.

NOTE2: Returning only one authentication vector at a time is already recommended in EPS.

The AUSF-HN splits the parameter XRES into two equal parts XRES1 and XRES2 (e.g. by choosing XRES1 to be the n least significant bits of XRES where 2n is the length of XRES). The assumption is made here that the knowledge of XRES1 does not help in guessing XRES2.

NOTE3: This assumption is believed to be fulfilled when the expected authentication response XRES is pseudo-randomly generated, e.g. as in MILENAGE or TUAK.

The AUSF-HN stores XRES temporarily until a protocol timer expires.

Editor's Note: The protocol timer is to be defined by CT4.

The AUSF-HN then returns an authentication vector AV* in a Response AV message to the SEAF in visited network. The only difference between AV* and an authentication vector AV, as described for EAP-AKA' in TS 33.402, is that AV* contains only XRES1 while AV contains the full XRES. The AUSF-HN also indicates that EAP-AKA* has been chosen, and it should be terminated in the visited network.

The SEAF in visited network understands from the "chosen:EAP-AKA*@VPLMN" parameter that it includes AV*, not AV.

The AUSF-VN sends RAND, AUTN to the UE. The UE returns RES, as described for EAP-AKA' in TS 33.402.The AUSF-VN splits RES into RES1 and RES2 in the same way as the AUSF-HN did and compares RES1 with XRES1. If they coincide the SEAF considers the authentication successful. If not the SEAF rejects the authentication.

If the authentication was successful, the AUSF-VN sends RES, as received from the UE, in a newly defined Next Gen Authentication Confirmation message (containing identifications of the subscriber and the visited network) to the AUSF-HN/SDM in home network. The RES can also be sent in the Update Location procedure, however, in this case the receiver is SDM, and the RES needs to be further forwarded to AUSF-HN.

When the RES was received from SDM and was received in time (cf. protocol timer above) the AUSF-HN compares the received RES with the stored XRES. If they coincide the AUSF-HN considers the authentication successful and records the event, together with the time, the identity of the visited network and the subscriber identity, in a database of successful authentications.

NOTE4: Solution #2.21 explains how EAP AKA* can be used to address key issue #2.11.

5.2.4.9.5 Evaluation

Security:

- There are no known attacks on EAP AKA(') that would prevent the use of these methods in NextGen.
- All EAP method specifications in IETF are expected to include a section describing the security claims of the method. These claims should be further studied if an EAP method is to be supported in NextGen.
- Channel binding: Channel binding could be related to the use of EAP over various channels, and about binding the EAP to the channel itself. Channel binding is typically implemented by adding some integrity protected channel property into the authentication, and comparing this property in the end-points to another value communicated out of band. Some EAP methods, such as EAP-TLS, does not include channel binding, and it would need to be specified in normative phase if desired. The topic of channel binding has been studied by SA3 before in the context of GBA.
- There exists some EAP methods that may not be suitable for NextGen (or that are only suitable in certain accesses, e.g. in fixed access). 3GPP should give recommendations on EAP methods are not recommended.

Lenovo Ex. 1007
Page 188

Authentication delay:

- EAP AKA requires one additional round-trip between VN and HN during authentication if compared e.g. to EPS AKA. However, EAP AKA also increases the control of HN for authentication, and consequently the HN can be sure that the UE is involved in authentication. Increased HN control is available also in other AKA variants, such as EPS AKA* or EAP-AKA*.

- ERP is able to reduce the delay by authorizing a trusted VN to perform subsequent re-authentication locally. For less-trusted VNs, the HN may still choose to run end-to-end authentication. However, the security anchor SEAF is most likely able to perform similar re-keying. A potential benefit of ERP is that the HN is able to set a limit to the lifetime of the master key, and that the HN is able to make policy decisions if certain networks are trusted for ERP and other not. Similar properties can also be added when delivering the security anchor key through any other authentication methods. The potential benefits of ERP are no different between 3GPP and non-3GPP accesses.

- Optimization where an EAP method is implemented in the VN, and the use of home terminated EAP, or VN terminated EAP is negotiated, is also possible. If chosen, this optimization should probably be limited to EAP AKA. This optimization may also be enhanced with a mechanism similar to EPS AKA* where the HN control is increased. Otherwise, the home control of authentication is lost. Furthermore, the home network may not be able to check the authorization of the SN in a freshly manner if the SN stores old AVs.

Possibility of enhancements and 3GPP control:

- EAP AKA and EAP AKA' are under control of IETF. If there was a need for new EAP AKA variant, the one should probably be specified in IETF. Companies present in SA3 are also very active in IETF, and have successfully standardized many IETF standards including e.g. EAP-AKA'. Therefore, it can be expected that it would go quick in IETF this time as well. Standardization would not require opening a new working group in IETF but could be done e.g. as an area director sponsored activity.

- Not all EAP methods need to be specified in IETF. It is possible to have 3GPP specific EAP methods that are documented only in 3GPP. However, it is generally recommended that enhancements to EAP AKA should be done in IETF because EAP AKA was originally developed there.

5.2.4.10 Solution #2.10: Equipment Identifier Authentication using the Device Certificate

5.2.4.10.1 Introduction

This solution addresses the Key issue #2.4: Equipment Identifier authentication(or EIAuth for short). In this solution, during the manufacturing of the device, it is securely provisioned with a device certificate and the private key associated with the certificate. The device certificate includes the equipment identifier (e.g., IMEI in EPS) within a field of the certificate.

The device certificate is signed by a Certificate Authority (CA). The CA can be a device manufacturer CA or a 3rd party CA that is trusted by the manufacturer. Irrespective of the CA used to sign the device certificate, the operator (or the entity that is performing authentication of the reported equipment identifier) makes the decision (e.g., as part of operator device certification process) on whether to trust the CA used to sign the device certificate.

5.2.4.10.2 Solution details

5.2.4.10.2.1 Introduction

In this solution, the equipment identifier authentication is proposed to be performed using NAS messages after the NG-UE's subscription is successfully authenticated and the security protection is established using keys derived from subscription authentication (similar to NAS Identity Request and Identity Response in EPS). The method proposed here is very similar to the variant 1 of the solution described in clause 5.4.4.2.2 (Enhanced AKA authentication) in TR 33.868 [26].

Providing equipment identifier authentication requires that the device has been provisioned with the device certificate. A secure part of the device stores the sensitive device keys such as the private key associated with the device certificate and performs all cryptographic operations that make use of these sensitive keys are performed within the secure part.

Lenovo Ex. 1007
Page 189

NOTE: Secure storage and processing requirements for device credentials and identifiers within the NG-UE is covered in key issue 5.y.

The high-level message flow for NG-UE attachment with equipment identifier authentication to the NextGen systems using the device certificate is given in the figure below.

Editor's Note: The split of functionality within the CP-CN for equipment identifier authentication is FFS.

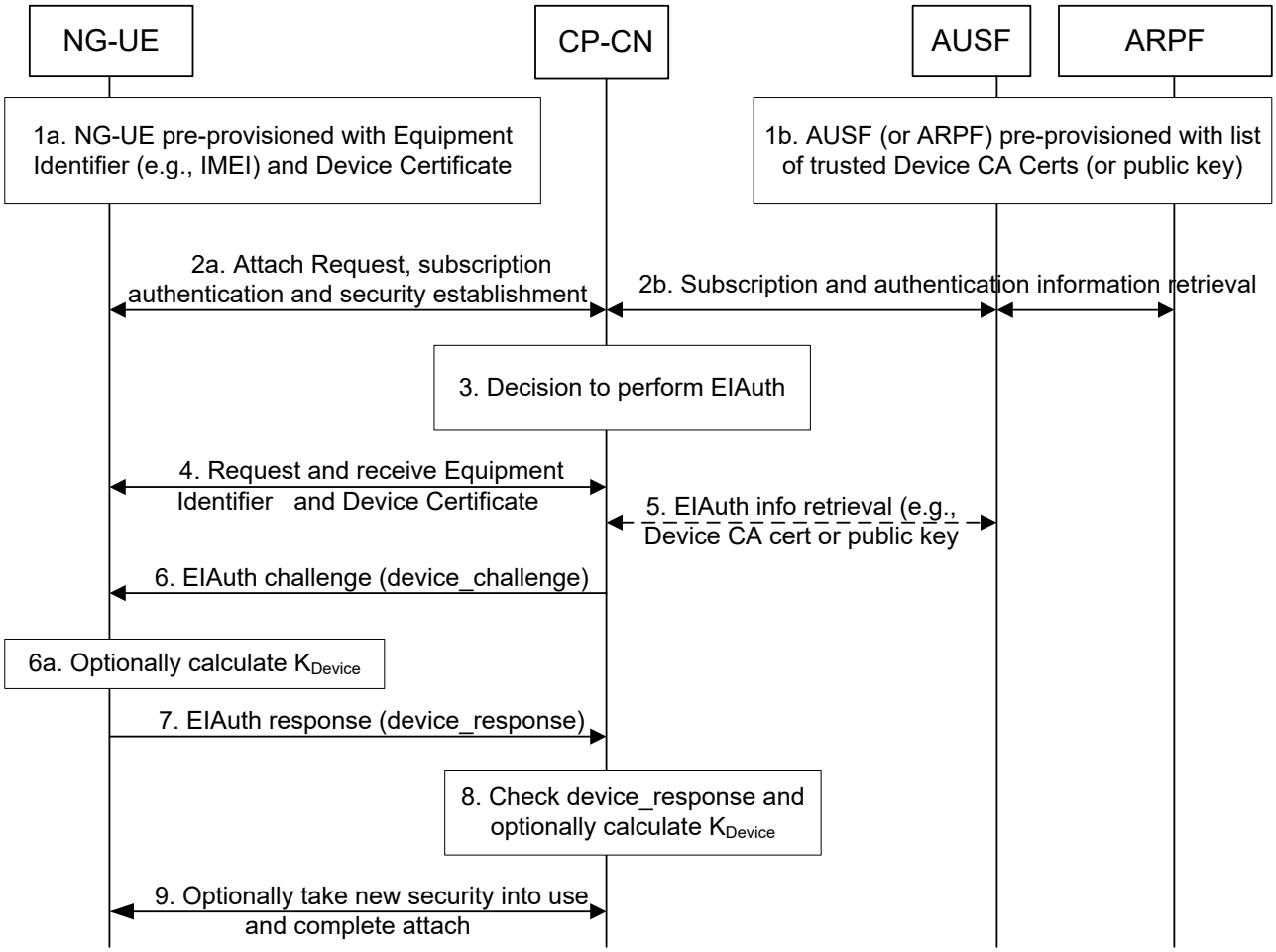


Figure 5.2.4.10.2-1: NG-UE attach with equipment identifier authentication

Editor's Note: It is FFS whether some of the steps in the message flow in the above figure can be optimized (e.g., by combining some of the steps).

1) NG-UE is pre-provisioned (e.g., during device manufacturing) with the device certificate. The certificate (or the public key) of the CA used to sign the device certificate is provisioned in the AUSF by operator. Alternatively, this information can be provisioned in the ARPF, in which case the AUSF has to retrieve the CA certificate from the ARPF. Note that the AUSF may be configured with the CA certificate(s) for the device(s) that are authorized by the operator.

Editor's Note: It is FFS exactly where the CA cert (or public key of the CA cert) used to sign the device certificate is stored within the Next-Gen system (e.g., AUSF or ARPF or another network entity).

2) The NG-UE sends attach request to the network. After successful subscription authentication (e.g., EPS AKA) by the network, secure communication is established between the UE and the network.

3) CP-CN decides to perform equipment identifier authentication. This decision may be made based on either the subscription information retrieved from the AUSF/ARPF or the local policy of the CP-CN.

Lenovo Ex. 1007
Page 190

4) CP-CN sends the request for equipment identifier and the certificate associated with the device and receives it using protected NAS messages (e.g., Identity Request / Identify Response). Use of protected NAS messages ensures that the equipment identifier privacy is maintained. The device certificate is only requested by the CP-CN if it wants to perform equipment identifier authentication and can be skipped if CP-CN wants to only retrieve the equipment identifier of the device or can obtain the device certificate by other means (e.g. from NG-UE subscription profile).

5) CP-CN retrieves from AUSF the information necessary for performing the equipment identifier authentication. This step can be skipped if the CP-CN has all the information necessary for performing the equipment identifier authentication.

6) CP-CN sends the equipment identifier authentication challenge. Optionally, if the network wants to refresh the security context by binding it with the equipment identifier authentication credentials, it may request the UE to generate a key (K_{Device}) during the equipment identifier authentication process.

7) UE generates the equipment identifier authentication response and sends it to CP-CN.

8) CP-CN verifies the device response and optionally calculates the K_{Device}.

9) If the network decides to bind the security context using keys derived from equipment identifier authentication (e.g. to provide a binding between IMSI and IMEI), the network initiates a security mode command and completes the attach procedures.

5.2.4.10.2.2 Service Provider issued device certificate enrollment

In order to avoid the continued dependence of the operator (or service provider) on the manufacturer issued device certificate, operators (or service provider) may want to issue (e.g., using a CA owned or trusted by the operator) their own device certificate using a certificate enrollment procedure and use the service provider issued certificate for equipment identifier authentication. This has the benefit that once the NG-UE is enrolled, the operator no longer needs to trust the CA used by the device manufacturer.

If an NG-UE has an MNO or service provider issued device certificate, it should be used instead of the manufacturer issued device certificate for the equipment identifier authentication. The service provider issued device certificate that is used for equipment identifier authentication shall include the equipment identifier in an attribute within the issued certificate (e.g., subjectAltName field includes the equipment identifier in FQDN format, such as <equipment-identifier>.serviceprovider.com). This will allow the network function performing the equipment identifier authentication to extract the equipment identifier from the service provider issued certificate (e.g., in EIR procedures in clause 5.2.4.10.2.3).

There are two well-known methods that can be used for certificate enrollment, namely, Simple Certificate Enrollment Protocol (SCEP) and Enrollment over Secure Transport (EST), specified in IETF RFC7030.

Although SCEP is widely used, it requires the use of shared secrets between the client and the CA for securing the certificate signing request (CSR). An IETF draft is available for SCEP (e.g., https://www.ietf.org/id/draft-gutmann-scep-03.txt), however, its path to becoming an RFC seems uncertain due to lack of support within IETF.

The EST uses TLS for the secure transport of messages and certificates between the CA/RA (Registration Authority) and the client. Furthermore, the manufacturer issued device certificate can be used to authenticate the NG-UE to establish a mutually authenticated TLS tunnel that can be used as a secure transport for certificate issuance. The EST also support cryptographic agility and automatic certificate re-enrollment.

NOTE: The authentication of the certificate enrollment procedure relies on the manufacturer issued device certificate.

Therefore, if a certificate enrollment method needs to be specified in 3GPP, then the use of EST seems preferable compared to SCEP.

Another option to consider for the certificate enrollment method is the use of CMPv2 (IETF RFC 4210) used for the enrollment of the base stations with operator issued certificates specified in clause 9 of TS 33.310. However, the use of EST compared to CMPv2 has the following benefits for device certificate enrollment:

- Privacy / confidentiality protection: Use of TLS as the transport for EST ensures that all certificate enrollment messages/procedures are confidentiality protected. CMPv2 uses message layer security to provide integrity

Lenovo Ex. 1007
Page 191

protection to all its fields but encryption is applied only to the Certificate field and not to the entire messages (cf. requirement 3 in section 3.1.2 of RFC 4210).

- Attributes types to include in the Certificate Signing Request (CSR): EST natively supports the ability for the EST client to request the CA/RA to provide the list of specific attributes that the EST client should include in the CSR. This capability may be beneficial in scenarios where the EST will be used to enrol multiple device certificates with set of different attributes (e.g., based on the application need).

It should be noted that workarounds can be found to provide these benefits for CMPv2. However, these require further specification work and might not be compatible with CMPv2 profile in TS 33.310. Therefore, the use of EST as the method for device certificate enrollment also seems preferable compared to CMPv2.

Editor's Note: It is ffs whether a certificate enrollment method needs to be specified in NextGen System (e.g., by profiling the use of EST).

5.2.4.10.2.3 Use of Equipment Identifier Authentication with EIR

The Equipment Identity Register (EIR) is used in the existing 3GPP systems to check whether the device identified by the equipment identifier (e.g., IMEI) is reported stolen. If it is, then the network may deny service to these devices. However, in the existing 3GPP systems, the reported equipment identifier is not authenticated. A malicious user may be able to report an equipment identifier that is not reported stolen, thereby bypassing the EIR check by the network.

The high-level call flow below shows how the equipment identifier authentication solution can be used with EIR to improve the security of the EIR procedures.

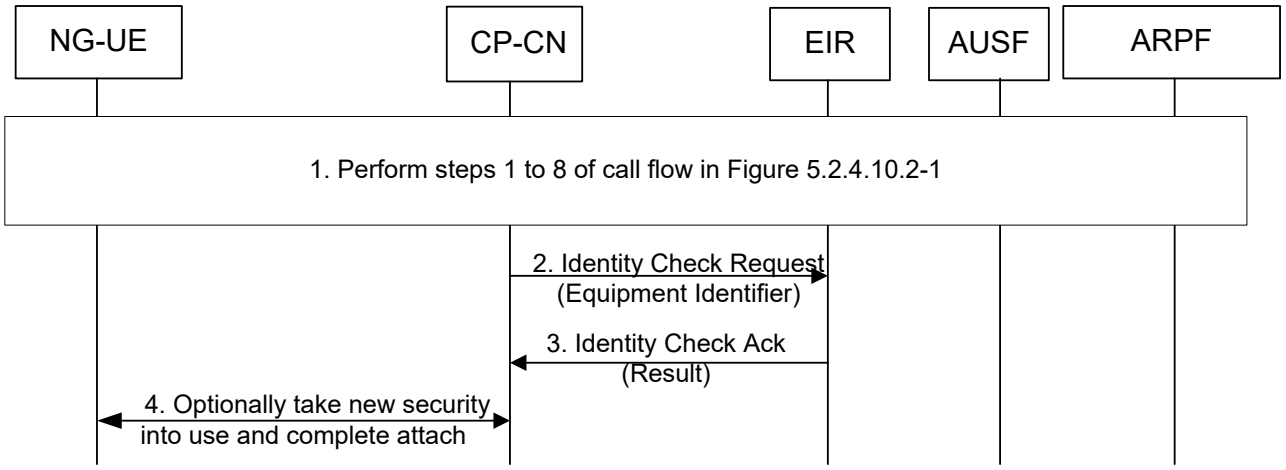


Figure 5.2.4.10.2-2: EIR check after equipment identifier authentication

1) NG-UE performs attach and equipment identifier authentication as shown in steps 1-8 of Figure 5.2.4.10.2-1.
2) CP-CN decides to perform EIR check and sends Identity Check Request message including the authenticated equipment identifier.
3) CP-CN receives result of the EIR authorization check. If the device is blacklisted, the CP-CN may abort the attach procedures by sending attach reject message. Otherwise, proceed to the next step.
4) CP-CN sends the attach complete message to the NG-UE with optionally taking into account the new security context that is bound with the equipment identifier authentication.

5.2.4.10.3 Evaluation

FFS

Lenovo Ex. 1007
Page 192

5.2.4.11 Solution #2.11: Blocking the UE which repeats authentication in a short period

5.2.4.11.1 Introduction

This solution addresses key issue 5.2.3.7 of reducing signalling overload. In particular, it addresses the issue where a large number of UEs controlled by the attacker to repeatedly initiate the authentication process in a short period of time.

5.2.4.11.2 Solution details

Legal UE which is controlled by an attacker and repeatedly initiates the authentication process in a short period will cause network resources to be maliciously exahusted. This proposal allows the network to monitor the authentication frequency of the UE. If the authentication frequency of one UE is higher than a certain threshold, then the network will consider the UE's behaviour as abnormal and block the UE's authentication process for a back-off time.

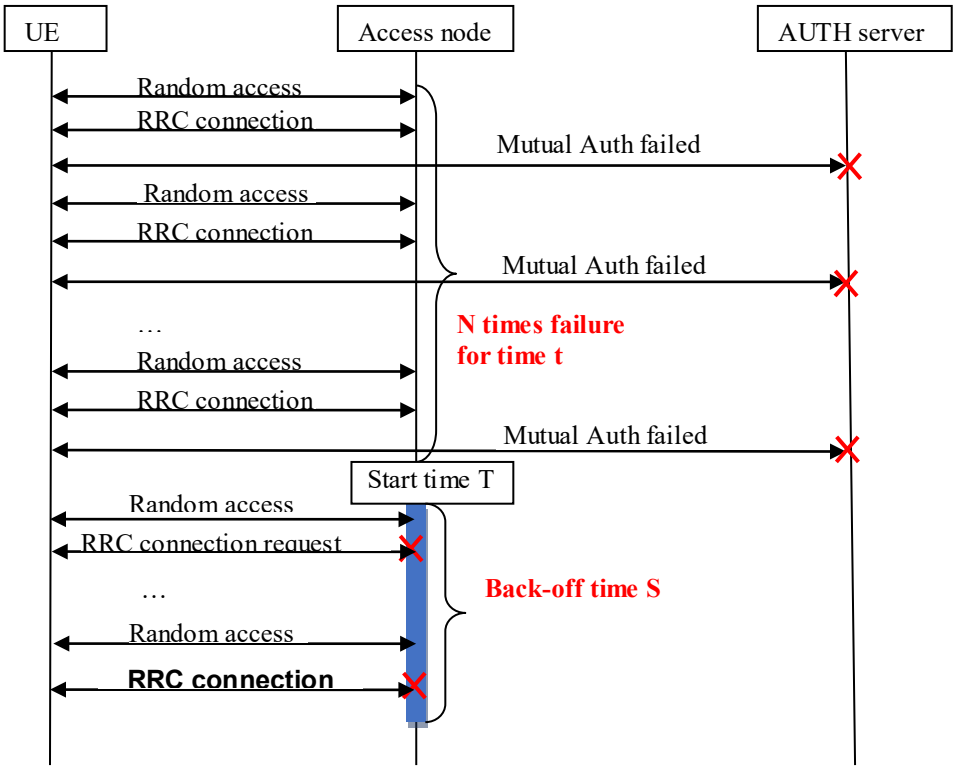


Figure 5.2.4.11.2-1 : Procedure for Blocking Illegal UE causing repeated authentication

For the illegal UE, each time the UE authentication fails, to save the radio network resouce for normal UE, it's suggessed that the access node monitor the authentication failure frequency of the UE. When the authentication failure frequency of one UE is higher than a certain threshold, then block the UE's RRC connnection request for a back-off time. Here, in order to identify a specical UE, RRC connnection request has to carry the UE identifier that can be used to identify the UE for a consistent period of time, e.g. Temp ID or a longer term identifier.

NOTE: If the UE authentication fails, the authentication server should send a message to notify the access node to release the UE context with the cause of authentication failure. E,g. in the LTE 3GPP-AKA authentication, the MME sends the UE context release command with the cause of authentication failure to the eNB.

Editor's Note: This solution does not address the case of malicious UE that keeps changing its ID.

Lenovo Ex. 1007
Page 193

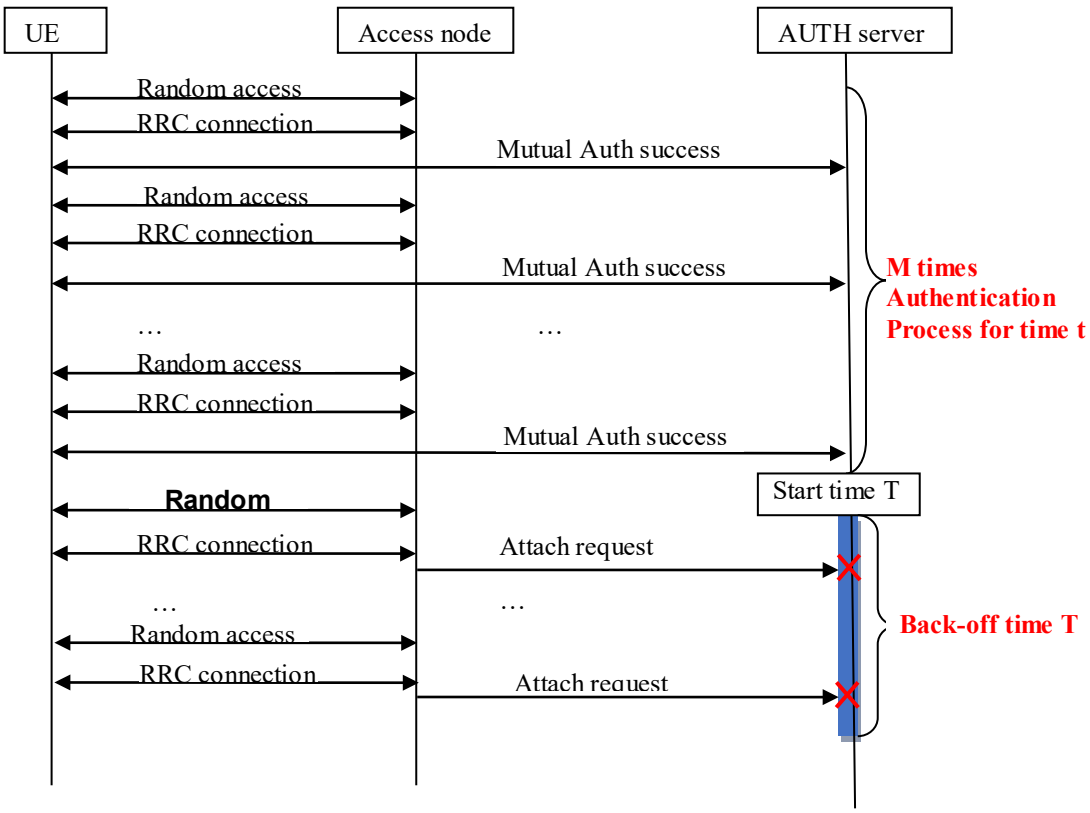


Figure 5.2.4.11.2-2 : Procedure for Blocking legal UE

For the above case of legal UE, only when the authentication frequency is higher than the normal frequency, then network decides the UE is abnormal and block it, so the threshold of the authentication frequency depends on the specific service model. E.g. the normal authentication frequency is A, then set the threshold to 2*A. For the case of illegal UE, if the frequency of authentication failure is higher than a certain vaule, e.g. 3 times per second, then think the UE is abnormal and block it immediately. Therefore, the threshold of the authentication frequency should be set to different value for the different two case. And the back-off time also can be set to different value. How to set the threshold of the authentication frequency and the back-off time, it depends on the operator's requirement and the vendor's implemention.

Editor's Note: This solution interworking with privacy solutions is ffs.

Editor's Note: This solution assumes that the UE is capable of triggering the authentication procedure. This solution needs to be revisited if a UE triggered authentication mechanism is considered for NextGen.

Editor's Note: What kind of ID available to access network for tracking the UE and how it is protected, e.g., Temp ID, RAN specific ID, or IMSI, is ffs.

NOTE: To identify a special UE in the access node, the RRC connection request message has to carry an identifier that can be used to identify the UE for a consistent period of time, e.g. Temp ID or a longer term identifier.

5.2.4.11.3 Evaluation

The procedure for handling Illegal UE repeated authentication may introduce a DoS attack on a specific UE using this UE specific temporary or permanent Identifier.

This solution is effective only against signalling measures due to massive attaches.

Note: This solution is a congestion control like measure that is to be specified by SA2.

Editor's Note: A complete evaluation is still needed.

Lenovo Ex. 1007
Page 194

5.2.4.12 Solution #2.12: Mutual Authentication and Security Agreement

5.2.4.12.1 Introduction

This solution addresses key issue #2.1, #4.1. #7.2, #7.3, and the following security areas in TR 33.899:

1. Security Area No. 2, Authentication. Provides a mutual authentication mechanism.
2. Security Area No. 3, It leverage the EPS-AKA mechanism for deriving security and keying materials for protecting all signaling and userplane traffic between the NG-UE and the network. It also derives keys for protecting the Initial authentication.
3. Seciurity Area No. 4, It provides a mechanism to allow the network to integrity protect any message at the level of NAS and AS even in the scenarios when the UE and the network goes out of synchronization or the network is not able to validate the authenticity of the NG-UE or any of its signaling messages.
4. Security Area No. 7: It protects the user/device privacy by protecting the subscriber and device identifiers at all times and in all scenarios.

5.2.4.12.2 Solution Details

5.2.4.12.2.1 NG Security Architecture

This solution assumes the following Next Generation security architecture principles:

- There is a Security Anchor Function (SEAF) that resides in the core of the serving network.
- The SEAF performs the role of the authenticator.
- The security architecture shall consider the case of CP and UP split and have mechanisms to provide the needed security materials to the UP node.

5.2.4.12.2.2 NG-MASA Main Security Aspects

Initial Authentication:

- Initial Authentication is executed when the NG-UE does not have any currently valid security association with the access network.
- Initial Authentication utilizes Asymmetric public key of the Home Network in addition to the subscriber symmetric key ‘K’ and other security material that is stored in the (e)UICC.
- Initial Authentication is completed in 4 messages which includes the security agreement exchange for Non-Access Stratum signaling, e.g., NAS.
- Initial Authentication utilizes the Home Network public key to encrypt the Initial Authentoication Request message and protect the subscriber identity, e.g., IMSI.
- Initial Authentication utilizes the subscriber symmetric key ‘K’ and other security credentials to secure and protect the Initial Authentication Response (IAS) sent from the SeAN to the NG-UE.
- Mutual security agreement is derived and agreed upon between the NG-UE and Network for all signaling and user plane traffic; NAS, RRC, user plane traffic, etc.
- The serving network public key is securely communicated to the NG-UE in the Initial Authentication Response. This SN public key is used by the NG-UE to validate network signature in odd and error case scenarios.
- Initial Authentication utilizes Asymmetric public key of the Home Network to the Initial Authentication Request while using the subscriber symmetric key ‘K’ and other security material that is stored in the (e)UICC to secure the Initial Authentication Response (IAS) from the SeAN to the NG-UE.

Lenovo Ex. 1007
Page 195

- During Initial Authentication, the AUSF/ARPF generates the normal AV(s) and delivered to the SEAF . SEAF follows current procedures to deliver respective AV to the NG-UE in the Initial Authentication Response. The AV is used to develop the security keying material for securing communications between the NG-UE and the serving network beyond the Initial Authentication procedure.

(Re)-Authentication:

- This is executed when NG-UE and access network has a current valid security association but the network request the NG-UE to re-authenticate.
- It follows the current LTE 3GPP EPS-AKA mechanism when using UE Temporary Identifier only.

NOTE: MASA provides full concealment to subscription permanent identifier, IMSI, even during Initial attach. Therefore, MASA solution meets the potential requirements of key issues 7.2, 7.5, and 7.6.

NOTE: MASA provides a mechanism for full concealment to equipment permanent identifier, IMEI, even during Initial attach. Therefore, MASA solution meets the potential requirements of key issues 7.3 except in the case of emergency call that does not have a valid subscription.5.2.4.12.2.3 NG-UE Functionality

5.2.4.12.2.3.1 Initial Authentication Request (IAR)

- Initial Authentication Request is sent from the NG-UE to the serving network SEAF in resonse to Identify Request message from the SEAF.
- Initial Authentication Request carries two main blocks of information which can be identified as follows:
  - **IAR Inner Block**
    - This block of the IAR includes security information related to NG-UE, e.g., UE security capabilities, IMSI, RAND1, RAND2, COUNTER.
    - NG-UE generates RAND1 and RAND2 to be used to protect the respective blocks of the IAR and IAS as described in the following sections.
    - NG-UE uses the RAND1 and the 'K' key to generate an Initial Authentication Request encryption and integrity protection keys, **K**IARenc + **K**IARint
    - NG-UE uses **K**IARenc to encrypt the IAR inner block. The encrypted block is referred to as the IAR inner block.
  - **IAR Outer Block**
    - NG-UE will add RAND1 and IMSI.
    - NG-UE uses **K**IARint to integrity protect both the Inner and outer IAR blocks and generate MAC.
- NG-UE encrypts the IAR message (including Inner and the Oter Blocks) using the Home Network public key.
- NG-UE includes the Home Network Identifier (HID) that is associated with the home network public key that was used to encrypt the IAR. This comprises the entire IAR,

5.2.4.12.2.3.2 Initial Authentication Response (IAS)

- Initial Authentication Response is sent from the serving network SEAF to the NG-UE in resonse to Initial Authentication Request.
- In addition to the existing security material the SEAF currently receives from AUSF/ARPF, SEAF also receives the security keys to integrity protect and encrypt the IAS, **K**IASenc + **K**IASint.
- SEAF includes the security parameters that SEAF agrees with to use with UE based on the UE security capabilities that was received from the AUSF/ARPF. SEAF encrypts the information in the inner block using **K**IASenc.

Lenovo Ex. 1007
Page 196

- In addition, the SEAF adds the serving network ID (SNID), the serving network public key (SNPK), and the RAND2 and then integrity protect the whole IAS message using **K**IASint and includes the MAC.
- NG-UE Check the RAND2 as the same number that was included in the inner block of the respective outstanding IAR.
- NG-UE uses RAND2 and the subscriber 'K' with other keying material to derive **K**IASenc + **K**IASint. These keys could be derived ahead of time at the time of IAR initiation.
- NG-UE calculates the MAC for the IAS and compare with the MAC included in the IAS. If validation passes, then the NG-UE decrypts the inner block of the IAS using KIASenc to recover the rest of the material.
- NG-UE can use AV material received AUTN and RAND to validate the newtwork authenticity.
- NG-UE validates the security parameter agreed upon and selected by the access network.
- NG-UE recovers the SNID and SNPK and save them to be used to validate error messages received from the serving network.
- When everything is successful, NG-UE sends Security and Authentication Complete message with the RES and IMSI included while being integrity protected and encrypted using NASenc and NASint keys based on the communicated AV material.

NOTE: If NAS encryption is not mandatory and is not enabled in the visiting network, requiring the UE to send IMSI in the Security & Authentication Complete message does not provide privacy protection.

NOTE: It is in the best interest of the serving network to securely deliver its public key to the NG-UE. This provides a protection against false basestation attack.

5.2.4.12.2.3.3 Changes to S6a User Authentication and Data Request

- SEAF includes in the Authentication and Data Request the entire received Initial Authentication Request as received from the NG-UE.

5.2.4.12.2.4 Changes to AUSF/ARPF Functionality

5.2.4.12.2.4.1 Handling of Authentication and Data Request

- When AUSF/ARPF receives the Authentication and Data Request from the SEAF, AUSF/ARPF retrieves the IAR message.
- AUSF/ARPF uses the HID to retrieve the home network private key (this could be done by the authentication center).
- AUSF/ARPF uses the Home Network private key to decrypt the IAR and recover the user IMSI, RAND1.
- AUSF/ARPF access the subscriber record associated with the recovered IMSI and retrieve the 'K' key and other subscriber information.
- AUSF/ARPF uses the RAND1 and 'K' to derive **K**IARenc + **K**IARint.
- AUSF/ARPF uses **K**IARint and the inner and outer block of the IAR to calculate the MAC and compare it to the MAC included to validate the integrity of the IAR. If validation passes, AUSF/ARPF validate the freshness of the message by checkeing the COUNTER received in the Inner Block of the received IAR as listed in next step.

Editor's Note: The current solution does not have the details of addressing the NG-UE going out of sequence with the home network.

- If integrity of IAR passes, AUSF/ARPF uses **K**IARenc to decrypt the IAR inner block. Then the AUSF/ARPF does the following verifications:
  - Check the freshness of the IAR by checking the received COUNTER.

Lenovo Ex. 1007
Page 197

- Recover the UE security capabilities to be included back to the SEAF in the respective Authentication and Data Response.
- Recover RAND2 to be used to derive **K**IASenc + **K**IASint keys which will be used to secure Initial Authentication Response.

5.2.4.12.2.4.2 Handling of Authentication and Data Response

- AUSF/ARPF includes the following information in the Auth & Data Response:
  - Received UE Security Capabilities
  - **K**IASenc + **K**IASint
  - Received RAND2.
  - The user subscription IMSI.

Editor's Note: Protocol goals and how they are achieved are ffs in the evaluation section.

NOTE: UE Security Capabilities could be sent in the IAR message on the clear outside the inner and outter blocks of the IAR message. In this case, the UE security capabilities needs to be protected against bidding down attack by mandating the SEAF to send the same UE Security Capabilities received in the IAR in the IAS message while is integrity protected.

5.2.4.12.2.4.3 Changes to SEAF Functionality

In comparison to the current LTE MME functionality and the possibility for SEAF being the NG security Anchor Node, the following are the changes required to handle Initial Authentication.

- Authenticity and validation of the NG-UE through the Initial Authentication procedure is communicated by the AUSF/ARPF to the SEAF.
- SEAF uses the received UE Security Capabilities to decide on security parameters with the UE. SEAF includes these security parameters in the IAS Inner Block.
- SEAF includes the serving network ID, SNID, and the serving network public key, SNPK, and security parameters that are needed outside the Inner block of the IAS.
- SEAF uses the received KIASint + KIASenc keys to integrity protect and encrypt the IAS.

NOTE: In order to prevent some potential DoS attacks on the Home Network, the Serving Network should enforce a reasonable rate limit of IAR message per UE. Even if a UE is still un-identified in the SN, the SN is supposed to give the UE some "radio ID" in order to route messages back to the UE. So there should be a rate limit, e.g., 1 IAR message per second per "radio ID". If the UE is malicious, the UE could also claim several times to be another one in order to receive different "radio IDs". Therefore, there should also be an overall IAR rate limit per base statione.

Lenovo Ex. 1007
Page 198

5.2.4.12.2.5 Initial Authentication Call Flow Details

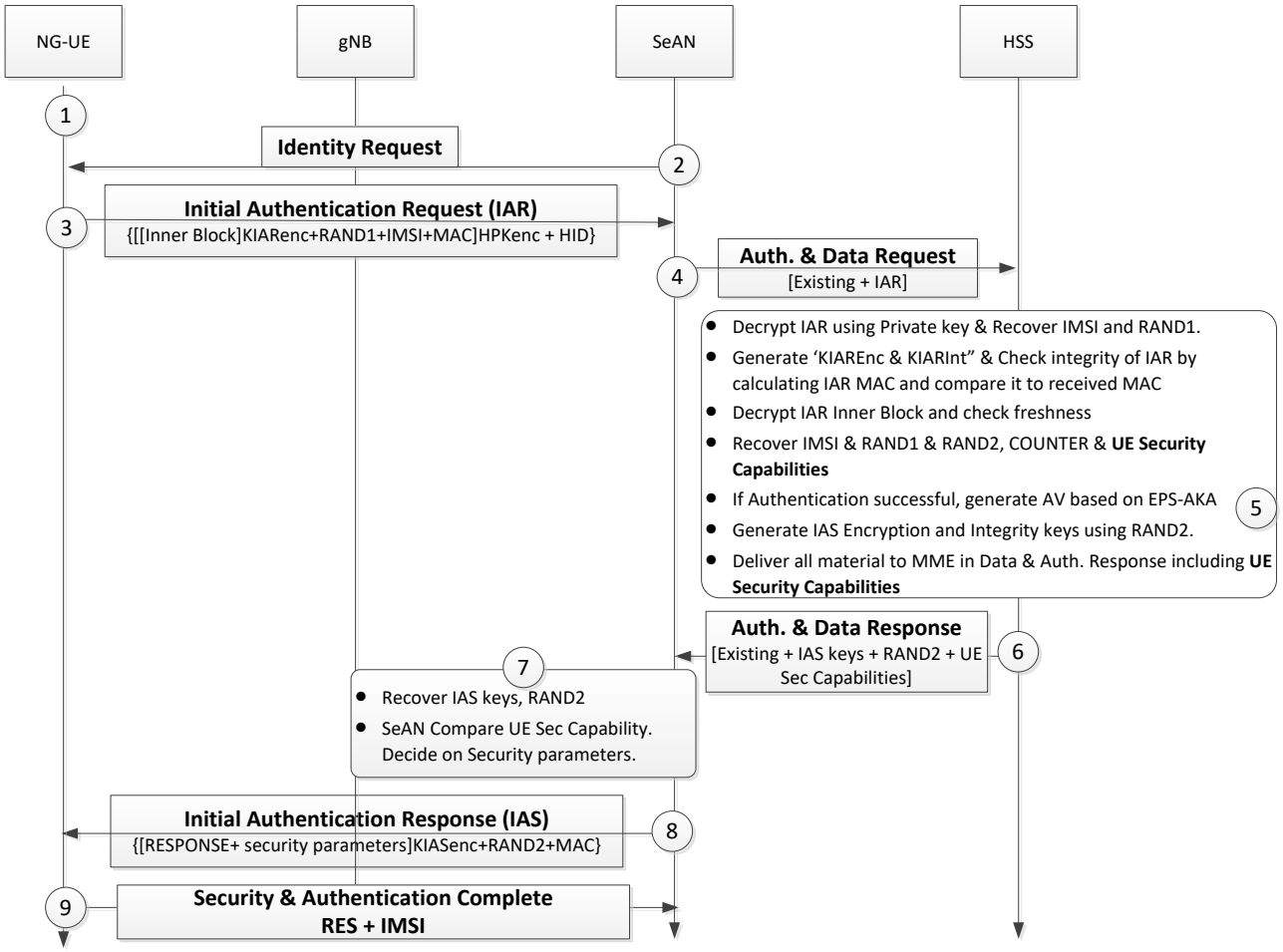


Figure 5.2.4.12.2.5-1: Call flow of NG-MASA Initial Authentication

The Key steps are as follows:

1. UE is configured with a (e)UICC with 'K' key and the Home Network ID and its associated public key.

   NOTE: Home network ID and Home network public key can reside either in the UICC or in the UE. It is an operator specific configuration option.

2. SEAF send Identity Request message to NG-UE. NG-UE considers this as an indication to initiate Initial Authentication.

3. NG-UE performs the following:

   a. Request the (e)UICC application to generate required security material for initial authentication, RAND1, RAND2, KIARenc, KIARInt, KIASenc, KIASint, and COUNTER.

   b. NG-UE builds IAR with Inner block being encrypted using KIARenc and Inner and Outer blocks are integrity protected by KIARInt.

   c. NG-UE encrypts the whole Inner & Outer blocks of the IAR including the MAC with the home network public key.

   d. NG-UE sends IAR to SEAF.

4. SEAF identifies the Home Network based on HID in the IAR and send Authentication and Data Request to the AUSF/ARPF. SEAF ensures including the IAR in the message.

Lenovo Ex. 1007
Page 199

NOTE: Having the HID on the clear may contribute to the possibility of tracking the UE or a group of UEs which belong to the same home network and using the same HID.

5. When AUSF/ARPF receives the Authentication and Data Request message, AUSF/ARPF perform the following steps:

    a. Decrypt IAR using Home Network Private key that is associated with the HID & Recover IMSI and RAND1.

    b. Access the Subscriber record based on IMSI and Generate 'KIAREnc & KIARInt" based on 'K' and RAND1.

    c. Generate the IAR message MAC based using KIARInt key and check the integrity of IAR and authenticate the UE.

    d. Decrypt IAR Inner block, recover UE Security Capabilities, RAND2, and COUNTER. Use COUNTER to check freshness of the message.

    e. If successful, AUSF/ARPF generates AV based on EPS-AKA

    f. Generate IAS Encryption and Integrity keys using RAND2 and 'K'.

    g. Deliver all material to SEAF in Data & Auth. Response including the UE Security Capabilities, RAND2, and KIASenc and KIASint.

6. AUSF/ARPF sends Authentication and Data Response to the MME with the following information:

    a. Subscriber Identifier, IMSI

    b. UE Security Capabilities.

    c. KIASenc, KIASInt, RAND2. and

    d. Authentication Vector(s)

7. SEAF recovers the Subscriber IMSI, UE security Capabilities, IAS keys, RAND2, and does the following:

    a. Examine the UE Security Capabilities and decides on the Security parameters.

8. SEAF builds IAS and send to the NG-UE.

    a. SEAF uses the KIASenc to encrypt the Inner Block

    b. SEAF adds the RAND2 In the outer block of IAS

    c. SEAF integrity protect the whole IAS using KIASint before sending the IAS to NG-UE

9. NG-UE perform the following steps:

    a. Validates the freshness of the IAS using RAND2.

    b. Validate the integrity of the IAS message using KIASInt.

    c. Decrypt the Inner block using KIASenc key and recover the AV, security parameters that the SEAF agrees on, KSI, etc.

    d. The UE uses the current LTE 3GPP-AKA procedure to authenticate the network using RAND and AUTN as received in the IAS

    e. NG-UE can generate NAS security keys.

    f. After all is successful, the NG-UE sends Security and Authentication complete message with the RES and IMSI included while being integrity protected and encrypted using the KNASInt and KNASenc.

5.2.4.12.3 MASA support 4G USIM

The following subsections describe how MASA supports the use of existing 4G USIM. This section describes the delta from the overall solution as described in Clause 5.2.4.12.2.

Lenovo Ex. 1007
Page 200

Editor's Note: A clarification of 4G USIM and whether Release 99 USIM can be used is FFS.

5.2.4.12.3.1 Initial Authentication Request (IAR)

When a 4G USIM is being used in the UE, and the UE supports 5G access and MASA, the UE will initiate this process only after receiving an Identity Request from the serving network. Since the UE has a 4G USIM, the UE construct the Initial Authentication Request message as follows:

- In this case the IAR message contain only one single block that is being encrypted by the home network public key.
- This single block carries the following information:
  - IMSI
  - RAND2
  - COUNTER
  - UE SECURITY CAPABILITIES
  - Etc.
- Outside the block that is encrypted using the home network public key, the UE includes the Home Network ID (HID) and a flag to indicate that this IAR message is generated for 4G USIM.

5.2.4.12.3.2 Initial Authentication Response (IAS)

- Initial Authentication Response is sent from the serving network SEAF to the NG-UE in resonse to Initial Authentication Request.
- In addition to the existing EPS_AKA security material the SEAF currently receives from HSS, SEAF also receives the security keys to integrity protect and encrypt the IAS, **K**IASenc + **K**IASint.
- SEAF includes the security parameters that SEAF agrees with to use with UE based on the UE security capabilities that was received from the AUSF/ARPF. SEAF encrypts the information in the inner block using **K**IASenc.
- In addition, the SEAF adds the serving network ID (optional SNID), the serving network public key (SNPK), the RAND & AUTN of the respective AV, and the RAND2 and then integrity protect the whole IAS message using **K**IASint and includes the MAC.
- NG-UE Check the RAND2 as the same number that was included in the respective outstanding IAR.
- NG-UE uses RAND and AUTN to access the USIM and generate RES, KASME & **K**IASenc + **K**IASint based on RAND2 and the subscriber 'K'.
- NG-UE calculates the MAC for the IAS and compare with the MAC included in the IAS. If validation passes, then the NG-UE decrypts the inner block of the IAS using KIASenc to recover the rest of the material.
- NG-UE can use AV material received AUTN and RAND to validate the newtwork authenticity.
- NG-UE validates the security parameter agreed upon and selected by the access network.
- NG-UE recovers the SNID (if included) and SNPK and save them to be used to validate error messages received from the serving network.
- When everything is successful, NG-UE sends Security and Authentication Complete message with the RES and IMSI included while integrity protected and encrypted using NASenc and NASint keys based on the communicated AV material.

Lenovo Ex. 1007
Page 201

5.2.4.12.3.3 AUSF/ARPF Functionality

5.2.4.12.3.3.1 Handling of Authentication and Data Request

- When AUSF/ARPF receives the Authentication and Data Request from the SEAF, AUSF/ARPF retrieves the IAR message. AUSF/ARPF validates that this IAR is for the support of 4G USIM.
- ASUF/ARPF uses the HID to retrieve the home network private key (this could be done by the authentication center).
- AUSF/ARPF uses the Home Network private key to decrypt the IAR and recover the user IMSI, RAND2, COUNTER
- AUSF/ARPF access the subscriber record associated with the recovered IMSI and retrieve the 'K' key and other subscriber information.
- AUSF/ARPF validates freshness of the IAR message using COUNTER.
- If IAR freshness validation passes, AUSF/ARPF Recovers RAND2 to be used to derive **K**IASenc + **K**IASint keys which will be used to secure Initial Authentication Response. AUSF/ARPF recovers UE security capabilities to be included in the respective Authentication and Data Response message.

5.2.4.12.3.3.2 Handling of Authentication and Data Response

- AUSF includes the following information in the Auth & Data Response:
  - Received UE Security Capabilities
  - **K**IASenc + **K**IASint
  - Received RAND2.
  - The user subscription IMSI

5.2.4.12.3.4 SEAF Functionality

In comparison to the current LTE MME functionality, the following are the functionalities required to handle Initial Authentication.

- SEAF uses the received UE Security Capabilities to decide on security parameters with the UE. SEAF includes these security parameters in the IAS Inner Block.
- SEAF includes the serving network ID (optionally), SNID, and the serving network public key, SNPK, and security parameters that are needed outside the Inner block of the IAS.
- SEAF includes the respective AV material outside the inner block, i.e., RAND and AUTN.
- SEAF uses the received KIASint + KIASenc keys to integrity protect and encrypt the IAS.
- SEAF authenticates the UE via the received RES in the Security and Authentication Complete message and recovers and saves the received IMSI in the NG-UE context.

Lenovo Ex. 1007
Page 202

5.2.4.12.3.5 4G USIM Initial Authentication Call Flow Details

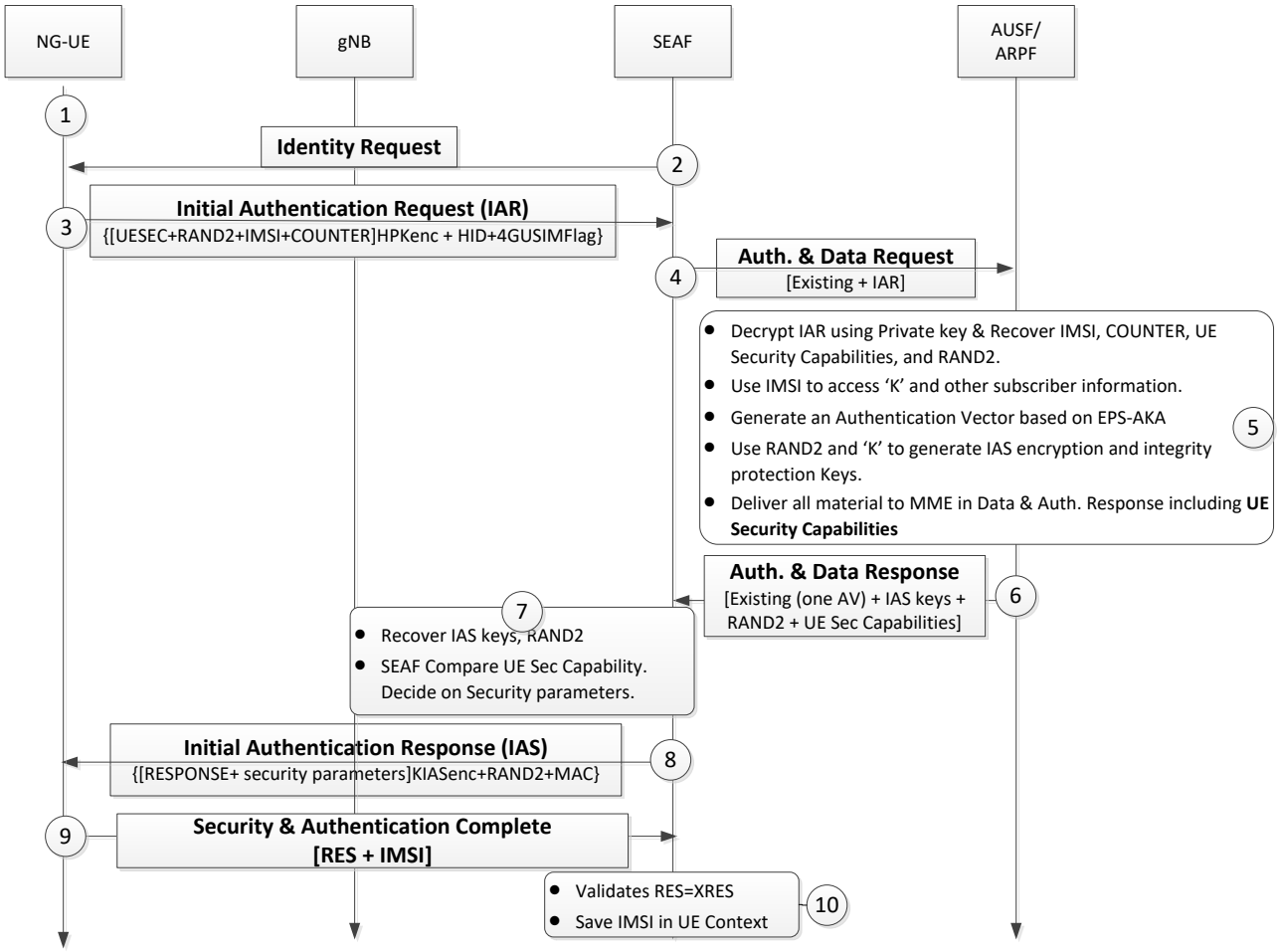


Figure 5.2.4.12.3.5-1: Call flow of MASA Initial Authentication using 4G USIM

The Key steps are as follows:

1. UE is configured with a 4G USIM with 'K' key and the Home Network ID and its associated public key.
2. SEAF send Identity Request message to NG-UE. NG-UE considers this as an indication to initiate Initial Authentication.
3. NG-UE performs the following:
    e. Request the (e)UICC application to generate required security material for initial authentication, RAND1, RAND2, KIARenc, KIARInt, KIASenc, KIASint, and COUNTER.
    f. NG-UE builds IAR as one block with UE SEC Capabilities, IMSI, RAND2, and COUNTER.
    g. NG-UE encrypts the entire single block of the IAR with the home network public key. NG-UE includes the HID and the 4GUSIMFlag in the outer part of IAR.
    h. NG-UE sends IAR to SEAF.
4. SEAF identifies the IAR for 4G USIM and the Home Network based on HID in the IAR and send Authentication and Data Request to the HSS. SEAF ensures including the IAR, HID, and 4GUSIM in the message.
5. When AUSF/ARPF receives the Authentication and Data Request message, AUSF/ARPF perform the following steps:
    h. Decrypt IAR using Home Network Private key that is associated with the HID & Recover IMSI, COUNTER, UE SEC Capabilities and RAND2.

Lenovo Ex. 1007
Page 203

i. Access the subscriber record based on IMSI and validate the freshness of the message based on COUNTER.

j. If successful, AUSF/ARPF generates AV based on EPS-AKA

k. Generate IAS Encryption and Integrity keys using RAND2 and 'K'.

l. Deliver all material to SEAF in Data & Auth. Response including the UE Security Capabilities, RAND2, and KIASenc and KIASint.

6. SEAF sends Authentication and Data Response to the SeAN with the following information:

   a. Subscriber Identifier, IMSI if needed.

   b. UE Security Capabilities.

   c. KIASenc, KIASInt, RAND2. and

   d. Authentication Vector.

7. SEAF recovers the Subscriber IMSI, UE security Capabilities, IAS keys, RAND2, and does the following:

   a. Examine the UE Security Capabilities and decides on the Security parameters.

8. SEAF builds IAS and send to the NG-UE.

   a. SEAF uses the KIASenc to encrypt the Inner Block

   b. SEAF adds the RAND2, AV material, In the outer block of IAS

   c. SEAF integrity protect the whole IAS using KIASint before sending the IAS to NG-UE

9. NG-UE perform the following steps:

   a. Validates the freshness of the IAS using RAND2.

   b. Recovers the RAND and AUTN and access the 4G USIM to generate RES, Kasme, and IAS keys.

   c. Validate the integrity of the IAS message using KIASInt.

   d. Decrypt the Inner block using KIASenc key and recover the AV, security parameters that the SEAF agrees on, KSI, etc.

   e. The UE uses the current LTE 3GPP-AKA procedure to authenticate the network using RAND and AUTN as received in the IAS

   f. NG-UE can generate NAS security keys.

   g. After all is successful, the NG-UE sends Security and Authentication complete message with RES included while integrity protected and encrypted being optional and as needed using the KNASInt and KNASenc.

10. SEAF compares RES to XRES and if passed, it saves received IMSI in the NG-UE context. SEAF compares the received IMSI to the IMSI received from the AUSF/ARPF in step 6

5.2.4.12.4 MASA NG-UE Security Capabilities Negotiation

The following subsections describe how NG-UE security capabilities are being negotiated for NAS, gNB-CP (RRC), and UP-GW (UP) protection and supported as per MASA Initial Authentication procedure. The following clauses avoid details that are being described in the main section of MASA solution details.

5.2.4.12.4.1 NG-UE Functionality

- NG-UE builds IAR message according to MASA.
- UE includes inside the encrypted inner block of the IAR message its UE security Capabilities for NAS, gNB-CP, UP-GW and other parameters. UE sends IAR to SeAN.

Lenovo Ex. 1007
Page 204

- When the NG-UE receives the IAS message and after it authenticates the integrity of the message and authenticates the serving network, the NG-UE recovers the security parameters related to the agreed upon security capabilities as received in the inner block of the IAS message. These security capabilities cover NAS, gNB-CP, and UP-GW security capabilities.
- NG-UE generates the respective NAS, gNB-CP, and UP-GW security keys and sends the Authentication and Security Complete message to the SEAF.

5.2.4.12.4.2 gNB-CP Functionality

1. Option 1: A flag is used in RRC or similar protocol to indicate to gNB-CP that this is IAR message.
2. Option 2: SEAF uses the infrastructure DNS server or other means to recover the gNB-CP security capabilities.
3. In the case of option 1 which is described in the call flow in figure 5.2.4.12.3.5.1, gNB-CP adds its gNB-CP security capabilities to the message sent to the SEAF. This is outside the NAS message but within the transport protocol between the gNB-CP and SEAF, e.g., in LTE it is S1AP.
4. In both options 1 & 2, gNB-CP recovers the gNB-CP agreed upon security paramneters with the UE from the message that carries the IAS message to the NG-UE. SEAF includes these parameters outside the NAS message and inside the transport protocol between the SEAF and gNB-CP.

5.2.4.12.4.3 SEAF Functionality

A. SEAF acquires gNB-CP security capabilities

The following are different options for SEAF acquiring gNB-CP security capabilities:

1. gNB-CP includes its security capabilities inside the transport protocol (e.g., S1AP) in the message that carries the Initial Authentication Request.
2. Whenever the gNB-CP comes up to service, the gNB-CP communicates its security capabilities to the available SEAF(s) and SEAF saves the gNB security capabilities against the gNB-CP ID.
3. SEAF uses the infrastructure DNS server to acquire the gNB-CP security capabilities.

B. SEAF acquires UP-GW security capabilities

The following are different options for SEAF acquiring UP-GW security capabilities:

1. SEAF acquires the UP-GW security capabilities either during provisioning or,
2. SEAF acquires UP-GW security capabilities using the infrastructure DNS server based on the UP-GW ID.

   NOTE: In many LTE implementations, the MME acquires the IP address of the S/P-GW via the infrastructure DNS server. In NG, similarly, it is possible when SEAF acquires the UP-GW IP address to also acquires its security capabilities.

C. SEAF Communicates all protocols security capabilities

1. After the SEAF receives the successful Authentication & Data Response from the AUSF/ARPF, it decides on the security capabilities for the NG-UE for the following protocols, NAS, gNB-CP, UP-GW based on the available NG-UE security capabilities, gNB-CP security capabilities, UP-GW security capabilities.
2. SEAF follows operator policy when deciding the security parameters for all respective protocols.
3. SEAF communicates the all protocols agreed upon security parameters to the NG-UE inside the IAS message.
4. SEAF communicates the gNB-CP protocol agreed upon security parameters to the gNB-CP node inside the S1AP message that carries the IAS message.
5. SEAF communicates the UP-GW protocol agreed upon security parameters to the UP-GW during the bearer establishment for the respective NG-UE.

Lenovo Ex. 1007
Page 205

NOTE: This solution provides one option for how NG-UE may negotiate its NAS, RRC, and UP security capabilities with the serving network. Other options can be used, e.g., using AS security mode command messages exchange. In case of shared RAN, the use of AS security mode command is required in case the shared RAN operator does not to share its RAN secyurity capabilities with SEAF.

5.2.4.12.4.4 AUSF/ARPF Functionality

No changes from the standard MASA functionality.

5.2.4.12.4.5 UP-GW Functionality

The SeAN communicates the security capabilities for UP agreed upon with the UE to the UP-GW during the NG-UE bearer setup.

5.2.4.12.4.5.1 Initial Authentication Call Flow with NG-UE Security Capabilities Negotiation

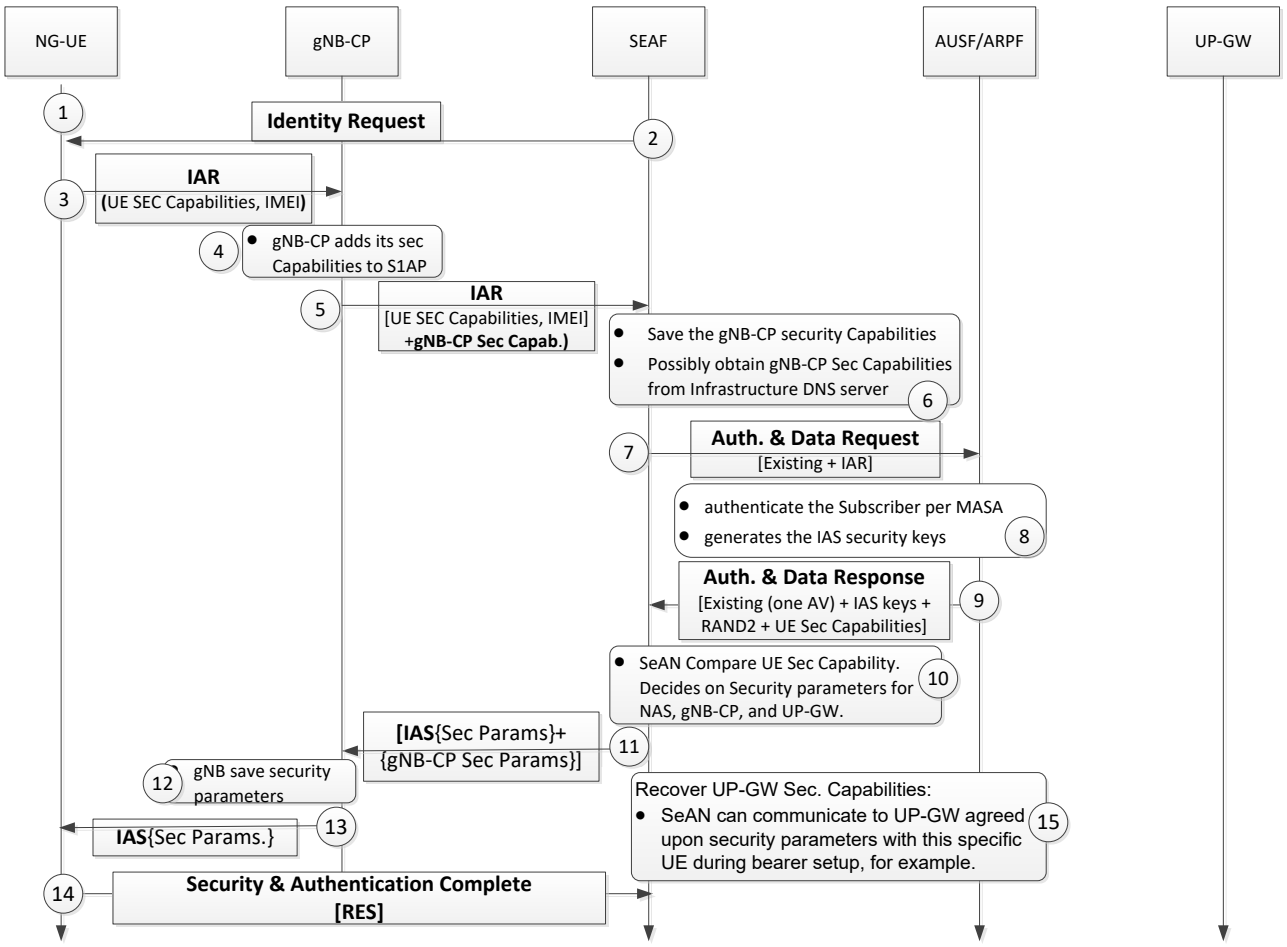


Figure 5.2.4.12.3.5-1: MASA Initial Authentication with NG-UE Security Capabilities Negotiation

The Key steps are as follows:

1. UE is configured with 5G (e)UICC with 'K' key, the Home Network ID, and its associated public key.

2. SEAF send Identity Request message to NG-UE. NG-UE considers this as an indication to initiate Initial Authentication.

3. NG-UE performs the following:

   i. Request the (e)UICC application to generate required security material for initial authentication, RAND1, RAND2, KIARenc, KIARInt, KIASenc, KIASint, and COUNTER.

Lenovo Ex. 1007
Page 206

j. NG-UE builds IAR as per MASA. In this step NG-UE includes NG-UE Security Capabilities inside the inner block of the IAR message. It also may include its IMEI.

k. NG-UE encrypts the whole Inner & Outer blocks of the IAR including the MAC with the home network public key.

l. NG-UE sends IAR to SEAF.

4. Optionally, gNB-CP node adds its Security Capabilities to the transposrt message between the gNB-CP and the SEAF (e.g., inside S1AP message as per 4G).

5. gNB-CP sends the respective S1AP message that carries the NG-UE IAR message to the SEAF.

6. SEAF acquirs the gNB-CP security capabilities as per the listed options in clause 5.2.4.12.4.3and save them as part of the temporary context for the NG-UE.

7. SEAF follows MASA and forward the Authentication and Data Request message to the AUSF/ARPF.

8. When AUSF/ARPF receives the Authentication and Data Request message, authenticate the NG-UE as per MASA and generates the IAS respective keys. AUSF/ARPF may recover the NG-UE IMSI and validate the NG-UE security capabilities.

9. AUSF/ARPF sends Authentication and Data Response to the SEAF as per MASA with NG-UE Security Capabilities included.

10. SEAF recovers the Subscriber IMSI, UE security Capabilities, IAS keys, RAND2, and does the following:

    a. Examine the UE Security Capabilities and decides on the Security parameters.

    b. SEAF may acquire the UP-GW security capabilities at this point after receiving the UP-GW identity from AUSF/ARPF or allocate it dynamically through provisioning and load balancing.

11. SEAF builds IAS and send to the NG-UE following MASA. In addition, SEAF include the gNB-CP protocol agreed upon security parameters in the S1AP message being sent to the gNB-CP node.

12. gNB-CP recovers gNB-CP protocol agreed upon security parameters and save it as part of the NG-UE current context.

13. gNB-CP forwards the IAS message to the NG-UE.

14. NG-UE validates the authenticity of the IAS and authenticates the network as per MASA. In addition, the UE saves all protocols agreed upon security parameters as part of its context. NG-UE sends the Security and Authentication Complete message to the SEAF.

15. SEAF communicates the agreed upon UP-GW security parameters to the UP-GW during the NG-UE bearer setup.

5.2.4.12.5 Solution Evaluation

5.2.4.12.5.1 Evaluation#1 Summary

- **Security:**

This solution proposes a mutual authentication and a security agreement mechanism that addresses all the known security vulnerabilities that has been documented against LTE 3GPP EPS-AKA. It addresses the following issues:

1. It protects the subscriber and device long term identifier (e.g., IMSI) at all times and prevents IMSI leakage.

2. It provides a dynamic mechanism to deliver the serving network public key material to the NG-UE in a secure manner which allows the network to always deliver NAS and AS messages with at least integrity protection. This mechanism protects against reported MITM attack on using attach response with error code.

- **Possibility of a common transport for a variety of authentication methods:**

This solution introduces a mechanism for Initial Authentication which is being introduced using 3GPP NAS signaling. However, the same initial authentication mechanism can be used over EAP.

Lenovo Ex. 1007
Page 207

- **Efficiency:**

  This solution provides an at least two messages saving over 3GPP EPS-AKA which counts for about 33% signaling saving. This mechanism utilizes the secure exchange of IAR and IAS to exchange the UE security capabilities within the Initial authentication messages.

- **Interworking**:

  This solution is based on 3GPP EPS-AKA and after Initial Authentication, the UE and the network can use EPS-AKA mechanism for handover and idle mode mobility. This mechanism can be adopted over EAP and thus can be seamlessly used to support interworking with non-3GPP accesses.

- **Migration**

  This solution utilizes all the strength from 3GPP EPS-AKA and symmetric keys as used in (e)UICC. It is 100% backward compatible with 3GPP EPS-AKA.

- **3GPP control over possible enhancements of authentication method used over 3GPP-defined access network**

  This solution is completely under the scope of 3GPP. However, if it is used over EAP for interworking with non-3GPP accesses, then the control of EAP lies within IETF.

5.2.4.12.5.2 Detailed Evaluation#1

5.2.4.12.5.2.1 MASA Goals and Evaluation

5.2.4.12.5.2.1.1. HN Authenticate Subscriber First & Subscriber Privacy

This goal allows the home network to achieve the following:

- Allow Home Network to have complete control over its subscribers by authenticating the subscriber first.
- Provide complete Subscriber privacy by allowing HN to reveal Subscriber private information and/or security parameters only after successful authentication and as needed by regulatory and HN policy.

5.2.4.12.5.2.1.1.1. HN Authenticate Subscriber First:

In 3GPP EPS-AKA, the home network relies on the serving network to authenticate the subscriber by comparing the user "RES" to the "XRES" as it is provided by the home network via the AV. In reality, the home network never authenticates the susbcriber as it implicitly realizes the subscriber has been successfully authenticated after the home network, i.e., HSS, receives the second Authentication and Data Information Request message from the serving network, i.e., MME to request the authorization of the user services.

In addition, the 3GPP EPS-AKA, allows the serving network during initial authentication to have access to all private and security information of the subscriber before even the home network has the chance to authenticate or validate the subscriber information, for example, the subscriber permanent identifier (IMSI).

Thus one of the main goals of MASA solution is to allow the home network operator to authenticate the subscriber first and after the subscriber has been successfully authenticated, the home network has full control to which subscriber information that is necessary to be revealed to the serving network.

Finally, MASA provides the means to meet potential requirements for key issue 2.11 by providing the home operator the full control to authenticate the subscriber before providing the visited network with any information about the NG-UE including the AV(s). This means MASA solution guarantees the home network of the presence of the NG-UE and when it moves to a new NG visited network.

5.2.4.12.5.2.1.1.2. Subscriber Privacy

tba.

5.2.4.12.5.2.1.1.3. General

MASA solution provides the flexability to have the Home Network ID (HID) included in the IAR message outside the encrypted block. HID identifies the home network public/private key pair used for encrypted the

Lenovo Ex. 1007
Page 208

IAR message included. This mechanism provides a great flexability to the home network operator to not be restricted to a single or few public/private key pairs.

5.2.4.12.5.2.1.2. Provide High Effeciency

MASA solution is highly efficient and provides the following optimization in comparision to 3GPP EPS-AKA in addition to NAS security mode command exchange.

a. It achieves mutual authentication and security key exchange in an efficient way with a single round trip.

b. It allows the flexability of having the authentication and service authorization to be completed during the Initial authentication round trip.

MASA provides mutual authentication as described in details in goal 2.3 below in as ingle round trip. It provides a saving of at least 33% of signaling in terms of the number of messages exchanged in comparison to 3GPP EPS-AKA by eliminating the need for NAS Security Command messages exchanges. In addition, it can eliminate the need for AS security command exchange and by doing this it can eliminate as much as 50% of the signaling in comparison with 3GPP EPS-AKA in addition to NAS security mode command exchange.

On the other hand, since 3GPP EPS-AKA does not provide the option for the home network to authenticate the subscriber but rather relies on the serving network authenticating the subscriber, the current 3GPP EPS-AKA provide authentication and ONLY after authentication is completed, the serving network will request service authorization in another round trip signaling between the serving network, e.g., MME, and the home network, e.g., HSS.

Since MASA allows the home network to authenictae the subscriber first, the home network has the opportunity to provide the authorization of applicable subscriber services in the same reponse (Authentication & Data Information response) which carries the indication of the authentication success to the serving network, e.g., MME. This saves at least 50% of the signaling between the serving network and the home network.

5.2.4.12.5.2.1.3 Mutual Authentication: Provide a mutual authentication mechanism between the subscriber and the home network

5.2.4.12.5.2.1.3.1. Home Network Authenticate NG-UE

In 3GPP EPS-AKA, the home network relies on its trust relationship with the serving network to validate the authenticity of the UE. In EPS-AKA there is no clear indication from the serving network to the home network that the UE has been successfully authenticated, however, the home network may implicitly realize this after receiving another request from the serving network to authorize the user services.

In MASA, the home network is the network which is trusted to authenticate the UE. As a matter of fact, the home network is able to validate and authenticate the NG-UE before sending any security credential to the serving network. In other words, if the NG-UE failed authentication, the home network will only send a failure cause to inform the serving network to release resources for this specific NG-UE.

The home network authenticates the NG-UE based on the authentication of the IAR message that is received through the serving network in the Authentication and Data Request message, as follows:

1. Home network recovers the HID which is associated with the home network public and private key pairs.
2. Home network decrypts the IAR using the home network private key.
3. Home network recovers the IMSI from the IAR message, along with COUNTER, MAC, and RAND1.
4. Based on IMSI, home network uses the subscriber ‘K’ and derive the IAR keys (IARKint + IARKenc) based on ‘K’, RAND1, and other derivation material.
5. Home network validates the authenticity and integrity of the IAR message by calculating the Network-MAC.

Lenovo Ex. 1007
Page 209

6. Home network checks Network-MAC against received MAC and verify the authenticity of the message and authenticate the UE.

5.2.4.12.5.2.1.2.3.2. Serving Network Authenticate NG-UE

The serving network authentication of the NG-UE can be achieved in two ways :

1. Serving Network can rely on the home network to communicate to it whether the UE is authentic or not based on the IAR validation.

2. Serving Network can use the "RES" received in the Authentication and Security Complete message received from the NG-UE at the end of the Initial Authenoictaion procedure to compare with the "XRES". The serving network follows the same process as per EPS-AKA.

   Editor's Note: Whether allowing the serving network to receive two indications of NG-UE successful authentication is needed is FFS.

5.2.4.12.5.2.1.2.3.3. NG-UE Authenticate the Network

When the NG-UE receives Initial Authentication Response (IAS) from the serving network, the NG-UE authenticates the network in two ways as follows:

5.2.4.12.5.2.1.2.3.3.1. NG-UE Authentiucate Network based on IAS Integrity

1. NG- UE validates the received RAND2 to be the same RAND2 that NG-UE sent in the IAR message encrypted in the inner block of the IAR message. This validates the IAS is not being replayed.

2. NG-UE uses the IASKint key to calculate the UE-MAC over the IAS message. NG-UE compares the UE-MAC to the MAC included in the IAS to validate the authenticaity and integrity of the IAS message that was recievd from the serving network.

3. When IAS message integrity validation is successful, the UE is assured that the serving network it is attached to is trusted by its home network and authentic to the extent that the home network provided the IAS keys to the serving network to protect the NG-UE IAS message.

5.2.4.12.5.2.1.2.3.3.2. NG-UE Authentiucate Network using EPS-AKA AV

1. After NG- UE validates the authenticity and integrity of the IAS message, NG-UE recovers the AV material received in the IAS message, AUTN and RAND.

2. NG-UE reaches its (e)UICC application to authenticate the network based on RAND and AUTN and following the EPS-AKA.

Editor's Note: Whether allowing the NG-UE to authenticate the network in two different ways is needed is FFS.

5.2.4.12.5.2.1.2.4 Addressing Vulnerabilities: Address existing 3GPP EPS security

The following two vulnerabilities and security attacks have have been documented in the literature:

1. User Privacy and tracking via what is called IMSI Catchers.

2. Although, fake basestation attacks which could cause a UE denial of service by sending Unauthenticated REJECT MESSAGES, e.g., ATTACH REJECT and TAU REJECT is a generic problem not specific to EPS-AKA, MASA solution provides a dynamic mechanism to communicate the serving network public key to NG-UE is asecure manner.

In order to address the privacy issue of 3GPP EPS-AKA, MASA solution never allows the user permanent identifier, e.g., IMSI, to be sent on the clear. When the UE receives the Identity Request message from the serving network, e.g., MME, the UE always respond by sending the IAR message which is encrypted using the home network public key.

In order to prevent the attack that is caused by a ROGUE basestation using unauthenticated REJECT MESSAGES, MASA solution provide a dynamic mechanism which allows the serving network to securely communicate its ID and its respective public key that can be used for protecting all REJECT MESSAAGES by signing the message with the serving network private key at any later time.

Lenovo Ex. 1007
Page 210

When the serving network receives an indication from the home network that the user has been successfully authenticated, the serving network includes in addition to other parameter the following two parameters:

1. Serving Network ID (SNID) – This ID can reflect the serving network public ID and could be used to identify the public/provate keys pair that is included in the IAS message.

2. Serving Network public key which is also can be linked to the serving Network ID in the above item.

This process does not only allow the serving network the flexiability to protect itself against any ROGUE basestation attack but also it provides the flexability to the serving network to use public/private keys pairs with a very flexible granularity with the following as examples:

a. Serving Network ID could reflect a single public/private keys for the whole serving network.

b. Serving Network ID could reflect a single public/private keys that maps to a single Cloud (Centralized) RAN which serve certain number of basestations.

c. Serving Network ID could reflect a single public/private keys that maps to a specific Tracking Area or a group of tracking areas.

5.2.4.12.5.2.1.2.5. Utilize (e)UICC Technology: Utilize the strength of 3GPP symmetric keying technology that relies on (e)UICC

MASA solution utilizes the strength of the (e)UICC symmetric keying technology which has proven strong reliability for many years. The only attack that has been documented on this technology was carried by an agency that belongs to a super power. If that is the case, this attack is not a realistic attack to be carried by a common attacker.

It is also well understood that an attacker like the one carried the attack against the UICC "K" keys for many subscribers also has the potential of breaking other security procedures that uses other technologies.

5.2.4.12.5.2.1.2.6. Limited Asyemmetric Keying Usage: Utilize the strength of Asymmetric keying technology without the need for 3GPP operator to deploy a full PKI

The overhead of utilizing a full fledged asymmetric keying technology that requires a full deployment of PKI is quite expensive and has it great scalability challenges that is related to certificate management, certificate revocations, Certificate Authentities, etc, even though, many operators have already deployed such a PKI and are using it on network nodes such as eNBs. However, it is quite well accepted to use public and private keys within the network as long as it is not extended to the end user certificate. In other words, having a solution that utilizes the strength of the asymmetric keying technologies for the network elements only is something that well contained and acceptable to every 3GPP and network operator.

That is well within the goals of the MASA solution. It utilizes the strength of asymmetric keying technology by using the public-private keys for the network elements to protect communications between the UE and the Home network and communications between the serving network and the UE in the case of REJECT MESSAGES.

MASA solution capitalizes on the strength of Asymmetric keying without the need to neither deploy a full fledged PKI solution nor the need to manage end user certificates.

NOTE: Managing infrastructure public/private keys without deploying a fully-fledged PKI is a generic problem that needs to be evaluated for all proposed solutions in this TR that require public/private keys.

5.2.4.12.5.2.1.2.7 Dynamic Security Parameters Update & Policy Provisioning

First and for most, one of the main goals of MASA solution is to provide complete privacy and protection of the user and UE information from the visiting serving network and make these information available only based on local regulatory and the Home Network policy. With this in mind, MASA solution offers a mechanism to shield every piece of private information and/or security capabilities from the serving network and provide the home network full control over which information the serving network needs to know about the user and the UE security capabilities after the home network successfully authenticate the user.

In addition, MASA solution provides a secure Initial Authentication Exchange mechanism that allows the home network operator to achieve the following:

1. When the UE IMEI is included in the encrypted IAR, the home network will have the opportunity to authenticate the UE and validate whether the UE is blacklisted, for example.

Lenovo Ex. 1007
Page 211

2. When the UE IMEI is included in addition to the UE security capabilities, MASA solution provides a secure mechanism for the home network to dynamically provision a security policy that takes in consideration, UE security capabilities, Local regulatory, geographical location, and the identity of the serving network the UE is attached to.

MASA solution provides a secure mechanism for the UE to include the subscriber security capabilities and for the home network to update the subscriber security capabilities when needed or whenever a specific security parameter(s) or algorithm(s) is obseleted or becoming vulnerable.

5.2.4.12.5.3 Evaluation#2

Editor's Note: This evaluation met with sustained objections from a small number of companies.

The main points addressed in this evaluation#2 are:

- Lack of modularity, which makes it hard to evaluate and compare MASA with competing proposals
- Unclear relation between system assumptions and protocol design resulting in unnecessary complexity and superfluous parameters
- Security issues with the protocol
- Doubtful claims of efficiency gains

Lack of modularity

MASA combines several features that should be specified as separate functions or procedures for clarity and ease of protocol analysis. It could then be studied later whether to piggy-back messages from one of these procedures onto messages of other procedures for efficiency reasons. At least the following features are identified:

- Mutual authentication and key establishment
- IMSI protection over the air
- Security Mode procedure / negotiation of crypto algorithms
- Prevention of attacks using unprotected authentication error messages

These features are addressed one by one in the following.

IMSI protection over the air

MASA achieves this by encrypting the IMSI with a public key of the home network. It seems the home network public key is not used for any other purpose in MASA.

- This feature can be separated out. It is present in other authentication protocols as well, cf. e.g. solution 7.3 in security area#7 or the proposal for EAP-AKA in untrusted access in S3-161664.
- Furthermore, there are proposals in security area#7 that claim to achieve IMSI protection over the air without the use of public keys, which is another reason to consider the IMSI privacy issue separately.
- Finally, MASA lacks the sophistication of a multi-layered identity approach of some of the proposals in security area#7 that have pseudonyms assigned by the home network as well as temporary identities assigned by the serving network. As a consequence, the IMSI is encrypted with a public key in every Attach request, which is very costly.

Security Mode procedure / negotiation of crypto algorithms

- Bidding down protection needs to be considered separately and should not be integrated with the authentication protocol in a monolithic fashion. The usual approach so far has been: UE sends the supported capabilities to the network, the network replies with an integrity-protected message containing both, a (hash of) the UE-supported capabilities, as received from UE, and the capabilities selected by the network. It needs to be explained why this approach would not work in 5G.

Lenovo Ex. 1007
Page 212

- Sending the UE-supported capabilities from the UE in a protected message, as done in MASA, is actually a disadvantage as it requires the UE to already select an algorithm for protection; but the selection of algorithms should be the outcome of the procedure.

Preventing attacks using unprotected authentication error messages

MASA provides a serving network public key to the UE for the explicit purpose of protecting future error messages.

- A serving network public key is simply assumed to be available. But it is a major discussion whether and how serving network public keys could be supported in 5G. The present evaluation is not suggesting that they cannot be supported, but at least issues around a global PKI, cross-certification among all operators, impact on security when some operators do not have private/public key pairs, and more, need to be thoroughly discussed. No such discussion is present in MASA.

- While it is true that DoS attacks on the UE are possible using error messages, it is doubtful whether one can get ever rid of unprotected authentication error messages: there can always be a mismatch, or a lack of UE authorization to access this particular network, or some other reason that prevents a successful run of an authentication and key establishment protocol.

- And after a successful run of an authentication and key establishment protocol, NAS security is available to protect further communication. When the NAS security context no longer works, for whatever reason, one is back to the need of running another round of authentication, with the unavoidable possibility of unprotected error messages, cf. previous bullet.

Unclear relation between system assumptions and protocol design, superfluous parameters

MASA has the following properties:

- The first authentication message is sent by the UE (as opposed to AKA where the first authentication message is sent by the network).

(The identity request is discounted here. It seems inspired by the optional identity request in the EAP framework. However, it can be argues that the EAP identity request is not needed in a 5G setting as the identity could be sent with the Attach request.)

- MASA is a three-way authentication handshake.

- Both sides generate random numbers for freshness, namely UE generates RAND1, RAND2, and HSS generates RAND (as part of AKA).

    - Under the assumptions above, one can find authentication protocols that are well understood, and even standardized. Existing protocols are not analyed and compared to MASA, so it is not clear why a totally new protocol like MASA is needed.

    - It is not clear why there should be a need for additional freshness parameters like the COUNTER and SQN (part of AKA) used in MASA, given that both sides already generate random numbers for frehsness. It is not explained what should be done if COUNTER gets out of synch between UE and HSS.

    - In contrast, AKA knows only two freshness parameters: RAND to guarantee freshness to the HSS, and SQN to guarantee freshness to the UE.

- IMSI and RAND1seem, according to the description part of both, the inner and the outer block of IAR.

So, MASA seems a convoluted mix of AKA and something new. Just having AKA, or just having something new without AKA, (with modular additions for IMSI privacy and algorithm negotiation for each) may be simpler while allowing to achieve the same goals. Of course, it would have to be demonstrated for the ‘something new’ in how much it would be superior to other proposals, e.g. EPS AKA* or EAP-AKA’ or EAP-TLS.

Lenovo Ex. 1007
Page 213

Security issues with the protocol

- HN cannot ascertain the freshness of KIARenc, KIARint, KIASenc, KIASint because they are derived from RAND1 and RAND2 generated by UE.
- It is not explained why the responder (HSS) has to even check that IAR, the first message from the initiator (UE), is fresh. This is unusual in authentication protocols.
- It is not explained why anything in the IAR, apart from the IMSI, needs confidentiality protection. The UE capabilities most likely do not need it. In the IAS from SEAN to UE, nothing seems to require confidentiality protection, and yet IAN is encrypted.
- It is not clear why the IAR inner block needs to be encrypted with a symmetric key when the whole IAR message is encrypted with the public key of the home network anyhow.
- SEAN can choose its own public key, there is no confirmation by the HN that the SEAN is authorized to use this public key, and the UE has no means to verify this authorization.

Doubtful claims of efficiency gains:

The claimed message saving is only due to the fact that the Security Mode procedure and AKA are combined into one procedure, i.e. they are achieved through piggy-backing of messages from one procedure onto the other, similar to what was done in GPRS with the Authentication and Ciphering Command. Of course, the usefulness of such piggy-backing should be investigated for 5G, but it has nothing to do with the efficiency of the authentication protocol, hence the comparison of MASA with AKA is skewed. 5.2.4.13Solution #2.13: AKA-based authentication for service provider connectivity

5.2.4.13.1 Introduction

The next generation system would be a flexible system supporting 3rd party services. According to Key Issue #2.9, based on the mutual trust between the operator and 3rd party services, the device/user related to 3rd party services should be authenticated to network access and the device should be able to authenticate the network. According to the Key Issue #2.1, providing the authentication capability of the network to operator and 3rd party services should be considered.

The goal of this solution is to provide an AKA-based authentication method for UE accessing to network for 3rd party service provider connectivity. The operator could control the authentication process entirely based on this solution.

5.2.4.13.2 Solution details

This solution addressed the Key issue #2.9 for security for service provider connectivity.

- The ARPF, AUSF, SEAF in the following figure are defined in clause 15.2.1.2:

Subscriber Repository Function: This function contains subscriber profiles for authorization, user identities and corresponding long-term credentials for authentication.

CP-AU authentication Function: A function in the core network that performs UE authentication process and interacts with Subscriber Repository Function for retrieving authentication materials.

- Assumptions of this solution:

3rd party service credential (Kser): Shared between the operator's network (e.g., AUSF) and 3rd party service provider after mutual trust between the operator and the 3rd party service provider is established. Also shared between the UE and the operator's network (e.g., AUSF).

It is assumed that Kser is preconfigured within ME device for the UE side.

There are several options for how AUSF obtains Kser:

Option1: The Kser is preconfigured in the AUSF

Option2: The Kser is preconfigured only in the ARPF residing in a 3rd party system as described in clause 5.2.1.2. And the AUSF could obtain Kser from this ARPF.

Lenovo Ex. 1007
Page 214

K_{NG}: The next generation key (like Kasme in LTE), derived from CK/IK and shared by UE and AUSF.

Editor's Note: How Kser is transferred is FFS.

Editor's Note: This is an optimized solution only for IoT device for one service; for multiple services it is ffs.

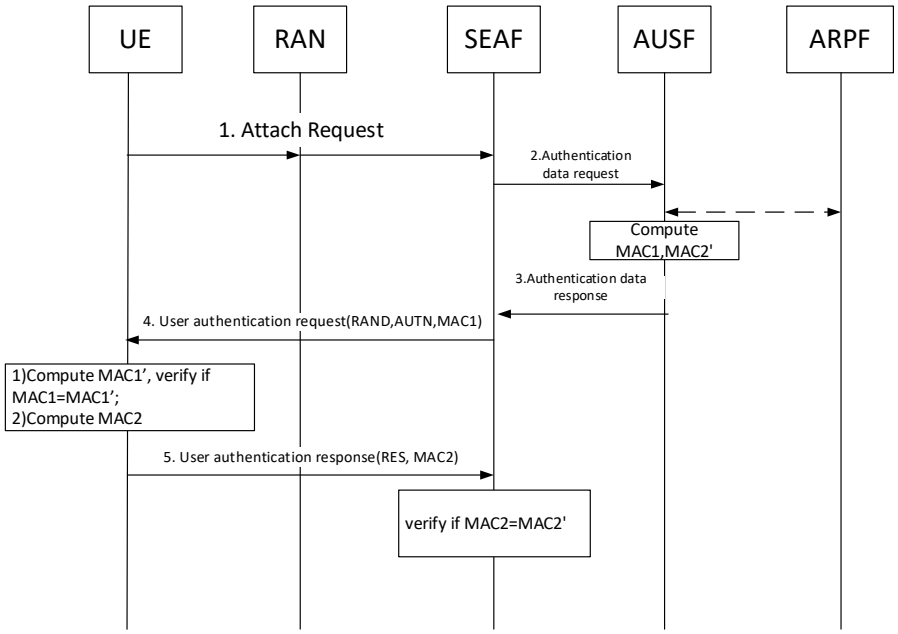


Figure 5.2.4.13.2-1 AKA-base network access authentication for service provider connectivity

1. UE sends request message to network to trigger the next authentication procedure which would be the attach request message. And the UE network identity (e.g., IMSI) and service identity are included in this message.

2. Upon receiving the request message from UE, the operator network needs to authenticate the UE, then the SEAF would fetch the authentication vector (RAND, AUTN, XRES, K_{NG}) from AUSF to perform user authentication. The K_{NG} could be generated in the similar way of Kasme.

3. The AUSF sends an authentication data response back to SEAF that contains the requested information (i.e., AV, MAC1, MAC2').

   The AUSF computes the MAC1 using the Kser, MAC and RAND. e.g., MAC1=f1 (Kser, MAC, RAND), where f1 function is the same as the f1 function used in the AKA procedure to generate MAC. The MAC1 could be used for the UE to authentication the network access for service provider connectivity based on Kser. Similarly, AUSF computes the MAC2' from RAND, XRES and Kser.

4. The SEAF sends to the UE the random challenge RAND, an authentication token AUTN for network authentication from the selected authentication vector and MAC1 included in a *user authentication request message*.

5. At receipt of this message, the USIM first computes XMAC and check if it equals MAC, if it's the same, then sends CK, IK, and RES to ME. Then ME could compute MAC1' from RAND, Kser and MAC to verify whether MAC1' equals MAC1. If the verifications are successful, the UE authenticates the operator and the 3rd party service provider.

   In order to allow the network to authenticate the UE, the ME computes the MAC2 from RAND, RES and Kser, and includes this parameter in a *user authentication response* back to the SEAF. e.g., MAC2=f1 (Kser, RES, RAND). The MAC2 could be used for the network to authentication the UE for service provider connectivity based on Kser.

6. At receipt of this message, the SEAF first checks if RES equals XRES, then verifies if MAC2' equals MAC2. If it's same, the network access authentication for service provider connectivity based on Kser has passed. If not, the SEAF might send an authentication reject message towards the UE.

Lenovo Ex. 1007
Page 215

5.2.4.13.3 Evalution

Tba.

5.2.4.14 Solution #2.14: Solution for non-AKA Authentication

5.2.4.14.1 Introduction

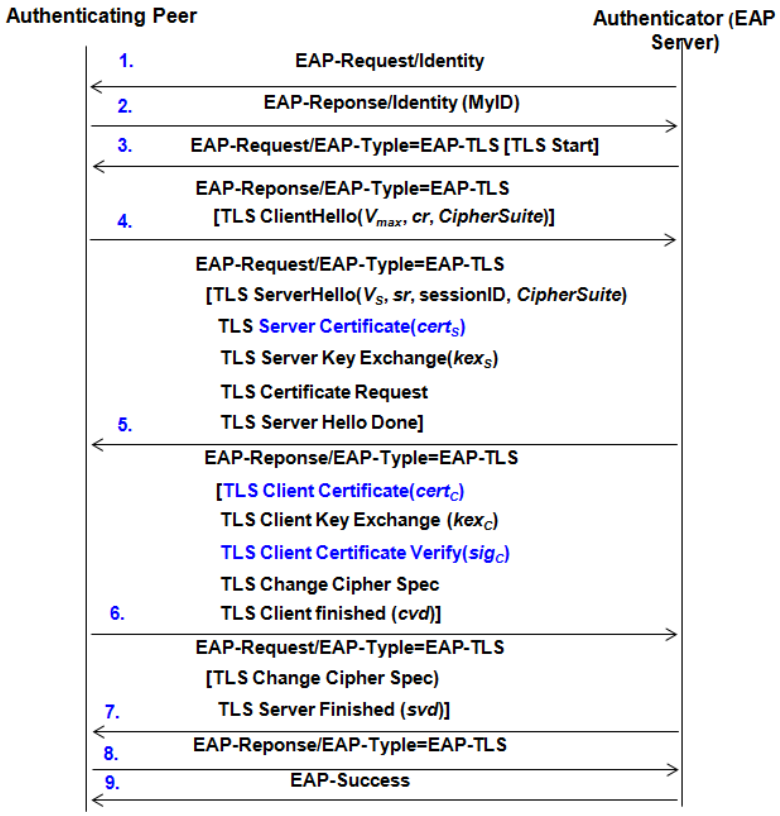
This solution addresses key issue #2.5.

In key issue 2.5, it requires the next generation system support non-AKA authentications. The requirement are as follows:

- The NextGen system needs to support an authentication process that can handle alternative authentication methods with different types of credentials.
- Impact of potential security breaches resulting from weaknesses in alternative authentication methods or in credential storage on the NextGen system as a whole has to be minimized. One possibility to consider is separation of the uses of different authentication methods into different network slices so that any negative effects of potential breaches are limited to one network slice.
- If, based on architectural decisions, 3GPP serving networks are to interact with security entities, e.g. AAA servers, of third party then the impact on the trust model needs to be studied.

There are a few potential candidates for alternative keys in a separate contribution, including password, PKI-based public key technologies, Identity-based public key technology etc. Considering the feasibility, efficiency (i.e. key size) and the capability of embedded service information into public key, Identity-based public key technology could be one of the suitable alternative keys for next generation system for alternative 3GPP subscriber credentials.

In this contribution, we propose an authentication framework and an example authentication protocol for the next generation system based on the Identity-based keys. The authentication is based on a revised EAP-TLS protocol as it is an EAP-based authentication protocol using public key for mutual authentication. Figure 5.2.4.14.1-1 depcits the generic authentication procedure based on the EAP-TLS. It can be further improved in the future.



Lenovo Ex. 1007
Page 216

Figure 5.2.4.14.1-1: a generic EAP-TLS authentication procedure

For the revocation, the main issue is to revocate the certificate or ID's of UE. A RSF can be setup at the network side for revocating various certificates. It can maintain a revocation list for different types of certificates, including PKI-based certificate or Identity-based IDs. For Identity-based cryptography, if RFC6507 is used for key generation, the revocation list need include the revoked ID, its PVT and expiration time. Operator can either revocate an ID or just revocate a PVT of a given ID.

UE and network use EAP-based authentication methods. In case UE roams to visit networks, it performs the mutual authentication with AUSF server within home network and pass the keys derived after authentication to the entities (e.g. SEAF) in the visit network.

To use the Identity-based Signature in mutual authentication, UE and network need to exchange information related Identity-based public keys. Since RFC 6507 is considerred for Identity-based public and private key generation. An entity, e.g. UE or AUSF need to be provisioned with (PVT, SSK) related to the ID of the entity, but only PVT and its expiration time need to be exchanged over the air interfae. So the overhead over air interface mainly consist of PVT and and its expiration time associated with the PVT. The overhead of ID is not considered since it is exchanged in other authentication methods also.

The size of PVT is related to the strength of security. For a security requirement of 128 bits, the size of PVT is 257 bits, or 33 bytes in length. The length of expiration time is 9 octets when using the unix time format, 5 octets for issuing time and 4 octets for validate time. Therefore, the additional overhead of using Identity-based mutual authentication is about 33 + 9 = 42 octets. In case signature is required, the size of signature is about 64 bytes.

For non-human IOT devices, the main concern of overhead is the computing power consumed in computing signauture. Comparing to the certificate, the required computing power is less since it does not need to verify the signature of certificates themselves. Table 1 shows the measured computing power for signature computing and signature validation.

Table 1: Computing Complexity Evaluation based on IETF 6507 (ARM M4 STM32F407, CPU 168 MHz, SRAM 128KB)

Operation	SECP128r1	SECP256r1
Signature Sign	20.8 ms	129 ms
Signature Verification	129 ms	683 ms

5.2.4.14.2 Solution details

5.2.4.14.2.1 A Framework for Non-AKA Authentication

To enable non-AKA authentication with ID-based credentials, a framework should be defined. A potential authentication framework is shown in Figure 5.4.2.14.2-1. In this framework, the authentication involves UE, AUSF, Revocation Server Fuction (RSF) and ARPF.

ARPF stores the master secret keys and system parameters that are used to generate SIGN-keys, include Public Validation Token (PVT), Secret Signing Keys (SSK), and KMS Secret (KSAK) according to the RFC 6507 [33].

AUSF stores the Identity-based keys and parameters, including ID_AUSF, PVT, SSK and KPAK. AUSF received keys and parameters from the ARPF. The PVT and SSK can be a short term key and only used for certain period and then the ARPF will provision another set of PVT and SSK to AUSF.

RSF stores those UE identities that have been revoked by the operator. The RSF is used to determine whether an UE is allowed perform mutual authentication with AUSF or not. After receiving an identiy from UE during the authentication procedure, the AUSF shall send a request to the RSF to check the validity of the UE_ID. RSF will return an indicator in the response to indicate whether the UE_ID is in the revocation list. If an identity is included in the list, AUSF shall terminate the authentication.

RSF could be co-located with AUSF or accessed through a non-standardized interface from AUSF.

Lenovo Ex. 1007
Page 217

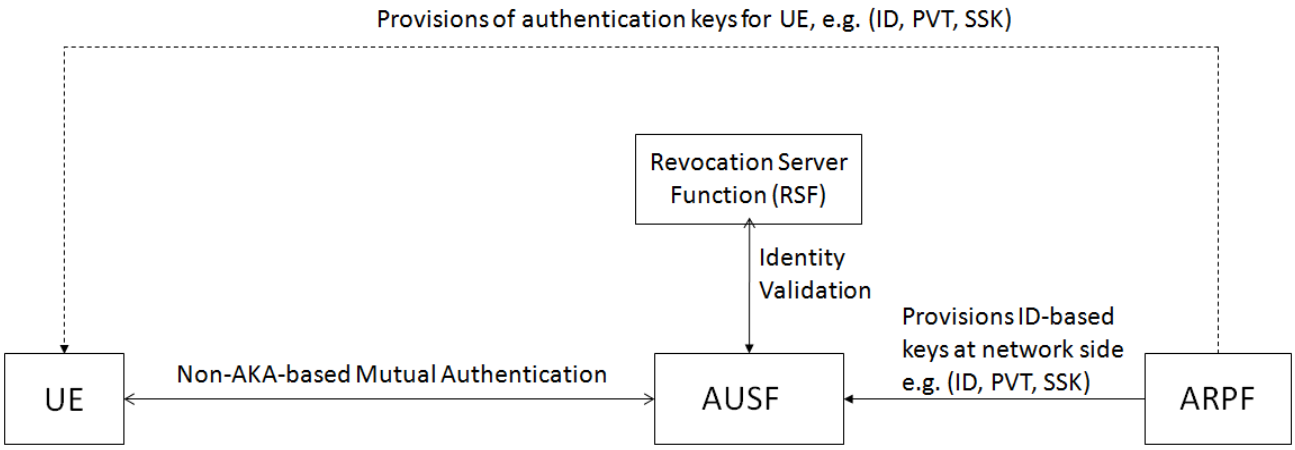


Figure 5.4.2.14.2.1-1: An Non-AKA based Authentication Framework with ID-based Credentials

5.2.4.14.2.2 Generic Procedure Description for Non-AKA Authentication

We assume that ARPF has all those secret keys and parameters that are required to generate Identity-based SING-Key as specified in the RFC 6507 [33]. We also assume UE has been provided with Identity based credential, including ID_UE, PVT, and SSK specific to the UE. ARPF also sends AUSF specific ID, PVT, SSK to AUSF. It is used by AUSF to generate signatures duringmutual authentication with UE.

To support the AUSF perform mutual authentication with UE, ARPF provisions UE with Identity-based credentials. The credentials can be a short term and used by AUSF for certain period such as one day and after that, a new set of credentials are provioned to the AUSF. The procedures are as follows:

a.1: ARPF provision AUSF with ID_AUSF, PVT and SSK.

a.2: AUSF stores ID_AUSF, PVT and SSK. It is used for mutual authentication with UE later.

When UE want to attach to the network, following procedure is perfomed:

1. UE sends its identity to the AUSF.
2. AUSF extract the identiy and send it to the RSF for validation.
3. RSF check whether the received identity is in the revocation list or not and a result is generated based on the validation.
4. RSF send back the result to the AUSF.
5. AUSF determine whether it should terminate the authentication procedure or not based on the results from RSF.

Lenovo Ex. 1007
Page 218

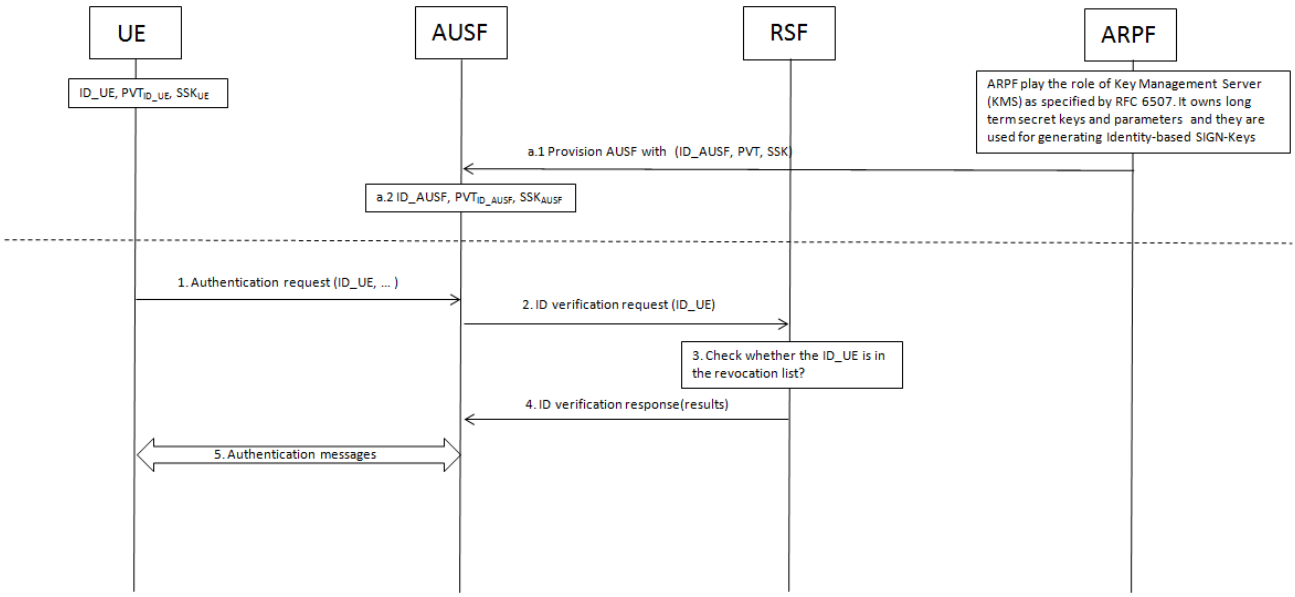


Figure 5.4.2.14.2.2-1: Generic Procedures for Non-AKA based Authentication with Identity-based Credentials

5.2.4.14.2.3 Non-AKA Authentication Protocols based on EAP-TLS

In this solution, we give an example authentication method. It can be improved further in the future, e.g. In this example solution, we assume that both network side and UE side are provisioned with Identity-based credentisals, which include an identity, a private key for signature and a KMS Public Authentication Key (KPAK) as defined in RFC 6507 [33] as a computing parameter.

We modify the EAP-TLS as follows:

Step 1, the same as EAP-TLS

Step 2, After receiving the EAP-Response with UE's identity, ID_UE.Step 3, AUSF send ID_UE to RSF for validation

Step 4, RSF validate the ID_UE based on the revocation list stored.

Step 5, RSF sends back the validation result to the AUSF

Step 6, If ID_UE is valid, then AUSF sends the EAP-TLS start message to UE.

Step 7, UE sends an EAP-TLS response to AUSF, including the CipherSuite used for AUSF.

Step 8, Server sends an EAP request with identity related public key information, including ID_AUSF, PVT_AUSF, and also signature signed with the SSK of AUSF..

Step 9, After verifying the Idenitity and signature of AUSF, UE sends EAP response including UE's ID and PVT, a signature signed with the SSK of UE, and also other fields required by EAP-TLS.

Step 10 - 12, the same as EAP-TLS step 6 – 8 as shown in Figure 5.2.4.14.1-1 .

Lenovo Ex. 1007
Page 219

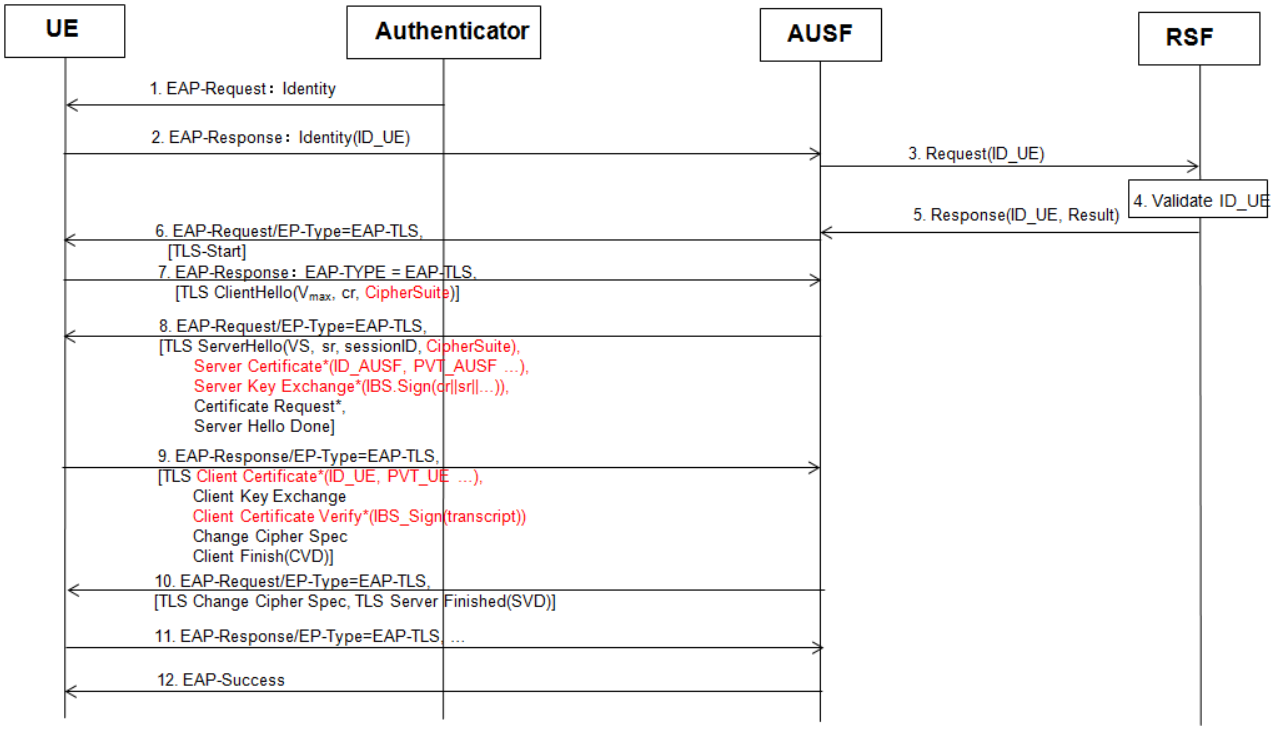


Figure 5.4.2.14.2.3-1: Non-AKA Authentication Methods with Identiy-based Credentials and EAP-TLS

NOTE: Using EAP-TLS for ID-based mutual authentication between UE and network is just one potential candidate.

In case an identity of UE is revocated, the operator adds the UE ID and PVT in the revocation list on the RSF. The operator can also notify the charging and billing system to stop charging on the relevant UE if it has no other valid PVT in use.

5.4.2.14.2.4 Non-AKA Authentication Protocols based EAP-PSK and Identity-based Credentials

In this solution, we give another example authentication method for non-AKA based authentication. Similar to the previous method, we assume that both UE and AUSF are provisioned with Identity-based credentials, which include an identity, a private key for signature (SSK) , a Public Verification Token (PVT) a KMS Public Authentication Key (KPAK) as defined in RFC 6507 [33] as a computing parameter.

With the provisioned credentials, the UE and AUSF can derive symmetric keys based on static Diffie-Hellman by exchanging the identity information and the PVT, and then use the SSK owned by each entity. For exampke, UE can derive a key after it receives the identity of AUSF and its PVT, denoted as ID_AUSF and PVT_AUSF respectively, as follows:

K_UE = [SSK_UE](KPAK+[hash(G || KPAK || ID_AUSF || PVT_AUSF)]PVT_AUSF))

where G is a generation point on the elliptic curve used by the KMS to generate keys for UE and networks. It is provisioned to UE and AUSF by the KMS together with SSK, PVT, and KPAK etc. The use of hash function can follow the Annex A of RFC 6507 [33].

Similarly, AUSF can derive also derive K_AUSF as follows after it receives the identity and PVT from UE as follows:

K_AUSF = [SSK_AUSF](KPAK+[hash(G || KPAK || ID_UE || PVT_UE)]PVT_UE))

It can be proved that K_UE actually equals to K_AUSF.

With above properties, we can use EAP-PSK for mutual authentication as follwows:

Step 1: UE send an attach request to the AUSF and indicate that EAP-PSK shall be used for mutual authentication.

Step 2: AUSF verify the authentication type and decide authentication method

Lenovo Ex. 1007
Page 220

Step 3: AUSF send the first message of EAP-PSK to UE with identity field contains the ID_AUSF and PVT_AUSF, and aso a random number RAND_S as required by EAP-PSK.

Step 4: UE derive a symmetric key as K = [SSK_UE](KPAK+[hash(G || KPAK || ID_AUSF || PVT_AUSF)]PVT_AUSF)). UE generates a random number RAND_P and further derives K' = KDF(K, RAND_P, RAND_S). UE derives Authentication Key AK and Key Derivation Key based on RFC 4764 for EAP-PSK [82].

Step 5: UE sends the second messges of EAP-PSK to AUSF, which contains RAND_S, RAND_P, a MAC for authentication, and identity field that consists of ID_UE and PVT_UE.

Step 6: AUSF send ID_UE to RSF for validation

Step 7: RSF validate the ID_UE according to its revocation list.

Step 8: RSF send back the validation results to the AUSF.

Step 9: If the ID is valid, then AUSF derive a symmetric key as K = [SSK_AUSF](KPAK+[hash(G || KPAK || ID_UE || PVT_UE)]PVT_UE)). UE generates a random number RAND_P and further derives K' = KDF(K, RAND_P, RAND_S). AUSF derives Authentication Key AK and Key Derivation Key based on RFC 4764 for EAP-PSK [82]. AUSF authenticates the UE based on the MAC_P received from the message. AUSF further derives session key base on RAND_P and KDK.

Step 10: AUSF sends the third message of EAP-PSK to UE with a MAC_S for authentication and other fields required by EAP-PSK.

Step 11: UE authenticates the AUSF with MAC_S received and derive session key with RAND_P and KDK derived previously.

Step 12: UE sends the last message of EAP-PSK to AUSF to finish the EAP-PSK authenticatin procedure.

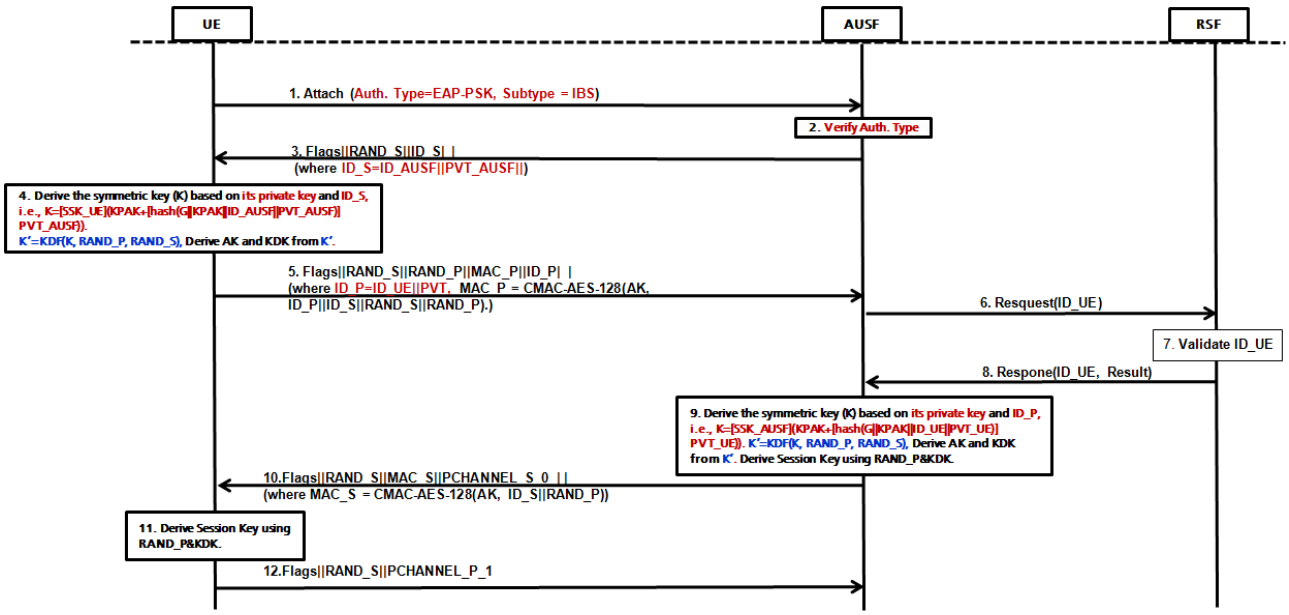


Figure 5.4.2.14.2.4-1: Non-AKA Authentication Methods with Identiy-based Credentials and EAP-PSK

5.2.4.14.3 Evaluation

tba.

5.2.4.15 Solution #2.15: Aggregate Authentication for massive IoT

5.2.4.15.1 Introduction

This solution is designed for the case that many UEs are trying to access the network at the same time.

Lenovo Ex. 1007
Page 221

This solution addresses the key issue 5.2.3.7:

- *Efficient authentication for a group of IoT devices to reduce the signalling overhead is required in NexGen network to lighten the impact on the network, and more importantly, to decrease the chance of signalling storm.*

The proposed solution is to aggregate the authentication message at an aggregation node (the aggregation node can be a base station, a relay UE, or a gateway), and then the aggregation node sends the aggregated authentication message to the authentication unit of the network for group authentication. In this way, we can greatly reduce the number of authentication messages and the size of the authentication message received by the authentication unit.

5.2.4.15.2 Solution details

The architecture of the proposed solution is given in Figure 5.2.4.15.2-1.

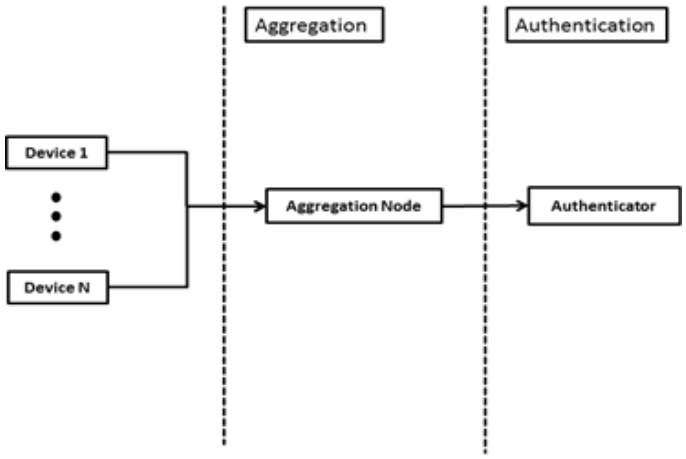


Figure 5.2.4.15.2-1: Proposed Architecture for Aggregation Authentication

In the proposed solution, we assume that both IoT UEs and the network authenticator are pre-provisioned with IBS credentials.

The solution details are as follows:

1. Each IoT UE generates a random number , and uses the random number to generate its Diffie-Hellman (DH) Public Key.

   1a. UE 1generates a random number denoted by RAND 1, and computes its DH public key A1 by $A1=g^{RAND\ 1} \bmod p$

   1b. UE 2generates a random number denoted by RAND 2, and computes its DH public key A2 by $A2=g^{RAND\ 2} \bmod p$

2. Each IoT UE generates an authentication message including its ID, its DH public key, and signs the message using its IBS private key, and sends the message to the aggregation node.

   2a. UE1 generates an authentication message including its ID (ID_UE1), its DH public key (A1), and signs the message using its IBS private key, and sends the message (ID_UE1, A1, Sig1_UE1, …) to the aggregation node.

   2b. UE2 generates an authentication message including its ID (ID_UE2), its DH public key (A2), and signs the message using its IBS private key, and sends the message (ID_UE2, A2, Sig1_UE2, …) to the aggregation node.

3. Upon receiving the messages from IoT UEs, the aggregation node does signature aggregation and generates an aggregated signature Sig1_AG, and packages the authentication message from IoT UEs into one aggregated authentication message.

Lenovo Ex. 1007
Page 222

4. The aggregation node sends the aggregated message to authenticator。The aggregated message includes an indicator (Aggre-indicator) that indicates the message is an aggregated authentication message. The aggregated message should include IoT UEs' ID and their DH public keys. A suggested message format is (Aggre-indicator, ID_Vec, A_Vec, Sig1_AG,…).
5. Upon receiving the message, the authenticator first verifies the aggregated signature (Sig1_AG). If the verification is successful, the authenticator generates a random number (RAND_AU), and computes its DH public key B by $B=g^{RAND\_AU} \bmod p$.
6. Authenticator sends an authentication response message to the aggregation node. The authentication message should include the authenticator's ID (ID_AU), the authenticator's DH public key (B), IoT UE's public keys (A_Vec). The authenticator should sign the message using its IBS private key.
7. Upon receiving the message, the aggregation node forwards the message to IoT UEs.
   7a. The aggregation node forwards the message (ID_AU, B, A_Vec, Sig_AU, …) to IoT UE1
   7b. The aggregation node forwards the message (ID_AU, B, A_Vec, Sig_AU, …) to IoT UE2
8. Upon receiving the message, IoT UEs verify the signature of the authenticator (Sig_AU), and generate session keys using the received DH public key (B).
   8a. IoT UE1 verifies the signature of the authenticator (Sig_AU), and generates the session key $K1=B^{RAND\ 1} \bmod p$.
   8b. IoT UE2 verifies the signature of the authenticator (Sig_AU), and generates the session key $K2=B^{RAND\ 2} \bmod p$.
9. Each IoT UE signs the authenticator's DH public key (B) using its IBS private key, and sends its back to aggregation node.
   9a. IoT UE1sends (B, Sig2_UE1, …) back to the aggregation node, where Sig2_UE1is the signature .
   9b. IoT UE2sends (B, Sig2_UE2, …) back to the aggregation node, where Sig2_UE2 is the signature.
10. Upon receiving the messages from IoT UEs, the aggregation node does signature aggregation and generates an aggregated signature Sig2_AG, and packages the authentication message from IoT UEs into one aggregated authentication message.
11. The aggregation node sends the aggregated message to authenticator。The aggregated message should include IoT UEs' ID and the fed back DH public keys of the authenticator. A suggested message format is (ID_Vec, B_Vec, Sig2_AG,…).
12. Upon receiving the message, the authenticator first verifies the aggregated signature (Sig2_AG). If the verification is successful, the authenticator generates the corresponding session key for each IoT UE, i.e., $K1=A1^{RAND\_AU} \bmod p$ and $K2=A2^{RAND\_AU} \bmod p$.

Lenovo Ex. 1007
Page 223

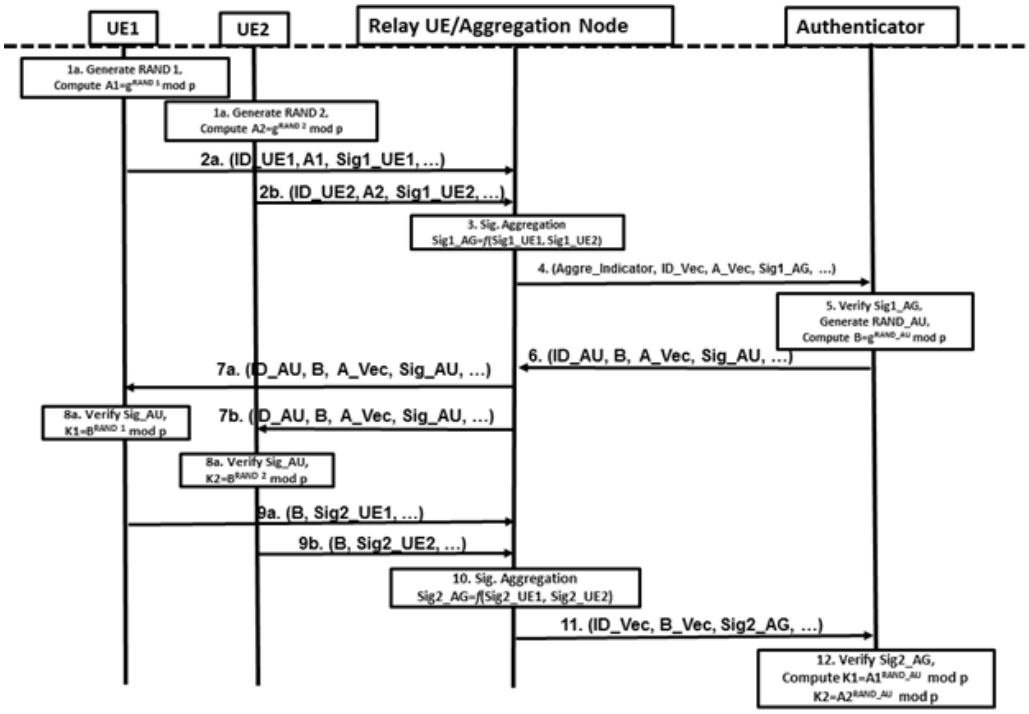


Figure 5.2.4.15.2-2: Aggregation Authentication for IoT Devices

When the aggregate authentication failed, the following procedure will be activated.

1. The Authenticator sends an message to indicate that the aggregate authentication failed.
2. Upon receiving the message, the aggregation node decides the re-authentication strategy. Three re-authentication strategies are suggested here:
   a. Redo the aggregate authentication;
   b. Divide users into subgroups and do the aggregate authentication for each subgroup;
   c. Instruct each UE to do mutual authentication with the network authenticator directly.
3. After the aggregation node decides the re-authentication strategy，it broadcasts a re-authentication indicator (ReAu_Sel_Indicator) to each UE, and each UE decides its re-authentication strategy based on the re-authentication indicator .

Lenovo Ex. 1007
Page 224

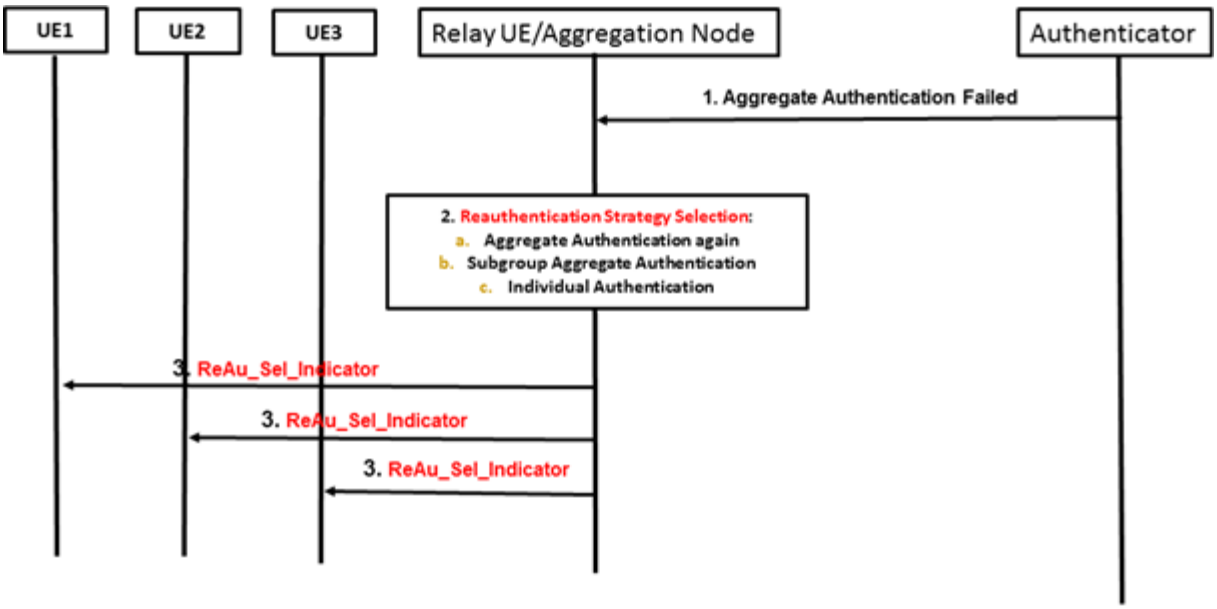


Figure 5.2.4.15.2.3: Procedures when Aggregation Authentication failed

5.2.4.15.3 Evaluation

5.2.4.16 Solution #2.16: Mutual Authentication between Remote UE and Network over A Relay based on ID-based Credentials

5.2.4.16.1 Introduction

This solution addresses the key issue 5.9.3.1:

- *It shall be possible to uniquely identify an UE (e.g. wearable device), when it is connected to the network via another UE (e.g. smart phone).*
- *It shall be possible to mutually authenticate the remote UE and the network when the remote UE is in direct network connection or in indirect network connection.*

In this proposal, we design use an IBS-based mutual authentication scheme between the remote UE and the network over a relay. The IBS-based mutual authentication scheme can achieve end-to-end authentication between the remote UE and the network. It can also help the network to identify an UE which is connected to the network via another UE.

Editor's note: it if ffs how network element other than the authenticator uniquely identifies the remote UE.

5.2.4.16.2 Solution details

In the proposed solution, we assume that both the remote UE and the network are pre-provisioned with IBS credentials. All the entities, including remote UE, relay UE and authenticator, belong to the same Key Management Server (KMS).

Editor's note: The relationship between remote UE and relay UE need to be clarified.

The solution details are as follows:

1. Remote UE generates a random number , and uses the random number to generate its Diffie-Hellman (DH) Public Key by $A=g^{RAND\ 1}$ mod p.

2. Remote UE generates a remote UE authentication request message including its ID (ID_UE), its DH public key (A), an indicator (RUE_Indicator) that indicates the message is remote UE authentication request, and signs the message using its IBS private key, and sends the message (RUE_Indicator , ID_UE, A, Sig1_UE, …) to the relay UE.

Editor's note: the terms "RUE" should be defined.

Lenovo Ex. 1007
Page 225

3. Upon receiving the message from the remote UE, the relay UE first identifies it is a remote UE authentication request message by identifying the indicator (RUE_Indicator).

4. After verifying the indicator, the relay UE forwards the remote UE authentication request message to the authenticator.

5. Upon receiving the message, the authenticator first verifies the signature (Sig1_UE). If the verification is successful, the authenticator generates a random number (RAND_AU), and computes its DH public key B by $B=g^{RAND\_AU}$ mod p.

6. Authenticator generates an authentication response message. The authentication message should include the authenticator's ID (ID_AU), the authenticator's DH public key (B), the remote UE's DH public keys (A). The authenticator should sign the message using its IBS private key. Authenticator sends the authentication response message (ID_AU, B, A, Sig_AU, …) to the relay UE.

7. The relay UE forwards the authentication response message (ID_AU, B, A, Sig_AU, …) to the remote UE.
8. Upon receiving the message, the remote UE verifies the signature of the authenticator (Sig_AU), and generates the session key using the received DH public key (B) by $K=B^{RAND\ 1}$ mod p.

9. The remote UE signs the authenticator's DH public key (B) using its IBS private key, and sends its back to the relay UE. The remote UE sends (B, Sig2_UE, …) back to the relay UE.

10. Upon receiving the messages from the remote UE, the relay UE forwards the remote UE authentication response message (B, Sig2_UE, …) to the authenticator.

11. Upon receiving the message, the authenticator first verifies the signature (Sig1_UE). If the verification is successful, the authenticator generates the session key for the remote UE, i.e., $K=A^{RAND\_AU}$ mod p.

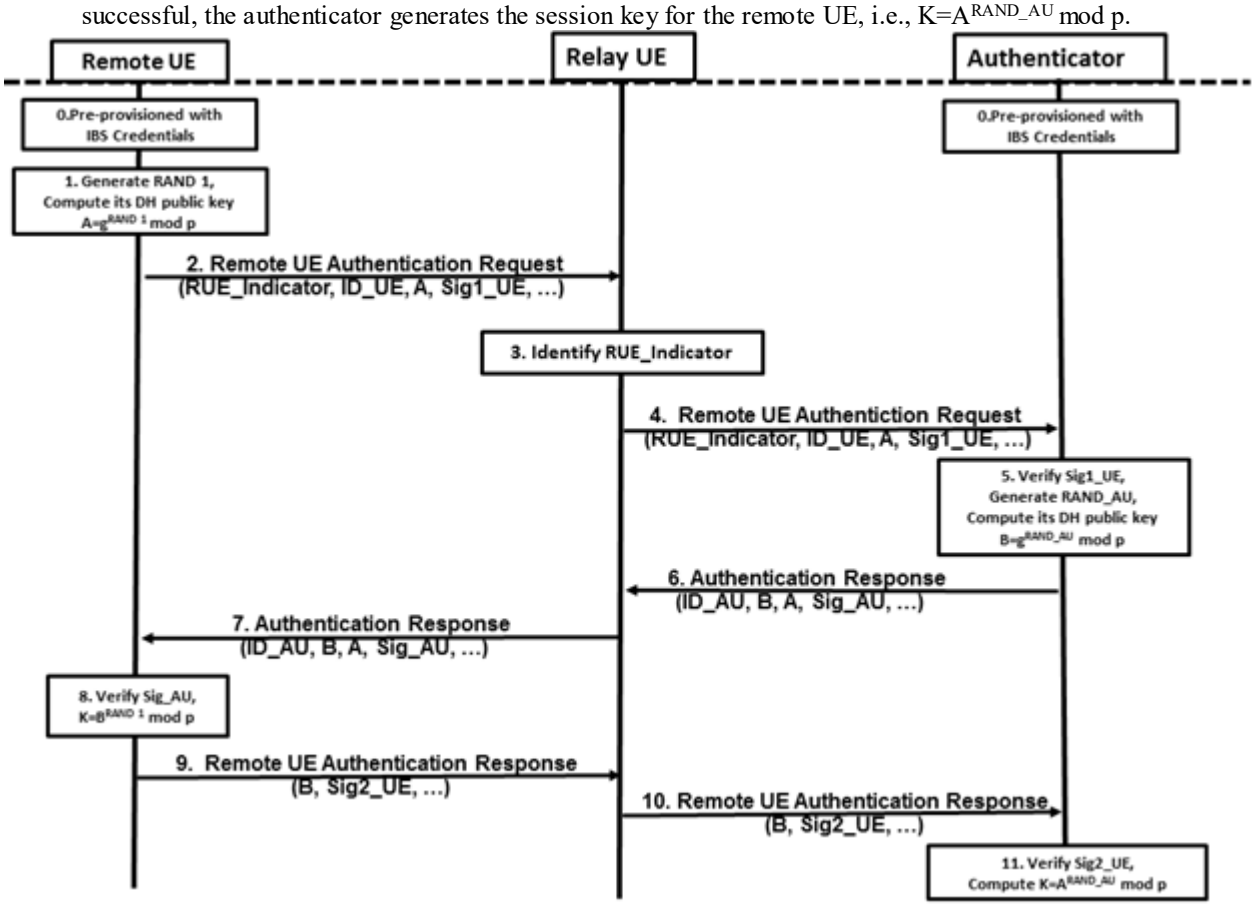


Figure 5.2.4.16.2-1: Mutual Authentication between Remote UE and Network over A Relay

Editor's note: it is ffs whether the relay UE need to authenticate the remote UE and how this is met.

Lenovo Ex. 1007
Page 226

5.2.4.16.3 Evaluation

5.2.4.17 Solution #2.17: Equipment identifier Authentication using the device certificate and IMEI binding

5.2.4.17.1 Introduction

This solution uses the (IMEI, device certification) binding to addresses Key issue #2.4: Equipment identifier authentication. In this solution, the following pre-configurations are needed:

- When a device is at the manufacture, a device certificate and the private key associated with the certificate are provisioned by the device's manufacturer or trusted third party. The device certificate is signed by a Certificate Authority (CA). The CA can be a device manufacturer CA or a trusted 3rd party CA that is trusted by the manufacturer.
- The private key associated with the device certificate shall be securely stored in the device.
- The device certificate and the equipment identifier (i.e. IMEI) are bound and the (IMEI, Device Certificate) binding is published in the manufacturer's device repository or third party's repository. The certificate does not need to include the plain text of the equipment identifier because they have been bound to each other in the repository. So the equipment identifier will not be disclosed even if the device certificate is published.

NOTE: It is ffs what information will be wroten in the subject field.

- An operator, if trusts the device manufacturer CA or a 3rd party CA, can inquire the (IMEI, Device Certificate) binding from the manufacturer's device repository or third party's repository.
- The CA's certificate or public key needs to be pre-configured in the operator's AAA/HSS or CP-AU/CP-CN. It can also be stored with the (IMEI, device Certificate) binding in the repository.

5.2.4.17.2 Solution details

The following figure describes the message flows of equipment identifier authentication:

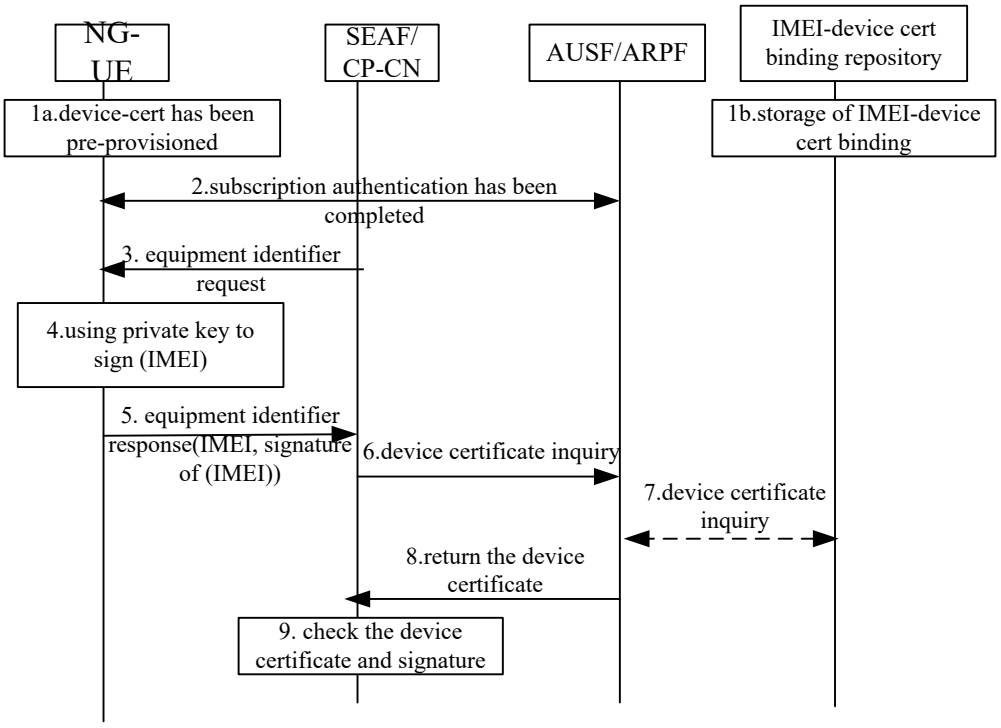


Figure 5.2.4.17.2-1: equipment identifier authentication based on (IMEI, device cert) binding

Lenovo Ex. 1007
Page 227

1) The device certificate has been pre-provisioned in the NG-UE and the private key associated with the device certificate has been securely stored in the device. The (IMEI, device certificate) binding has been published and stored in the repository of the manufacturer or 3rd party trusted by the manufacturer.

2) The mutual authentication has been performed between the network and the NG-UE.

3) The network entity (e.g. SEAF or CP-CN) sends the equipment identifier request..

4) The NG-UE uses the private key to sign the IMEI.

5) The NG-UE returns the equipment identifier response to the SEAF/CP-CN. This message includes the IMEI and the signature of the IMEI. This response should be encapsulated in a signalling message which can protect the identity from leaking and replay attack, like the NAS SMP message in LTE.

6) The SEAF/CP-CN sends the device certificate inquiry including the received device's IMEI to the AUSF/ARPF.

7) The AUSF/ARPF inquires the device certificate using the IMEI from the (IMEI, device certificate) binding repository.

Editor's Note: It is FFS whether the binding between the IEMI and device certificate can be cached in the AUSF/ARPF or not.

8) The AUSF/ARPF returns the device certificate to the SEAF/CP-CN.

9) The SEAF/CP-CN uses the CA's public key to verify the device's certificate. If the verification is successful, the SEAF/CP-CN uses the public key in the device certificate to check the signature. The equipment identifier is authenticated if the signature check is successful.

NOTE: The CA's public key can be pre-configureted in SEAF/CP-CN and can also be acquired from the (IMEI, device certificate) binding repository via AUSF/ARPF if the CA's public key is pre-stored in the repository.

5.2.4.17.3 Evaluation

This solution saves the valueable air resource as it does not transimit the device certificate in the air interface. Since the binding between the IMEI and the device certificate is maintained in the repository and only the authorized entities can inquire the binding, this solution can prevent the leakage of the equipment identifier.

The inquiring the (IMEI, device certificate) binding causes the inquiry workload less than the authentication of the device certificate directly (cf. the solution #2.10). Since the equipment identifier authentication is infrequent, the inquiry wokload does not seriously affect the network. The AUSF/ARPF can also store the (IMEI, device certificate) binding in the local to reduce the inquiry workload.

In this solution, the manufacturer or a 3rd party which issues the decive certificate nees to be trusted by the operators.

Editor's note: The solution should be modified to avoid the dependency on a 3rd party for the authentication of the reported equipment identifier (e.g., the operator doesn't need to make use of any entities outside of operator's network)

5.2.4.18 Solution #2.18: Equipment identifier Authentication using the device public key and IMEI binding

5.2.4.18.1 Introduction

To compare with Solution #2.x in section 5.2.4.x, this solution uses the (IMEI, device public key) binding to addresses Key issue #2.4. In this solution, the following pre-configurations are needed:

- When a device is at the manufacture, a device public key and the private key associated with the public key are provisioned by the device's manufacturer.

- The private key associated with the device public key shall be securely stored in the device.

Lenovo Ex. 1007
Page 228

- The device public key and the equipment identifier (i.e. IMEI) are bound and the (IMEI, device public key) binding is published in the manufacturer's device repository or third party's repository.
- An operator, if trusts the device manufacturer or a 3rd party, can inquire the (IMEI, device public key) binding from the manufacturer's device repository or third party's repository.

5.2.4.18.2 Solution details

The following figure describes the message flows of equipment identifier authentication:

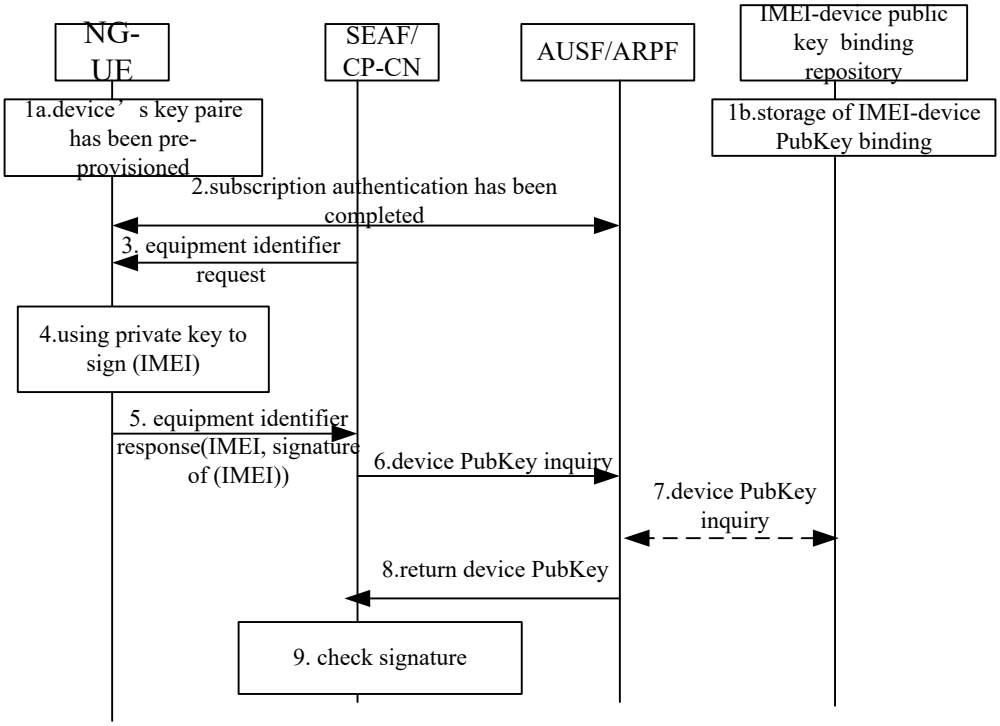


Figure 5.2.4.18.2-1: equipment identifier authentication based on (IMEI, device public key) binding

1) The NG-UE has been pre-provisioned the public key and the private key associated with the public key has been securely stored in the device. The (IMEI, device public key) binding has been published and stored in the (IMEI, device public key) bingding repository of the manufacturer or 3rd party trusted by the manufacturer.
2) The mutual authentication is performed between the network and the NG-UE.
3) The network entity (e.g.SEAF or CP-CN) sends the device identity request..
4) The NG-UE uses the private key to sign the IMEI.
5) The NG-UE sends the equipment identifier response to the SEAF/CP-CN. This message includes the IMEI and the signature of the IMEI. This response should be encapsulated in a signalling message which can protect the identity from leaking and replay attack, like the NAS SMP message in LTE.
6) The SEAF/CP-CN sends the device public key inquiry which includes the device's IMEI to the AUSF/ARPF.
7) The AUSF/ARPF inquires the device public key using the IMEI from the (IMEI, device public key) binding repository.

Editor's Note: It is FFS whether the binding between the IEMI and device public key can be cached in the AUSF/ARPF or not.

8) The AUSF/ARPF returns the device public key to the SEAF/CP-CN.
9) The SEAF/CP-CN uses the public key to check the signature. The equipment identifier is authenticated if the signature check is successful.

Lenovo Ex. 1007
Page 229

5.2.4.18.3 Evaluation

This solution is comparatively simple compared to the solution #2.17 as it does not need to deploy PKI. This solution can also save the valueable air resource as it does not transimit the device public key in the air interface. Since the equipment identifier is transmitted through a protected signalling message, this solution can prevent the leakage of the equipment identifier.

The inquiring the (IMEI, device public key) binding causes the inquiry workload less than the authentication of the device certificate directly (cf. the solution #2.10). Since the equipment identifier authentication is infrequent, the inquiry wokload does not seriously affect the network. The AUSF/ARPF can also store the (IMEI, device public key) binding in the local to reduce the inquiry workload.

In this solution, the manufacturer or a 3rd party which issues the decive public key needs to be trusted by the operators. Editor's note: The solution should be modified to avoid the dependency on a 3rd party for the authentication of the reported equipment identifier (e.g., the operator doesn't need to make use of any entities outside of operator's network)

5.2.4.19 Solution #2.19: Alternative EAP architecture for 3GPP access

5.2.4.19.1 Introduction

This solution addresses Key Issue #2.1.

This solution provides serving network binding to the key delivered to the 3GPP serving network for general EAP protocols by using EMSK to derive the key that is passed down from the EAP server. This allows the keys used in the 3GPP access to be bound to their specific role in a similar way to K_{ASME} in LTE.

In this solution, the nodes between the NG-UE and AUSF will just have to transparently pass on the EAP packets. For the description of the solution, we consider the element that terminates the NAS mobility management messages as the CN-MM.

5.2.4.19.2 Solution details

5.2.4.19.2.1 Protocol Stack

Figure 5.2.4.19.2.1-1 provides a possible protocol stack for carrying the EAP messages between the NG-UE and the AUSF.

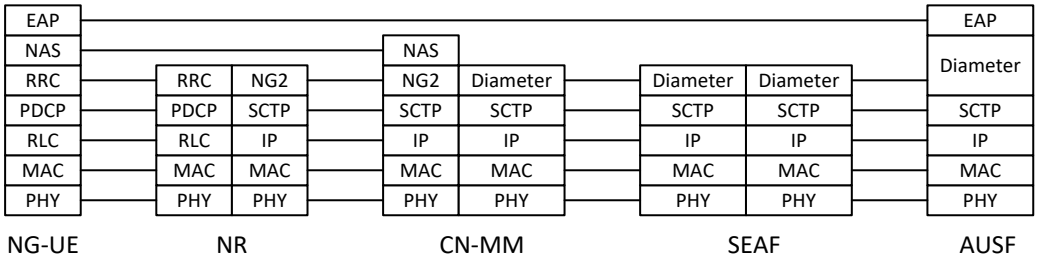


Figure 5.2.4.19.2.1-1: Protocol Stack

5.2.4.19.2.2 Authentication flows

Figure 5.2.4.19.2.2-1 provides the flows for EAP authentication in the NextGen network. A description of the steps follows the figure.

NOTE 1: Identity used in the below flow is the subscription identifier.

Editor's Note: the choice of authentication method may need to be added to the AUSF.

NOTE 2: For this solution, the AUSF is in the home network.

Lenovo Ex. 1007
Page 230

Editor's Note: It should be clarified whether the present solution would work with trusted and untrusted non-3GPP access.

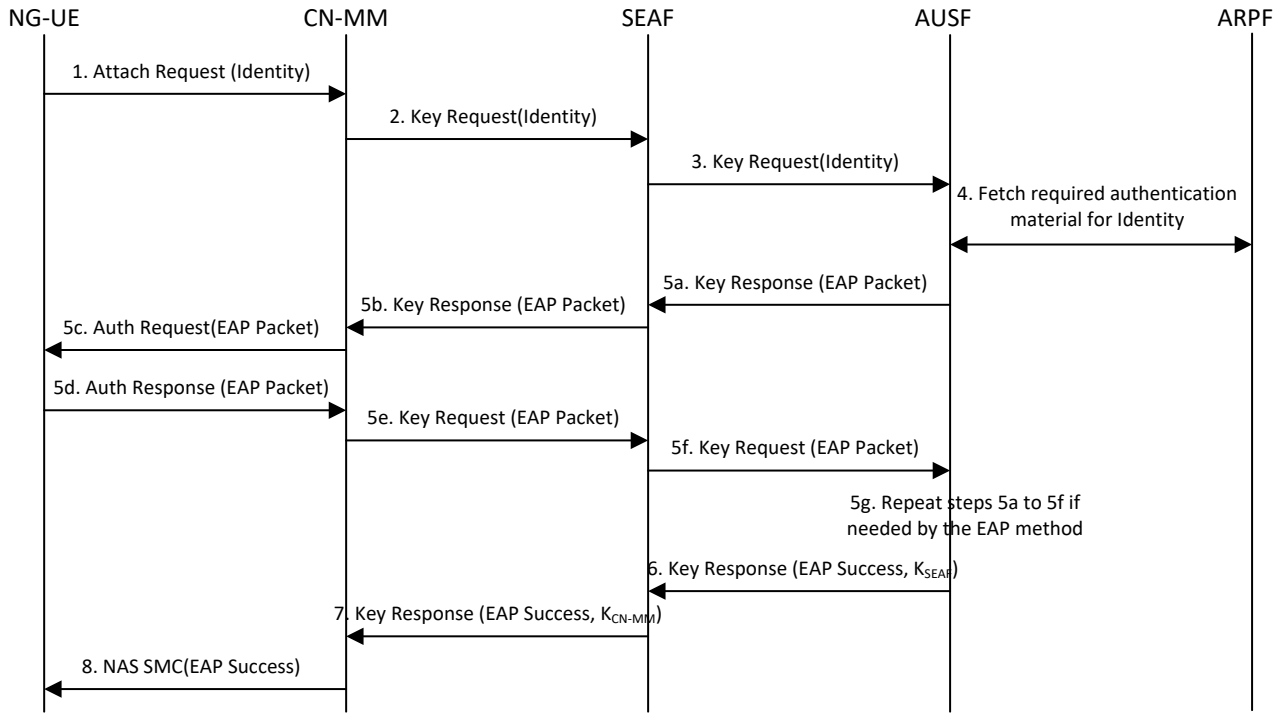


Figure 5.2.4.19.2.2-1: Authentication flow for EAP with AUSF as authenticator

1. The NG-UE sends Attach Request to the CN-MM and include its Identity.

2. The CN-MM requests a K_{CN-MM} for this NG-UE from the SEAF.

3. The SEAF request a K_{SEAF} for the NG-UE from the AUSF.

4. The AUSF decides to trigger an authentication for the NG-UE. It fetches the needed material to run the appropriate EAP method (identified by the Identity that is passed the AUSF) from the ARPF.

5a – 5g. The AUSF runs the EAP method with the UE. They may be several round trip between the AUSF and NG-UE.

NOTE 2a: Use of this propsal with an AKA method over EAP requires the setting and checking of the key separation bit as described in the EAP AKA' RFC 5448 [61]. Hence it is recommended to only use EAP AKA' with this method.

6. Once the EAP method has successfully completed, the AUSF calculates K_{SEAF} from the EMSK. It sends the K_{SEAF} along with the EAP Success packet to the SEAF.

NOTE 2b: EMSK (rather then MSK) is used to calculate K_{SEAF} as this means that there is no need to restrict the use of the credentials used to access to 3GPP access only. If such a restriction is not applied, then MSK may be sent to a non-3GPP entity which could then calculate the K_{SEAF}. If the MSK is stolen (e.g., by compromising the non-3GPP entity), then it would be used to impersonate 3GPP network.

7. Due to the presence of the K_{SEAF} or an indication in the lower layers, the SEAF is aware that the authentication succeeded. It calculates K_{CN-MM} from the K_{SEAF}. The SEAF sends K_{CN-MM} and the EAP Success packet to the CN-MM.

8. Due to the presence of the K_{CN-MM} or an indication in the lower layers, the CN-MM is aware that the authentication succeeded. It calculates the NAS keys from the K_{CN-MM}. The SEAF sends the EAP Success packet to the NG-UE in the NAS SMC.

NOTE 3: If for protocol reasons, the EAP Success cannot go with the NAS SMC, it is sent in a separate NAS message before the NAS SMC is sent.

Lenovo Ex. 1007
Page 231

NOTE 4: EAP-AKA' already achieves this goal by design. The present solution is therefore not needed for EAP-AKA'. Applying the present solution to EAP-AKA' would lead to a duplication of effort for achieving the same goal and should be avoided. But it is true that not all EAP authentication methods achieve the goal of serving network binding. Such methods could, in principle, benefit from enhancements providing such binding.

NOTE 5: The solution relies on calculating a key bound to the visited network in the home network. Hence the solution will not work if the EAP Server is placed in the serving network.

5.2.4.19.3 Evaluation

The stated protocol goal is to provide "serving network binding to the key delivered to the 3GPP serving network for general EAP protocols by using EMSK to derive the key that is passed down from the EAP server."

5.2.4.20 Solution #2.20: void

5.2.4.21 Solution #2.21: Linking update location with authentication confirmation

5.2.4.21.1 Introduction

This solution addresses key issue #2.16.

Editor's note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the security area.

5.2.4.21.2 Solution details

The solution consists in using an authentication protocol with UE authentication confirmation, e.g. EAP-AKA' or EPS AKA* (cf. solution #2.22), and link it to a Next Generation Update Location Request (NG-ULR). This can be done e.g. in the following way:

- The home network records the time of most recent successful authentication of the subscriber together with the identity of the NG visited network that was involved in the authentication. When a new NG-ULR arrives from a visited network the home network checks whether there is a sufficiently recent authentication of the subscriber by this visited network. If not the NG-ULR is rejected. The rejection message may include, according to the home networks policy, an indication that the visited network should send a new NG Authentication Information Request for fetching new authentication vectors before repeating the NG-ULR.

NOTE1: With this approach, the authentication procedure and the NG-ULR procedure are performed independently. They are coupled only through linking information in the home network. This is similar to the flows in EPS.

NOTE2: It is up to the home network to set a time threshold for defining what 'sufficiently recent' is.

- A variant of the above approach would be based on a more fine-grained policy applied by the home network: the home network could classify roaming partners into different categories, depending on the trust - e.g. derived from previous experience- placed in them, for example as follows:
    - For a visited network in the first category, the home network would require a successful authentication 'immediately preceding' the NG-ULR.
    - For a visited network in the second category, the home network would only check that an authentication in a network visited by the subscriber was sufficiently recent (taking into account that there may have been a security context transfer between the visited networks)
    - For a visited network in the third category, the home network would perform no checks regarding NG-ULRs and authentication at all.

Editor's Note: The procedures described in this solution need to be agreed together with CT4.

Lenovo Ex. 1007
Page 232

Editor's Note: It is ffs whether the use of any such measures taken in the home network are to be mandated, or whether they should be left to the operator as they do not affect interoperability. But the measures should be described.

NOTE3: An authentication protocol in itself does not provide a solution for key issue #2.11, even if it provides UE authentication confirmation to the home network, as e.g. EAP-AKA' or EPS AKA* do. The authentication result needs to be linked to the location update procedure somehow to achieve the desired solution.

5.2.4.21.3 Evaluation

tba

5.2.4.22 Solution #2.22: EPS AKA with UE authentication confirmation

5.2.4.22.1 Introduction

This solution addresses key issue #2.11.

Editor's note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the security area.

5.2.4.22.2 Solution details

The present solution enhances EPS AKA with providing an Authentication Confirmation message from the visited network to the home network that confirms successful authentication of the UE such that the message cannot be spoofed by the visited network with a reasonable probability. The solution leaves the authentication exchange between the UE and the visited network unchanged, compared to using EPS AKA in 5G, as e.g. described in solution 2.7. In particular, the solution does not affect the authentication behaviour of the UE, compared to EPS AKA.

The present solution is called EPS AKA*.

NOTE1: It was purposely avoided calling the new solution EPS AKA' as this would have suggested a wrong analogy between EAP-AKA and EPS AKA on the one hand and EAP-AKA' and the new EPS AKA' on the other. But the main difference between EAP-AKA and EAP-AKA' is that the latter provides serving network authentication while the former does not. However, EPS AKA already provides serving network authentication, too.

In the following, the agreed terminology for authentication-related functions from clause 5.2.1.2 of the present TR is used.

EPS AKA* works as follows:

The SEAF in the visited network requests a new authentication vector by sending a Next Gen Authentication Information Request (NG-AIR) to the AUSF in the home network.

The AUSF translates the NG-AIR into a request to the ARPF. The ARPF generates the authentication vector in the same way as for EPS AKA in TS 33.401 and returns it to the AUSF. Only one authentication vector shall be returned in response to an NG-AIR.

NOTE2: Returning only one authentication vector at a time is already recommended in EPS.

The AUSF splits the parameter XRES into two equal parts XRES1 and XRES2 (e.g. by choosing XRES1 to be the n least significant bits of XRES where 2n is the length of XRES). The assumption is made here that the knowledge of XRES1 does not help in guessing XRES2.

NOTE3: This assumption is believed to be fulfilled when the expected authentication response XRES is pseudo-randomly generated, e.g. as in MILENAGE or TUAK.

The AUSF stores XRES temporarily until a protocol timer expires.

Editor's Note: The protocol timer is to be defined by CT4.

Lenovo Ex. 1007
Page 233

The AUSF then returns an authentication vector AV* in a Next Gen Authentication Information Answer (NG-AIA). The only difference between AV* and an authentication vector AV, as described for EPS AKA in TS 33.401, is that AV* contains only XRES1 while AV contains the full XRES.

The SEAF understands from the NG-AIA that it includes AV*, not AV.

The SEAF sends RAND, AUTN to the UE. The UE returns RES, as described for EPS AKA in TS 33.401.

The SEAF splits RES into RES1 and RES2 in the same way as the AUSF did and compares RES1 with XRES1. If they coincide the SEAF considers the authentication successful. If not the SEAF rejects the authentication.

If the authentication was successful, the SEAF sends RES, as received from the UE, in a newly defined Next Gen Authentication Confirmation (NG-AC) message (containing identifications of the subscriber and the visited network) to the AUSF.

When the NG-AC message was received in response to an NG-AIA and was received in time (cf. protocol timer above) the AUSF compares the received RES with the stored XRES. If they coincide the AUSF considers the authentication successful and records the event, together with the time, the identity of the visited network and the subscriber identity, in a database of successful authentications.

NOTE4: Solution #2.21 explains how EPS AKA* can be used to address key issue #2.11.

Editor's Note: The extent to which the reaction of the AUSF needs to be standardised is ffs.

Editor's Note: It is ffs whether the SEAF should also report failed authentications. The feature "Authentication failure report" was available in 3G, cf. TS 33.102, clause 6.3.6, but was abandoned in 4G as it was not found useful.

5.2.4.22.3 Evaluation

Security:

1) *Probability of spoofing the response*:
Assume that an SEAF wants to spoof RES in the absence of the subscriber. (This is the first threat described in key issue #2.11.) The SEAF has obtained XRES1 from the AUSF, but needs to guess RES2. In EPS AKA, RES has a minimum length of 32 bits. (For the commonly used authentication algorithm set MILENAGE, the length of RES is 64 bits.) So, RES2 has a minimum length of 16 bits. This means that the SEAF has a chance of at most 1 in 2^16 =65.000 to guess RES2 correctly.

This success probability for a fraudulent SEAF is considered sufficiently low for the following reasons:

- A chance of at most 1 in 65.000 (1 in 4 billion for MILENAGE) is considered commercially unattractive.
- It would be highly suspicious to the home network if the visited network reported a high number of authentications as successful that the home network found incorrect. (The home network could, e.g., compare the corresponding figures among various networks to obtain heuristical values.)

2) *RES1 correct, but RES2 incorrect*
It can happen that the UE sends an incorrect RES where, however, the RES1 part is correct. The SEAF would then see the authentication as successful, but, when the UE was indeed not the one it claimed to be, the UE would not be able to compute (the NG equivalent of) K_{ASME} correctly, and the SEAF would notice the failure when trying to take (the NG equivalent of) K_{ASME} into use in the NG Security Mode procedure. The probability for a false UE to guess RES1 correctly is determined by the length of RES1 and is considered sufficiently low, cf. 1), for any practical purposes. If the UE did send the correct RES, but RES2 was corrupted over the air interface, while RES1 was not, the SEAF would indeed go ahead in serving the UE (rightfully so), but the AUSF would not record this as a successful authentication, which may result in an additional authentication requested by the home network. This is not believed to do much harm as corruption of a correct RES over the air should be a rare event.

3) *Impersonating an MME towards the home network*
Assume the SEAF presented itself as an MME to the home network. (This case is included for completeness, it is not clear if this was ever possible protocol-wise.) Then the home network would issue authentication vectors AV for EPS AKA, which include the full RES. However, the AUSF would not expect any Next Gen Authentication Confirmation message and would not record any successful authentications. So, this would not help the SEAF when the home

Lenovo Ex. 1007
Page 234

network would consequently link an NG Update Location request with recent successful authentications (as described in solution 2.21).

4) *Impersonating an MME towards the UE*
Assume that the SEAF correctly presents itself to the AUSF to obtain authentication vectors AV* for EPS AKA*. The SEAF would then present itself to the UE as an MME. Even if this was possible protocol-wise, it would not make any difference from a security point of view as the UE behaviour is the same for EPS AKA and EPS AKA*. In any case, the AUSF gets the guarantee, by receiving the Next Gen Authentication Confirmation message, that the SEAF had a recent successful authentication exchange with the UE (through whatever intermediate entities).

5) Key issued to SEAF before AUSF knows about UE authentication success
The security guarantees given to the home network by EPS AKA* are still lower than those given by EAP-AKA'. The difference lies in the point of time the intermediate key (which is K_{ASME} in EPS AKA* and MSK in EAP-AKA') is given to the SEAF: for EPS AKA*, the intermediate key is issued by the AUSF before authentication success is known, for EAP-AKA' this happens only afterwards.

The question is in how much this difference in security guarantees matters in practical terms.

At the time the authentication vector is sent, the home network has had the chance to check that the visiting network is authorized to serve the subscriber. So, when the subscriber is actually present at this time, everything is fine.

When the subscriber is not present in the visited network, the SEAF cannot generate a correct Authentication Confirmation message, but it has already received K_{ASME}. What attacks could a fraudulent SEAF mount in this case?

- The SEAF could wait until the subscriber finally arrives in the visited network and could then use the key K_{ASME}. This would constitute an attack only if the authorization to serve the subscriber had expired in the meantime. But such authorizations are believed to be quite long-term. Furthermore, sitting and waiting for a subscriber to stumble into the visited network does not seem a very effective attack strategy.

- So, the SEAF would have to pursue a more active strategy by following the subscriber around with a network-in-a-box piece of equipment and entice the subscriber to attach to this equipment. This would be possible, in principle, but it would probably require some IP connectivity from the network-in-a-box to provide Internet access for the subscriber. The attacker could mount the attack any time after receiving the key K_{ASME}, but only as long as the sequence number in the authentication challenge remains fresh from a UE point of view. The more authentications the UE successfully performs in other networks, the sooner the sequence number will become stale.

- An online variant of the attack in the previous bullet seems also possible with EAP-AKA': if the network-in-a-box had an IP connection to the real visited network, the network-in-a-box could transparently forward EAP authentication messages between the UE and the SEAF in the real visited network via the network-in-a-box, and the SEAF would then communicate with the AUSF in the home network as usual. A difference to the attack scenario in the previous bullet is that the attachment of the UE to the network-in-a-box would have to happen at the time of the EAP authentication exchange with the AUSF in the home network, and not at any time later. This difference does not seem a major obstacle, though, when IP connectivity from the network-in-a-box has been established, as the authentication would be initiated by the network-in-a-box via the SEAF towards the AUSF.

Furthermore, the second threat described in key issue #2.11 (correct authentication of UE, followed by detach and overbilling) could not be thwarted by the use of EAP-AKA' either.

Efficiency:

1) Authentication delay
The efficiency advantage of EPS AKA over EAP-AKA' is inherited by EPS AKA* as far as authentication delay over the air interface is concerned: The SEAF can go ahead with the NG Security Mode procedure etc. without having to wait for a second roundtrip of authentication with the AUSF. This is particularly useful in full authentications that do not entail an Update Location procedure or any further interaction with the home network.

2) Computation overhead
Computation overhead of EPS AKA* is also the same as for EPS AKA and lower than for EAP-AKA'. This may be an advantage for UEs with restricted capabilities.

3) Statelessness
The AUSF is no longer stateless as in EPS AKA. It becomes stateful as in EAP-AKA'. This does not necessarily imply,

Lenovo Ex. 1007
Page 235

however, that the effort for the AUSF for keeping protocol state would be the same for both EPS AKA* and EAP-AKA', as shown in the following:

Solution 2.21 on "Linking update location with authentication confirmation" explains that authentication confirmation may not be required for every authentication run. Rather, a more fine-grained policy could be applied by the home network where an authentication confirmation for an authentication vector sent to the visited network is requested only when the visited network is not fully trusted. But the traffic generated passing through such visited networks is expected to be only a small fraction of the total traffic because

- Most of the traffic is non-roaming traffic
- Most of the roaming partners will be fully trusted (e.g. local subsidiaries of a global MNO, major operator).

This then implies that the AUSF has to act in a stateful way only for a small fraction of the total number of authentication runs. Hence, the additional effort required of the AUSF for keeping state should be generally small in the case of EPS AKA*, while, for EAP-AKA' statefulness is required for every authentication run.*Overview of evaluation of EPS AKA**Supporting both EAP-AKA' and EPS AKA / EPS AKA* in the unified way described in solution 2.7, is justified by reasons including the following

- 5G NR access is likely to carry much more traffic than non-3GPP access, so efficiency considerations matter.
- EPS AKA is more efficient than EAP-AKA or EAP-AKA' in terms of roundtrips, computation and load on the AUSF / HSS.
- EPS AKA* provides increased home control, but the home operator can decide, for which roaming partners increased home control is needed.
- As the part of the traffic requiring increased home control due to an increased risk of roaming fraud is expected to be quite small this means that most of the authentication traffic can enjoy the full efficiency advantages of EPS AKA, while protection against roaming fraud is still provided.
- Providing support for EPS AKA and EPS AKA* allows a smooth transition for operators from its current base towards 5G.
- The key issue requirements contain "EPS AKA shall be supported for accessing to LTE network either during initial access or via mobility events".
- The functionality required in the UE is the same for EPS AKA and EPS AKA*.

5.2.4.23 Solution #2.23: Equipment Identifier Authentication using Identity-based Authentication

5.2.4.23.1 Introduction

This solution addresses Key issue #2.4: Equipment Identifier authentication. Similar to solution #2.10, during the manufacturing process, the device is securely provisioned with a private key; however, the private key is directly associated with the Equipment Identifier under an identity-based cryptosystem.

There is no need for any device certificates or device manufacturer Certificate Authority (CA) in this solution.

5.2.4.23.2 Solution details

The device manufacture provisions UEs with a set of credentials for Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI), as defined in IETF RFC 6507 [33]. Each UE requires a Public Validation Token (PVT) and corresponding Secret Signing Key (SSK) associated with its identity (e.g. the IMEI).

For each batch of devices, the device manufacture generates a KMS Secret Authentication Key (KSAK), and the corresponding public root of trust KMS Public Authentication Key (KPAK). The device manufacturer publishes the KPAK in a secure way so that network operators can easily determine the correct KPAK for any given IMEI (for example, the device manufacturer may publish a list of KPAKs via a secure web-site, or may sign a list of KPAKs using a conventional public key signature solution). It is up to the device manufacturer how often to change the KSAK/KPAK, but regular changes will limit the damage caused by key compromise.

Lenovo Ex. 1007
Page 236

The high level authentication flow at first attachment of the equipment to a mobile network is very similar to Figure 5.2.4.10.2-1 – however, it is simplified because there is no need for a device certificate to be presented in step 4. The network operator must instead install a list of known KPAKs into its AUSF (or ARPF).

As described in 5.2.4.10.2.2, the operator (or service provider) can also enrol the UE for a conventional certificate, using a CA owned or trusted by the operator or service provider – this removes a potential long-term dependency on the device manufacturer's KSAK/KPAK. Alternatively, the operator or service provider can ask the UE to generate a new public-private keypair, sign the public key using the identity-based private key, and then provide the signed public key to the operator/service provider, to store in an operator directory. (This could avoid some costs of an operator CA).

5.2.4.23.3 Evaluation

This solution addresses Key issue #2.4: Equipment Identifier authentication, but with lower overheads in certificate management (as there is no need for each device manufacturer to operate a CA). Further, a common objection to identity-based cryptography is that the KMS knows each private key in the system.

Long-term dependency on a manufacturer secret can be avoided by regular changes in the KSAK/KPAK, and by operators enrolling devices into their own PKI (or other directory of signed public keys).

Editor's note: the overhead of key revocation and key lifetime management need to be taken into account.

5.2.4.24 Solution #2.24: Combining solutions 2.2 and 10.2

5.2.4.24.1 Introduction

This solution addresses key issues 2.2 and 3.1. It consists in a combination of solutions 2.2 and 10.2. Solution 2.2 helps against purely passive attacks that use a leaked permanent subscriber key. Solution 10.2 helps against the interception of keys sent between operator entities.

5.2.4.24.2 Solution details

It is assumed for the present solution, as for solution 10.2, that the serving network possesses a private-public key pair, and the home network knows the public key.

Solution #2.2 adds a Diffie-Hellma key exchange to the key establishment over the radio interface. Solution #10.2 consists in encrypting keys in authentication vectors or security contexts transmitted between core network entities using the public key of the receiving entity. The present solution consists in applying solution #10.2 in addition to solution #2.2. In this way, also active attacks trying to impersonate the serving network can be mitigated.

5.2.4.24.3 Evaluation

See also evaluation of solution #2.6.

5.2.4.25 Solution #2.25: Authentication Procedure for un-trusted non-3GPP access

5.2.4.25.1 Introduction

This solution address KI #2.1 about non-3GPP RAT access.

5.2.4.25.2 Solution details

The call flow in Figure 5.2.4.25.2-1 describes Attach procedure via WLAN access to a NextGen core with the difference with the flow depicted in Figur 5.2.4.25.2-1:

- NAS message is carried directly as IKEv2 parameters (e.g. inside 3GPP-specific IKEv2 Configuration Payloads).

Lenovo Ex. 1007
Page 237

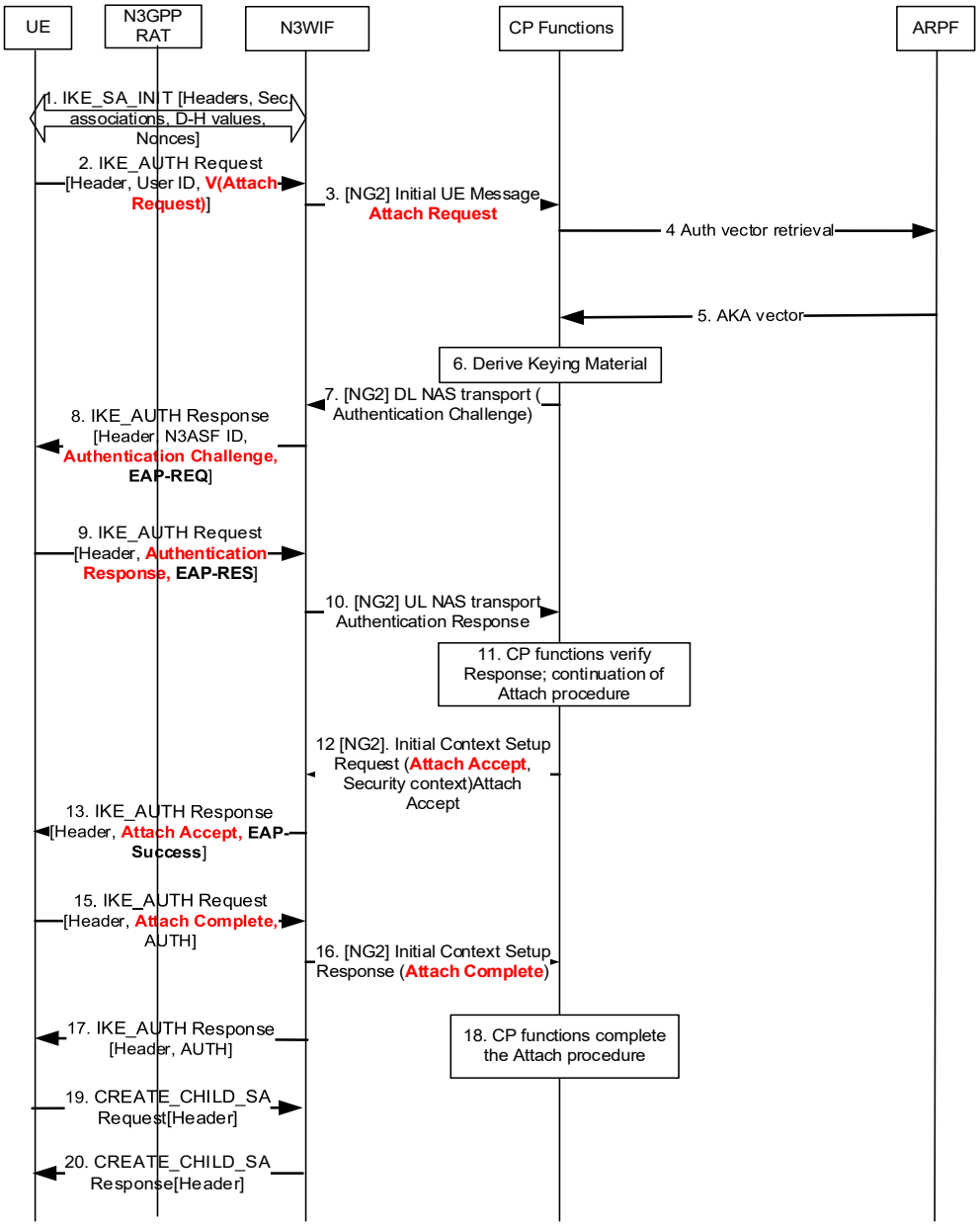


Figure 5.2.4.25.2-1: Example of Attach procedure

The call flow is self-explanatory with the following exception:

Step7. CP Functions may decide to use EAP authentication method. In this case, the content of Authentication Challenge message could be EAP-REQ.

Step8. If EAP method is used, N3WIF forwards the EAP payload to the UE within IKEv2 message. Otherwise, e.g. if traditional AKA is used, Authentication Challenge is carried directly as IKEv2 parameters.

Step19. CREATE_CHILD_SA Request is sent to the N3WIF to create a second Child SA to transport user plane data.

Step20. N3WIF responds with CREATE_CHILD_SA Response.

NOTE: The diagram flow does not represent the separation and interaction in NFs involved in Authentication.

Depicted in Figure 5.2.4.z.2-2 is NG1 protocol stack during the Attach procedure when NAS messages is carried directly as IKEv2 parameters.

Lenovo Ex. 1007
Page 238

Editor's Note: It is FFS how does UE find the home network and the N3IWF function.

Editor's Note: It is FFS when the UE initiates the IPSec connectivity to the NG Core through the non-3GPP access.

Editor's Note: It is FFS how to handle error cases.

Editor's Note: It is FFS how NAS security is addressed

Editor's Note: It is ffs if changes are required in the call flow to meet RFC 7296 requirements for using Configuration Payload in IKEv2 messages.

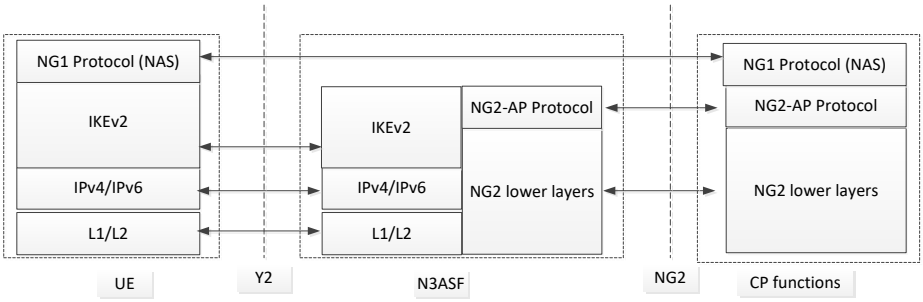


Figure5.2.4.25.2-2: NG1 Protocol stack during Attach procedure

Once the Attach procedure is complete, the NG1 messages for subsequent SM procedures are expected to be the same as for 3GPP access.

5.2.4.25.3 Evaluation

5.2.4.26 Solution #2.26: EAP based secondary authentication by an external DN-AAA server

Editor Notes: The three optional EAP based secondary authentication solutions need to be merged by next SA3 meeting.

Editor Notes: Credentials used for secondary authentication shall be different from primary authentication.

5.2.4.26.1 Introduction

This solution addresses key issue #2.1 Authentication framework which provides support for optional-to-use secondary authentication between the UE and an external data network (DN) possibly run by a 3rd party.

In the solution, EAP is used for authentication between the UE and AAA server in the external data network. The SMF acts as the EAP Authenticator and Diameter client to the DN-AAA server.

Between the UE and the SMF, EAP messages are sent in the SM NAS message. Standard EAP routing rules based on the realm of the received EAP Identity (in the form of NAI) is used to forward EAP messages to the DN-AAA server.

AUSF may take on an additional role of a transparent proxy AAA. In such a scenario, AUSF may be used to route AAA messages between SMF and an external DN-AAA.

Figure 5.2.4.26.2-1 shows a possible flow where this SMF based secondary authentication is run with an external AAA server.

5.2.4.26.2 Solution details

The following figure depicts the general information flow for the present solution.

Lenovo Ex. 1007
Page 239

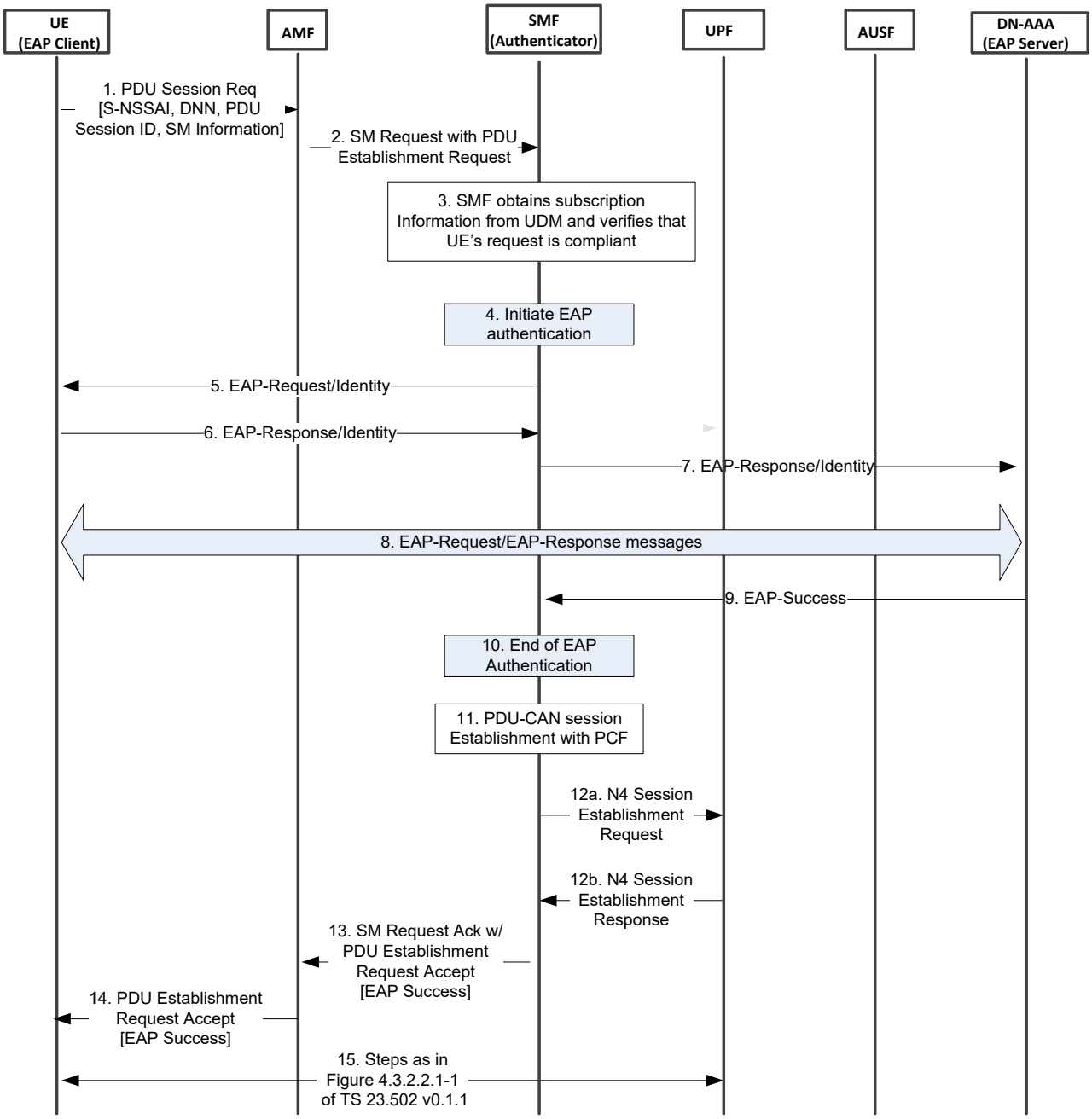


Figure 5.2.4.26.2-1 EAP Authentication with an external AAA server

1. The UE initiates a new PDU Session Establishment procedure by sending a SM NAS message containing a PDU Session Establishment Request within the SM Information field.

The PDU Session Establishment Request includes the service it would like to obtain (S-NSSAI) and the PDN it would like to connect to (DNN).

2. The AMF selects an SMF and sends a "SM Request" message with SM NAS as one of its payload. It also forwards the Permanent User ID and the received S-NSSAI, DNN.

3. The SMF obtains subscription data from UDM for the given Permanent User ID obtained from AMF in step 2. The SMF checks whether the UE request is compliant with the user subscription and with local policies. If not, the SMF will reject UE's request via SM-NAS signaling and skip rest of the procedure.

4. The SMF triggers EAP Authentication.

5. The SMF sends an EAP Request/Identity to the UE.

Lenovo Ex. 1007
Page 240

6. The UE sends an EAP Response/Identity message. The UE shall send its DN-specific identity complying with Network Access Identifier (NAI) format.

7. The message is routed to the DN AAA Server based on the realm part of the UE identity obtained in step 5. The routing path may include AUSF acting as the proxy AAA.

Editor Notes: Protection of the SMF from external access, and routing of EAP messages between SMF and the external network is FFS

8. The DN AAA server and the UE exchange EAP messages as required by the EAP method. This EAP signalling is sent between the UE and the SMF over NAS.

9. After the completion of the authentication procedure, DN AAA server sends EAP Success message to the SMF.

10. This completes the authentication procedure at the SMF.

11. The SMF may initiate PDU-CAN Session Establishment with the PCF to get the default PCC Rules for the PDU Session.

12a-12b. The SMF sends an N4 Session Establishment Request to the UPF as in step 8.a and 8.b of Fig 4.3.2.2.1-1 in TS 23.501 v0.1.1.

13. The SMF sends "SM Request Ack" to AMF as in step 9 of Fig. 4.3.2.2.1-1 in TS 23.501 v0.1.1. This message includes EAP Success to be sent to the UE within the NAS SM "PDU session establishment accept".

14. The AMF forwards NAS SM "PDU session establishment accept" that contains the EAP Success to the UE as described in step 10 and step 11 of Figure 4.3.2.2.1-1 in TS 23.501 v0.1.1.

15. The UE-requested PDU Session Establishment proceeds further as in steps of Figure 4.3.2.2.1-1 in TS 23.501 v0.1.1.

In case of a Home Routed deployment, it is the SMF in the HPLMN that takes the role of the authenticator.

5.2.4.26.3 Evaluation

FFS

5.2.4.27 Solution #2.27: EAP-based solution for secondary authentication, authorization and UP protection

Editor Notes: The three optional EAP based secondary authentication solutions need to be merged by next SA3 meeting.

Editor Notes: Credentials used for secondary authentication shall be different from primary authentication.

5.2.4.27.1 Introduction

This solution addresses KI #1.15, KI #2.10, KI #6.1, KI #6.3 and KI #8.3.

5.2.4.27.2 Solution details

5.2.4.27.2.1 Overall procedure

Figure 5.2.4.27.2.1-1 illustrates the flow of messages involving both a primary and a secondary authentication.

Lenovo Ex. 1007
Page 241

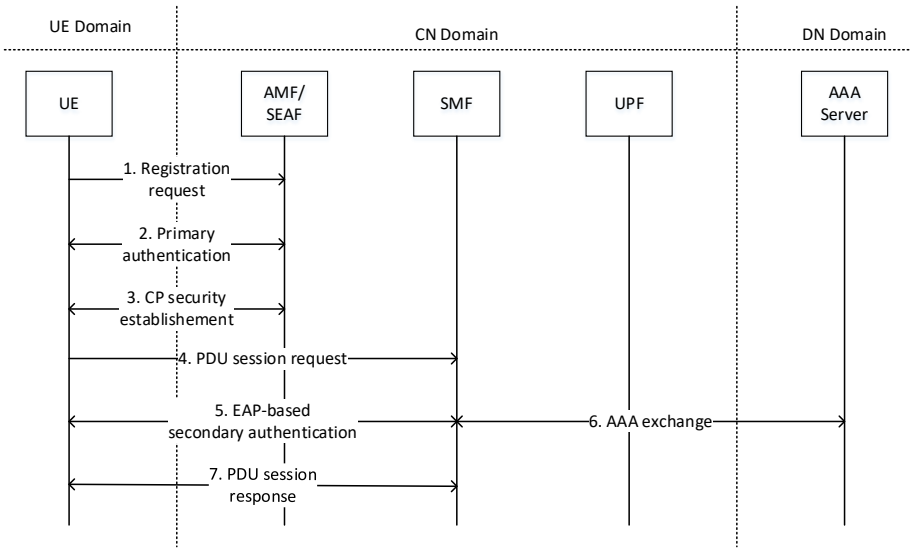


Figure 5.2.4.27.2.1-2: Message flow of the secondary authentication

1. The UE sends a registration request.
2. The primary authentication procedure is executed between the UE and the SEAF. Upon successful authentication the next steps are executed.
3. The NAS Security is set up. From now on all NAS messages are confidentiality and integrity protected.
4. The SMF receives a PDU session request
5. 6. The secondary authentication procedure is performed between the UE and the SMF. The EAP messages are transported over the NAS protocol. The EAP exchange over the air interface benefits from the protection at the NAS layer.
7. The SMF sends back a PDU session response depending on the outcome of the previous authentication steps.

In steps 4 and 5 the SMF endorses the role of the EAP authenticator and relies on a backend AAA server in the data network possibly in another security domain, e.g. controlled by a 3rd party. Then it is left open how the AAA messages are transported transparently over NG4-NG6 interfaces through the UPF. The UPF could endorse the role of a AAA proxy or even simpler, an IP router.

Figure 5.2.4.27.2.1-2 shows the protocol architecture for the support of the EAP based secondary authentication.

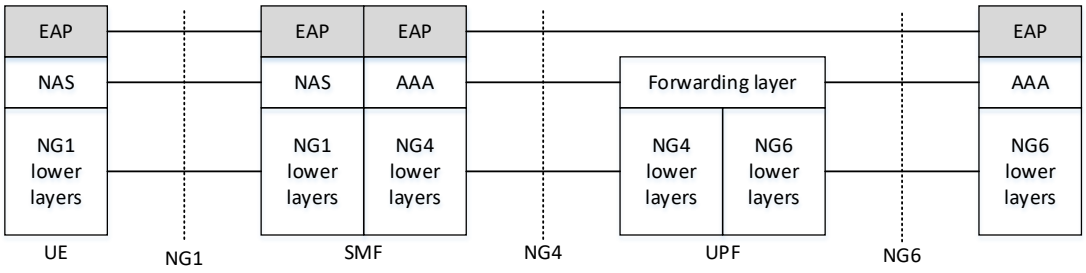


Figure 5.2.4.27.2.1-2: Protocol architecture for secondary authentication

Simlarly to the PCO based mechanism, the secondary authentication could be used for an additional authorization controlled by an external party upon the UE's request for the establishment of specific or additional PDU sessions. Other use cases related to the UP protection and slicing are described in the following clauses.

5.2.4.27.2.3 Support of Network Slicing

The secondary authentication could be used for Network Slice specific authorization. In fact, upon successful primary authentication via a certain AMF, the UE could potentially be provided services via all the Network Slices served by that particular AMF. It could be the case that the UE is automatically authorized to access all or some of the slices based

Lenovo Ex. 1007
Page 242

on subscriptions information. Alternatively, the authorization could be enforced on a slice specific basis using the secondary authentication during the creation of a PDU session for a particular slice.

For the protection of the UP traffic between the UE and a particular slice, the mechanism described in the previous clause could be used. However, the configuration of the slices in the sense of who manages or owns which network function becomes relevant. From a trust model perspective, this would require that the UPF and SMF are slice specific otherwise the protection would not serve any purpose.

5.2.4.28 Solution # 2.28: secondary authentication and authorization using SM NAS signalling

Editor Notes: The three optional EAP based secondary authentication solutions need to be merged by next SA3 meeting.

Editor Notes: Credentials used for secondary authentication shall be different from primary authentication.

5.2.4.28.1 Introduction

This solution addresses KI #2.10 and KI #6.1.

5.2.4.28.2 Solution details

This solution is presented based on the architecture described in the Figure 5.1.4.6.2.1-3: Architecture for authentication framework in non-roaming scenario with secondary authentication with a service provider. The secondary authentication is performed using SM NAS signalling that is exchanged between an NG-UE and an SMF via protected MM NAS signalling.

To enable the secondary authentication over the control plane, the SMF directly interfaces with the 3rd party AAA server and supports EAP authentication, playing the role of EAP authenticator.

NOTE 1: The SMF does not establish a PDU session for the UE until the authentication is successful.

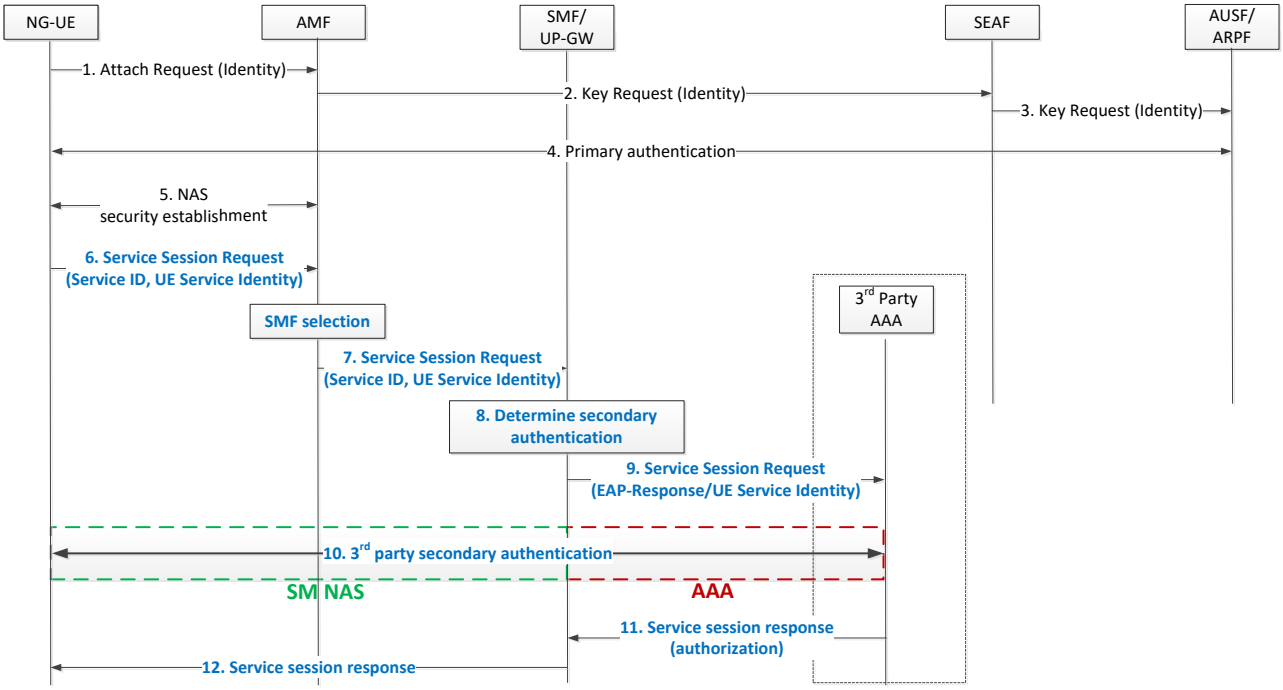


Figure 5.2.4.28.2. Secondary authentication over the control plane

1-5. The NG-UE attaches to the network performing primary authentication with AUSF/ARPF based on the network access credentials (e.g., AKA credentials) and establishes a NAS security context with AMF.

6. The NG-UE sends a service (PDU) session request for a 3rd party service to the AMF using a protected NAS MM message. The PDU session request includes the service identity of the NG-UE.

Lenovo Ex. 1007
Page 243

7. The AMF determines an SMF based on the service type or service identity provided by the NG-UE and forwards the PDU session request to the SMF.

NOTE 1: The SMF may optionally establish a SM NAS security context with the NG-UE. If SM NAS security is required, it is established at this point.

Editor's note: it is FFS whether a separate NAS SM security is needed.

8. The SMF determines whether the NG-UE is allowed to establish a PDU session for the service based on the subscription profile and whether a secondary authentication with 3rd party AAA server is required.

9. The SMF initiates EAP authentication by sending an Authentication Request message to the 3rd party AAA server. The request is a AAA message carrying EAP-Response/Service Identity.

10. Besed on the received UE Service Identity, the AAA determines the EAP method. The NG-UE and the 3rd party AAA perform EAP authentication over the control plane (i.e., using SM NAS signalling) with SMF playing the role of EAP authenticator.

NOTE 2: The supported mandatory EAP methods may be defined. EAP already natively supports PAP/CHAP.

11. If the EAP authentication is successful, the 3rd party AAA sends a service session response, including EAP success message to the SMF. The service session response is an AAA message that authorizes the requested PDU service session creation by the SMF.

NOTE 3: If the SMF determines (e.g., based on policy) that UP security termination at UPF is needed for the session, K_{UPF} may be provided to the SMF in this step.

12. The SMF sends a service session response that includes the PDU session information required to complete the PDU session creation to the NG-UE.

5.2.4.28.3 Evaluation

5.2.4.29 Solution #2.29: Equipment identifier authentication using EAP

5.2.4.29.1 Introduction

This solution addresses the key issue #2.4 "Equipment identifier authentication".

It refers in the key issue #2.4 that "*IMEI reported by the UE to network is not authenticated. Therefore, the network cannot place any trust on the reported IMEI of the UE*", and therefore the requirement that "*it should be possible for the network to authenticate the reported identifier of the device*" was added in the key issue.

5.2.4.29.2 Solution details

Assuming the equipment identifier (e.g. IMEI) in conjunction with its credential (e.g. certificate, shared key etc.) as supplied by the equipment manufacturer is provisioned in a secure location (e.g. ARPF) in the network side, this solution proposes a method to verify whether the identifier is genuine during equipment identifier authentication. The specific authentication method is based on EAP, which is beyond the scope of this solution. The AUSF and ARPF used for equipment identifier authentication may be collocated or separated as different network elements. They also can be third party network elements. Figure 5.2.4.29.2-1 shows the procedure of equipment identifier authentication.

Lenovo Ex. 1007
Page 244

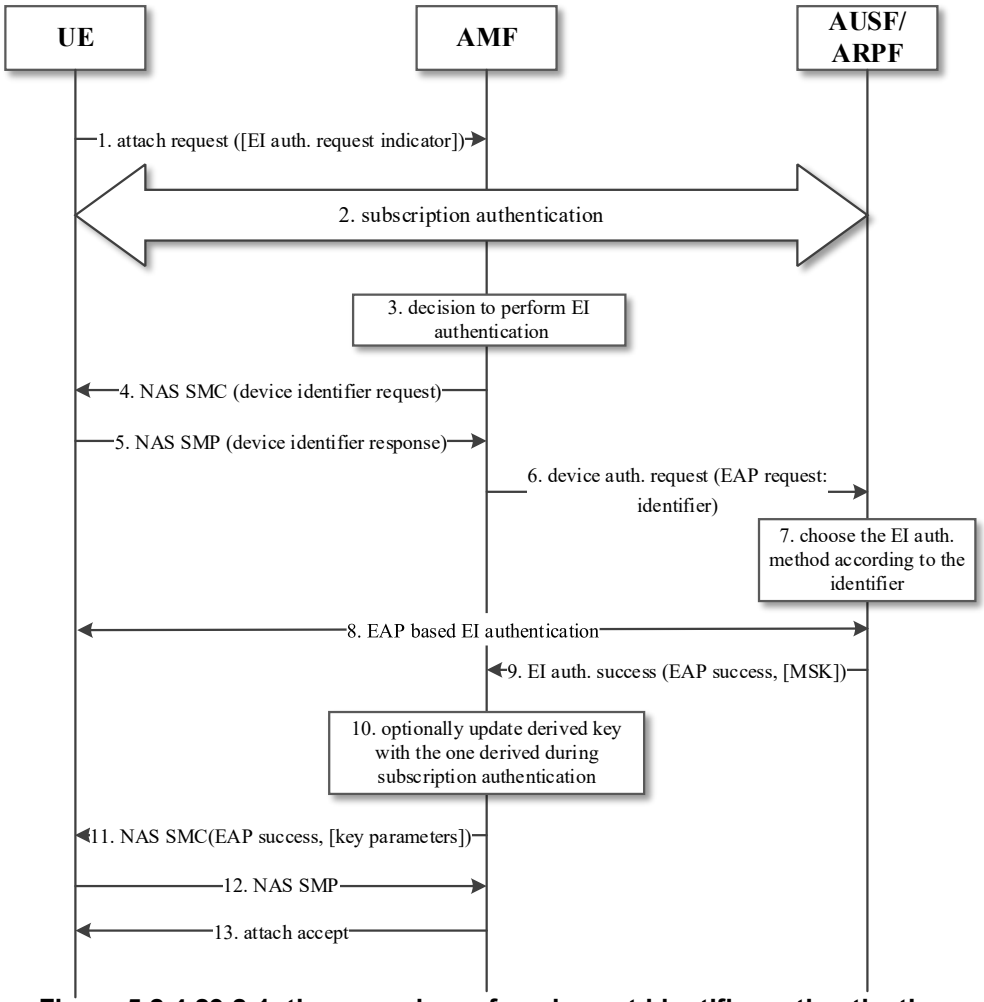


Figure 5.2.4.29.2-1: the procedure of equipment identifier authentication

1. UE sends an attach request to AMF in which contains an optional equipment identifier authentication indicator.

2. UE and the network perform the mutual authentication.

3. AMF decides whether perform the equipment identifier authentication to the UE according to the requirement of the operator or the subscription of UE.

4. AMF sends the equipment identifier request via NAS SMC to UE.

5. UE responds its identifier in NAS SMP to the AMF.

6. AMF sends the equipment identifier authentication request including UE's identifier to AUSF/ARPF. AUSF/ARPF in this step can be different with AUSF/ARPF in step 2 for subscription authentication.

7. AUSF/ARPF chooses the authentication method for UE according to the identifier.

8. The procedure of EAP based authentication between UE and AUSF/ARPF. The number of EAP message exchanges between the UE and the AUSF/ARPF depends upon the EAP Method AUSF/ARPF chooses.

9. AUSF/ARPF sends the equipment identifier authentication success message to the AMF which optionally contains an MSK.

10. AMF optionally updates the key derived during the equipment identifier authentication with the one derived during the subscription authentication if the network wants to refresh the security context by binding it with the equipment identifier authentication credentials.

11. AMF sends NAS SMC to the UE which contains EAP success message and key parameters to derive new keys if the key is updated by AMF.

Lenovo Ex. 1007
Page 245

12. UE responds with NAS SMP message.

13. AMF sends attach accept message to finish the attach procedure.

5.2.4.29.3 Solution evaluation

Tba

5.2.4.30 Solution #2.30: EAP based secondary authentication by an external DN-AAA server

5.2.4.30.1 Introduction

This solution addresses key issues #2.10, #6.1, #6.3 and #8.3.

The solution provides support for optional-to-use secondary authentication between the UE and an external data network (DN). It is based on the UE requested PDU Session Establishment procedure in clause 4.3.2.2 in TS 23.502 [83] and expands on the PDU session establishment authentication/authorization call flow in clause 4.3.2.3 in TS 23.502[83].

EAP is used for authentication between the UE and a DN-AAA server in the external data network. The SMF endorses the role of the EAP Authenticator and relies on an external DN-AAA server to authenticate and authorize the UE request for the establishment of a PDU sessions.

Between the UE and the SMF, EAP messages are sent in the SM NAS message. The SMF communicates with the external DN-AAA transparently via the UPF. For example, standard EAP routing rules based on the realm of the received EAP Identity (in the form of NAI) could be used in UPF to forward EAP messages to the DN-AAA server.

Figure 5.2.4.30.2-1 shows a possible flow where this SMF based secondary authentication is run with an external AAA server.

5.2.4.30.2 Solution details

The following figure depicts the general information flow for the present solution.

Lenovo Ex. 1007
Page 246

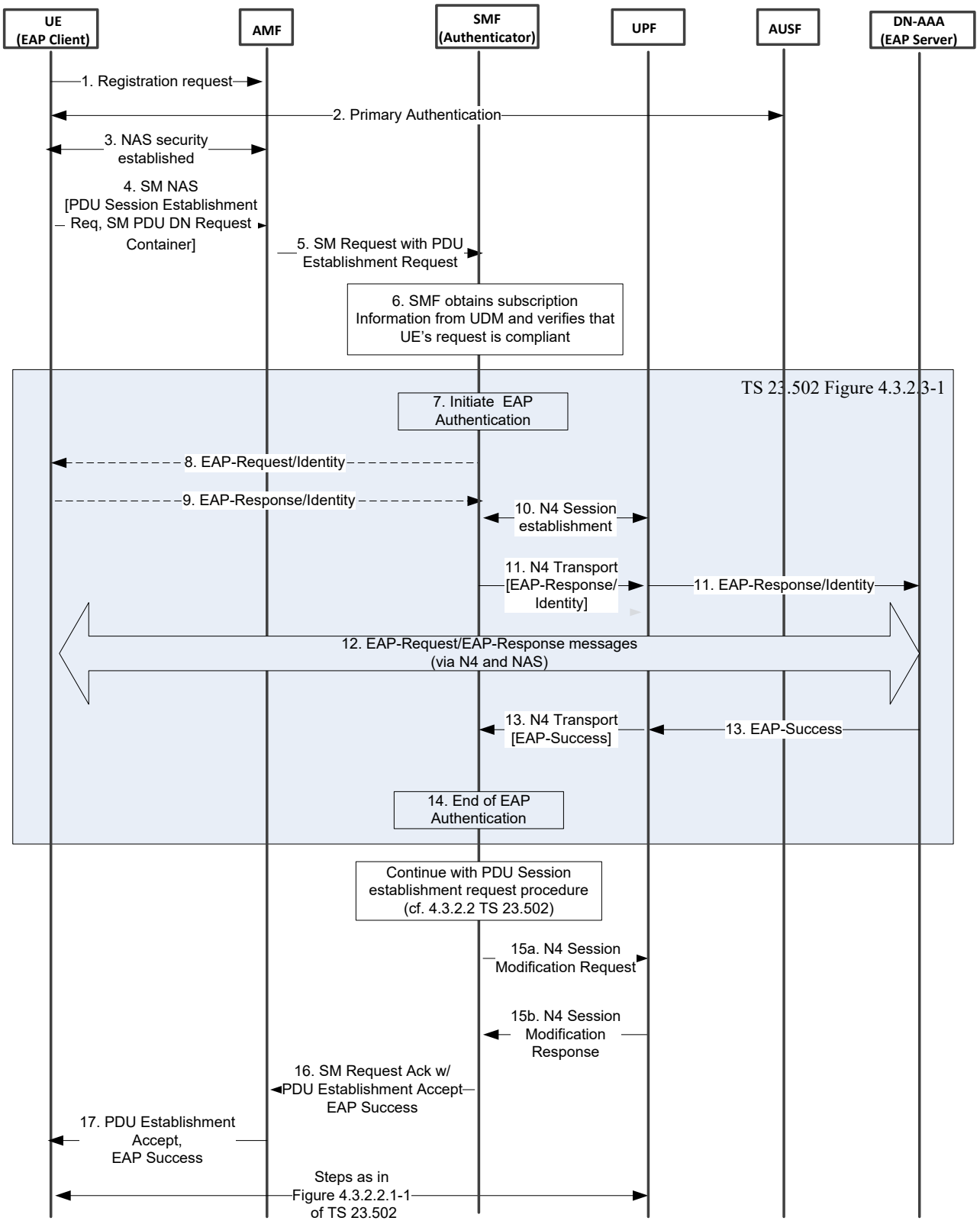


Figure 5.2.4.30.2-1 EAP Authentication with an external AAA server

1-3 The NG-UE registers with the network performing primary authentication with AUSF/ARPF based on the network access credentials (e.g. AKA credentials) and establishes a NAS security context with AMF.

4. The UE initiates establishment of a new PDU Session by sending a SM NAS message containing a PDU Session Establishment Request. The NAS message may also contain SM PDU DN Request Container containing information for the PDU session authorization by the external DN.

Lenovo Ex. 1007
Page 247

The UE includes the service it would like to obtain (i.e. S-NSSAI) and the PDN it would like to connect to (i.e. DNN).

5. The AMF selects an SMF and sends a "SM Request" message with SM NAS as one of its payload. It also forwards the Permanent User ID and the received S-NSSAI, DNN.

6. The SMF obtains subscription data from UDM for the given Permanent User ID obtained from AMF in step 5. The SMF checks whether the UE request is compliant with the user subscription and with local policies. If not, the SMF will reject UE's request via SM-NAS signaling and skip rest of the procedure.

7. The SMF triggers EAP Authentication to obtain authorization from an external DN-AAA server.

NOTE: Clause 4.3.2.3 in TS 23.502 [83] describes the transport mechanism for delivery of EAP messages between the UE and the external AAA server.

8. The SMF sends an EAP Request/Identity to the UE.

9. The UE sends an EAP Response/Identity message. The UE shall send its DN-specific identity complying with Network Access Identifier (NAI) format.

NOTE: Steps 8 and 9 are optional. To avoid this additional round-trip, the secondary authentication identity could be sent in step 4.

10. The SMF selects a UPF and initiates a N4 Session establishment procedure with it.

This establishes an end-to-end connection between the SMF and the external DN-AAA server for EAP exchange.

11. The EAP Response/Identity message is routed to the DN AAA Server by UPF.

12. The DN AAA server and the UE exchange EAP messages as required by the EAP method.

13. After the completion of the authentication procedure, DN AAA server sends EAP Success message to the SMF.

14. This completes the authentication procedure at the SMF.

If the authorization is successful, PDU Session Establishment proceeds further starting step 6a of Figure 4.3.2.2.1-1 in TS 23.502 v0.2.0.

15a-15b. The SMF initiates a N4 Session Modification procedure with the selected UPF as in steps 9.a and 9.b of Fig 4.3.2.2.1-1 in TS 23.502 v0.2.0.

16. The SMF sends "SM Request Ack" to AMF as in step 10 of Fig. 4.3.2.2.1-1 in TS 23.502 v0.2.0. This message includes EAP Success to be sent to the UE within the NAS SM "PDU session establishment accept".

17. The AMF forwards NAS SM "PDU session establishment accept" along with EAP Success to the UE as described in steps 11 and step 12 of Figure 4.3.2.2.1-1 in TS 23.502 v0.2.0.

The UE-requested PDU Session Establishment proceeds further as described in clause 4.3.2.3 in TS 23.502 v0.2.0.

In case of a Home Routed deployment, it is the SMF in the HPLMN that takes the role of the authenticator.

Figure 5.2.4.30.2-2 shows the protocol architecture for the support of the EAP based secondary authentication.

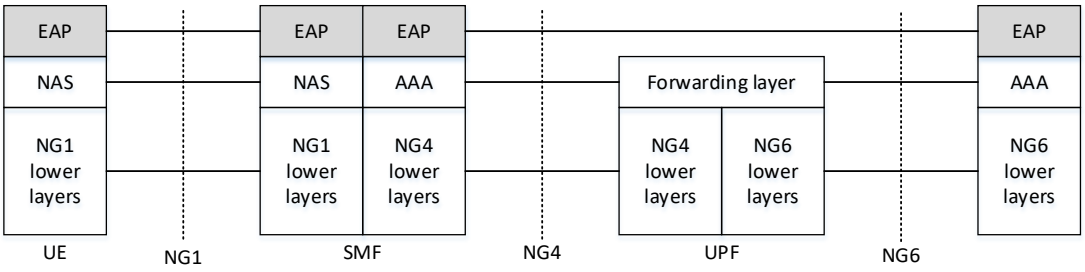


Figure 5.2.4.30.2-2: Protocol architecture for secondary authentication

The UE communicates EAP related information to the SMF over the NAS protocol (in NAS SM messages). This information is further sent to DN-AAA over NG4 and NG6 via the UPF.

Lenovo Ex. 1007
Page 248

5.2.4.30.3 Evaluation

FFS

5.2.4.z Solution #2.z: <solution name>

5.2.4.z.1 Introduction

Editor's note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the security area.

5.2.4.z.2 Solution details

5.2.4.z.3 Evaluation

5.2.5 Conclusions

Editor's note: This clause will contain the evaluation between the solutions, and the conclusions made by SA3.

5.3 Security area #3: Security context and key management

5.3.1 Introduction

Editor's Note: This clause gives background information on the security area.

5.3.2 Security assumptions

Editor's Note: This clause will document security assumptions related to each security area.

5.3.3 Key issues

5.3.3.1 Key Issue #3.1: Interception of radio interface keys sent between operator entities

5.3.3.1.1 Key issue details

In all of GSM/GPRS, UMTS and LTE, it is the case that the keys from which the for radio interface encryption keys are derived (and integrity, where applicable) are computed in the home core network – the AuC – and then transmitted to the visited radio network over signalling links such as SS7 or Diameter. This is a clear point of exposure, and it has been demonstrated repeatedly how keys can leak. Each operator network has to respond to signalling messages, which may come from any roaming partner – including roaming partners that are either hacked or misbehaving in any way. It should therefore be studied further whether and how EPS AKA and/or EAP-AKA' should be complemented with measures to counter the threat of insecurity of the Interconnect network. Such measures have to be standardized at least as far as they affect the interface between UE and visited network.

The most direct, and clearly recommended industry approach is for operators to improve SS7 / Diameter security, e.g. by introducing SS7 firewalls. But well-designed key management protocols for Next Generation Systems could also reduce the threat significantly.

In GSM terms, this key issue is about the leakage of the cipher key KC when sent between network nodes, whereas Key Issue a.1 is about the leakage of Ki. So the problems are different. There may, however, be some overlap in the set of possible solutions.

Lenovo Ex. 1007
Page 249

5.3.3.1.2 Security threats

An attacker who can successfully obtain current radio interface keys for a subscription can straightforwardly eavesdrop on that subscriber's traffic. A wide range of abuses is also possible if the attacker can spoof MACs on UMTS / LTE messages that should be integrity protected.

The following key theft attacks and re-routing attack are expected to be relevant for a NextGen Interconnection network. Many of these threats are likely to evolve from threats seen in today's SS7 networks; at least it has been explicitly stated in publications, e.g. [28], that many of the threats seen in SS7 networks are likely to carry over to DIAMETER Interconnection networks. These may in turn be used in NextGen Interconnection networks.

Key theft attacks:

An attacker could obtain keys in several different ways:

1. by passively eavesdropping on the communication between an HSS sending authentication vectors (AVs) to a genuine serving node. Attack 1 is not commonly described in the literature as an attack on SS7 networks (which does not, of course, mean that it could not be performed.);

2. by impersonating a genuine serving node towards the HSS and obtaining AVs in this way; [28, 29]

3. by impersonating a genuine serving node towards another serving node to obtain a current security context (e.g. sending a forged context request between SGSNs or MMEs used in handovers or idle mode mobility) [30]

Re-routing attack: The attacker could also impersonate a genuine serving node by sending a forged Location Update message to the HSS [30]. In this way, the downlink traffic could possibly be re-routed towards the attacker's serving node.

5.3.3.1.3 Potential security requirements

- An attacker who is able to observe or request session keys sent between network nodes should not be able carry out a passive eavesdropping attack on the subscriber's radio interface traffic (assuming that radio interface user plane encryption is in place).

5.3.3.2 Key Issue #3.2: Refreshing keys

5.3.3.2.1 Key issue details

In GSM/GPRS, UMTS and LTE it is entirely down to the visited network to determine when a reauthentication, and consequent change of radio interface keys, takes place. There is no way for the UE (or a service running on the UE) to demand – or even request – that keys should be refreshed. The only route open to the UE is to drop the connection and then reconnect, and hope that this triggers a reauthentication; even then, there is no guarantee.

5.3.3.2.2 Security threats

The main threat here arises when a UE roams onto a visited network that has a lax security policy, allowing the same radio interface keys to remain in use for a long time. There are two drivers to update a cryptographic key: either the length of time that the key is used for, or the volume of data that it's used to protect.

Also, a false network that has somehow managed to get hold of valid session keys can continue using those session keys indefinitely, unless the UE can demand an update.

After handover from a different generation (e.g. UMTS), which may have run a less strong authentication and key agreement procedure than the NextGen one, the same (or derived) session keys may continue to be used. Even if the standards recommend that a network should reauthenticate after handover, some networks may not do so.

5.3.3.2.3 Potential security requirements

- The UE should have some ability to trigger a refresh of AS and NAS security keys. Care must be taken not to create network overload, however.

- The UE should not congest the network by frequently requesting the radio interface keys to be refreshed.

Lenovo Ex. 1007
Page 250

Note1: The decision to refresh the keys is the responsibility of the network.

Editors' note: The action of the UE if the network fails to change the security is for ffs. Actions other than the dropping the connection should be investigated.

5.3.3.3 Key issue #3.3: Principles of security negotiation

5.3.3.3.1 Key issue details

In EPS, the security mode procedures for NAS and AS serve to establish, which cryptographic algorithms will be used for the security context about to be established. The network side takes the decision for both NAS and AS security mode procedures. The only security feature to negotiate is encryption, the decision on whether encryption is switched off or on is implicit in the choice of the encryption algorithm (NULL or non-NULL).

This situation already started to get a little more complex in the GPRS security enhancements defined in the EASE work item in Rel-13. According to EASE, cf. TS 43.020, Annex H, the MS informs the SGSN whether it supports user plane integrity or not. Furthermore, the subscriber profile optionally contains information about whether user plane integrity is required for this subscription or not. Finally, it was decided for EASE that the same set of cryptographic algorithms shall be used for both user plane and control plane.

Like in EASE, not all NG UEs will be required to support user plane integrity. Hence, again like in EASE, the UE will need to indicate to the network whether the UE supports this feature.

It is expected that, for NextGen, even more flexibility than already provided by EASE will be required. Many UEs will establish end-to-end or end-to-middle security associations with other devices or with application servers, providing confidentiality or integrity or both. In this case, confidentiality and/or integrity will not be needed over the air interface from the UE point of view. However, the network may still require one or both of these features, e.g. for protecting the network from attacks. Hence, the UE should be able to indicate whether it requires confidentiality and/or integrity. But it should still be the network to decide which security feature is provided, based on these indications from the UE and possibly additional information from the subscriber profile.

Note that there is no room for negotiation of integrity for the control plane as integrity is mandatory to use and little room for negotiation of confidentiality for the control plane as confidentiality is recommended to be used, subject to local regulations, which means that, in practice, the network will decide its use based on these local.

5.3.3.3.2 Security threats

tbd

5.3.3.3.3 Potential security requirements

- The UE shall support at least two encryption algorithms and at least two integrity algorithms. All of them shall be usable for both control plane and user plane.
- The UE shall support signalling to the network whether the UE supports user plane integrity.
- The UE may support signalling to the network whether the UE prefers to use or not to use user plane confidentiality.

NOTE1: The motivation for the above requirements is as follows: If the UE knows that there is e2e confidentiality it will signal "confidentiality not preferred" to the network. If the UE knows that there is no e2e confidentiality and the data sent by the application is confidential it will signal "confidentiality preferred". If the UE sends no signalling the UE leaves the decision entirely to network policy.

- The UE may support signalling to the network whether the UE prefers to use or not to use user plane integrity.

NOTE2: The motivation for the above requirements is as follows: If the UE knows that there is e2e integrity it will signal to the network "integrity not preferred". If the UE supports integrity and knows that there is no e2e integrity and the data sent by the application requires integrity it will signal "integrity preferred". If the UE sends no such indication the UE leaves the decision entirely to network policy.

Lenovo Ex. 1007
Page 251

- The network (access network entity or core network entity) shall take the final decision on which security features and algorithms will be used, taking into account what the UE has signalled and potential additional information in the subscriber profile.
- The network shall select one ciphering algorithm and one integrity algorithm to be used for both control plane and user plane.
- The network shall indicate whether user plane integrity is used.
- The UE may decide to refuse a connection that does not meet criteria set in a policy in the UE. A UE that has refused a connection may attempt to set up a connection at a later time again.
- UEs that use a local policy to refuse connections that do not meet the criteria should have a recovery mechanism to avoid a total lock-out. Such a recovery mechanism could be that the UE should be able to inform the end-user and allow the end-user to overrule the policy or could be that the UE should accept an unsecure connection after a number of failed tries.-Security negotiation shall not be susceptible to bidding down attacks.

5.3.3.4 Key Issue #3.4: Security context sharing

5.3.3.4.1 Key issue details

In the LTE networks, authentication for 3GPP and Non-3GPP access technologies are performed separately. For example, the authentication point for 3GPP connection is at MME and the one for WLAN is at AAA server. For the same UE with two connections using different access technologies, it has to perform two full authentication procedures with the core networks. This not only increases delay for security association establishment between UE and network, but also incurs overhead in signalling transmission.

For next generation networks, a unified authentication framework for different access technologies is adopted by 3GPP. Security context for different access technologies may reside on the same entities at both UE and core network side. This makes the security context sharing among different access technologies easier.

5.3.3.4.2 Security threats

In next generation networks, security contexts of one UE, e.g. keys used for data and signalling protection, for different access technologies may be coorelated. If one security context is compromised in one access technology, then this may compromise a security context on another technology in the same UE.

5.3.3.4.3 Potential security requirements

- To optimize the security association establishment procedure with authentication framework, security context information sharing mechanism for same UE among different access technologies should be studied. Keys used in different access technologies shall be cryptographically separated and bound to the access, e.g. by suitable key derivation

5.3.3.5 Key issue #3.5: Unnecessary dependence of keys between security layers

5.3.3.5.1 Key issue details

In LTE, there is an unnecessary dependence between the NAS security context and the AS security context. This issue only manifests itself when the MME is rekeying the whole key hierarchy and has succeeded in updating the NAS security context to a new K_{ASME}, but has not rekeyed the AS context to be based on the new K_{ASME}. For example, if an S1-handover involving MME relocation happens at this point, it is necessary to send both the old and new K_{ASME} to the new MME. While this is not an issue for LTE, due to the assumption that all MME are deployed in secure locations, it does unnecessarily allow the new MME to calculate previous keys (NAS layer and AS layer keys that were derived from the old K_{ASME}). It is preferable to avoid such a feature in NextGen as in particular it may be that MMEs (or the NextGen equivalent of an MME) are deployed in less secure locations.

Looking at the LTE Key Hierarchy, the reason the above problem exists is that K_{ASME} is required to calculate fresh NH values. Hence in effect the K_{ASME} is the root key needed for the operation of two different layer of security contexts. As NAS and AS security contexts are not changed simultaneously, this means that even after an MME has run and an AKA and NAS security mode procedure to take a new NAS security context based on a new K_{ASME} into use, it cannot

Lenovo Ex. 1007
Page 252

effectively delete the old NAS Security context as it must retain the previous K_{ASME}. This is contrary to good security practise where it is preferable to remove old security keys as soon as possible.

In summary, it is preferable in NextGen that the security context at a higher layer (as soon as it is finished with) can be completely deleted without affecting the ability to use lower layer security context (e.g. the same keys should not need to be used in both security contexts). Such a definition of the security contexts should not result in breaking the authorisation model, i.e. it is still possible to know that the two security contexts are associated with the same UE.

5.3.3.5.2 Security threats

When security contexts at different layers share a common key, it means that it is impossible to completely replace (for example in LTE replacing the NAS security context in an MME after an AKA) the higher layer security context until the lower layer security context has become obsolete. It may also result in this key being passed to another entity which then be capable of decrypting data that it would otherwise not get access to.

5.3.3.5.3 Potential security requirements

TBD

5.3.3.6 Key issue #3.6: Top-level key for access-network-specific keys

5.3.3.6.1 Key issue details

Authentication between UE and network will establish an authentication session key. This authentication session key may be derived in an access-network-independent manner. Further keys will be derived from this session key. Access-network-specific keys may be derived either directly from the authentication session key or from an AN-specific-top-level key. It matters for the overall security of the system where this top-level key, from which all access-network-specific keys are derived, resides.

The present key issue deals with the following questions:

- Whether an AN-independent authentication session key is to be maintained throughout a 'session' or 'registration period';

Editor's Note: The terms 'session', 'registration period' will be clarified as SA2 work progresses.

- Whether an AN-specific-top-level key is required, and, if so, whether it is different from the authentication session key;
- For any of the above keys, whether it shall reside in the NextGen core network and / or in a physically protected location.
- The relationship with the entity 'security anchor' in key issue #ARCH.2 needs to be clarified.

5.3.3.6.2 Security threats

tba

5.3.3.6.3 Potential security requirements

tba

5.3.3.7 Key issue #3.7: The storage of security context

5.3.3.7.1 Key issue details

Based on the types and states of EPS security context, different principle is applied for storage, e.g. the USIM shall never store a mapped security context. In NextGen system, the storage of security context may be different both from USIM and EPS system.

Editor’s note: LTE principle should be used as a working assumption for now.

Lenovo Ex. 1007
Page 253

5.3.3.7.2 Security threats

The main threat is when the security context stores in an unsecure environment both at the UE side and the NextGen system side where the security context can be obtained by attackers. The leakage or disclosure of security context can lead to serious attaks. The attacker can imitate to the user, as well as the network. The most serious thing is that neigher the user nor the NexGen system can not distinguish the attacker from the legitimate user.

5.3.3.7.3 Potential security requirements

The security context shall securely be stored both at the UE side and the NextGen system side.

5.3.3.8 Key issue #3.8: Security context for small data mode

5.3.3.8.1 Key issue details

One aim of the NextGen system is to support the services for Massive IoT devices. In SMARTER TR 22.891[7], a small data mode has been defined to support short data bursts. For supporting small data mode, a new type of security context may be introduced.

5.3.3.8.2 Security threats

Tba.

5.3.3.8.3 Potential security requirements

Tba,

5.3.3.9 Key issue #3.9: void

5.3.3.10 Key issue #3.10: void

5.3.3.11 Key issue #3.11: 5G security key and context identification

5.3.3.11.1 Key issue details

The EPC key identifier for K_{ASME} is called key set identifier eKSI which can be of type KSI_{ASME} or of type KSI_{SGSN}. The eKSI is stored in the UE and the MME together with K_{ASME} and the temporary identifier GUTI, if available.

As further detailed in TS 33.401:

> The key set identifier KSI_{ASME} is a parameter which is associated with the K_{ASME} derived during EPS AKA authentication. The key set identifier KSI_{ASME} is allocated by the MME and sent with the authentication request message to the mobile station where it is stored together with the K_{ASME}. The purpose of the KSI_{ASME} is to make it possible for the UE and the MME to identify a native K_{ASME} without invoking the authentication procedure. This is used to allow re-use of the K_{ASME} during subsequent connection set-ups.
>
> The key set identifier KSI_{SGSN} is a parameter which is associated with the mapped K_{ASME} derived from UMTS keys during inter-RAT mobility, cf. clauses 9 and 10 of the present specification. The key set identifier KSI_{SGSN} is generated in both the UE and the MME respectively when deriving the mapped K_{ASME} during idle procedures in E-UTRAN and during handover from GERAN/UTRAN to E-UTRAN. The KSI_{SGSN} is stored together with the mapped K_{ASME}.
>
> The purpose of the KSI_{SGSN} is to make it possible for the UE and the MME to indicate the use of the mapped K_{ASME} in inter-RAT mobility procedures.

For managing and accessing the security context and the key hierarchy in 5G and to identify the 5G security context a new parameter will be needed. This new parameter need to be associated with the master key derived during the 5G authentication and key agreement protocol and the security context established in the 5G system.

Lenovo Ex. 1007
Page 254

5.3.3.11.2 Security threats

Manipulation of UE context using mobility management messages during mobility events: During mobility events when UE moves between different access types under one CCNF or moves to a different CCNF/MME with change of technology NG to LTE or vice-versa, security context needs to be identified correctly to avoid re-authentication of the UE. In the case of inter technology handovers, security context needs to be mapped between technologies. Without a unique identifier for the context, mix up of security context between different UEs is a possibility. This needs to be avoided.

5.3.3.11.3 Potential security requirements

- The NextGen system shall have a unique key set identifier to manage and access the security context.
- The NextGen key set identifier should have a structure to indicate the system type as valid for next generation and the assigned value of the index.
- The NextGen key set identifier should be integrity protected and confidentiality protected when sent between network entities.

5.3.3.y Key issue #3.y: <key issue name>

5.3.3.y.1 Key issue details

5.3.3.y.2 Security threats

5.3.3.y.3 Potential security requirements

5.3.4 Solutions

5.3.4.1 Solution #3.1: Including a key exchange protocol into the derivation of the radio interface session keys

5.3.4.1.1 Introduction

This solution addresses key issues #2.2 and #3.1.

It ensures that an attacker who:

- either knows the long term secret key and Authentication and Key Agreement algorithm (including any global constants) that a subscription is using,
- or is able to observe or request keys sent between network nodes,

can still not abuse radio interface confidentiality in a purely passive attack, or abuse radio interface integrity by simple injection of a single spoofed message, but will instead have to carry out an ongoing active man-in-the-middle attack – which is harder, and more likely to be detected.

5.3.4.1.2 Solution details

NOTE: In this section we refer to the "UICC" and the "HSS". These should be understood as shorthand, referring respectively to the "device's UICC / secure element (or wherever the long term key is stored)" and the "HSS (or its Next Generation Systems equivalent)".

As in GSM/GPRS, UMTS or LTE, the Authentication and Key Agreement algorithm is run in the HSS, with a resulting authentication vector sent to the visited network, and also in the UICC to establish shared secret keys between the UE and a node in the visited network. However, instead of using those keys directly for radio interface security, or as inputs to a key derivation algorithm to produce radio interface security keys, they are instead used to authenticate a key exchange algorithm between the device (possibly its UICC) and that visited network node. Elliptic Curve Diffie Hellman would be a suitable key exchange algorithm.

Lenovo Ex. 1007
Page 255

In Figure 5.3.4.1.2-1, "Node X" represents whatever visited network node carries out the key exchange protocol with the device. It is premature to attempt to identify the most suitable node in Next Generation Systems, but if this solution were being retrofitted to LTE then the MME would be a natural choice.

Editor's note: The above paragraph needs to be revised to fit the NextGen architecture.

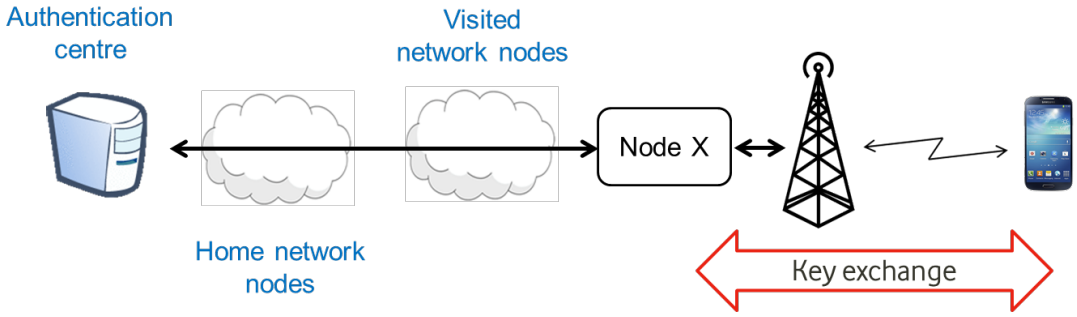


Figure 5.3.4.1.2-1: Key exchange to derive radio interface security keys

It is a good idea for both the initial shared secret keys (that were in the authentication vector, and were used to authenticate the key exchange) and the output of the key exchange protocol to be fed into a key derivation function, whose outputs are then used as the radio interface security keys. That way, an attacker would have to know the original shared secret and compromise the key exchange to learn the new radio interface keys. A suitable key derivation algorithm can use HMAC-SHA256, as defined in 3GPP TS 33.220 [27], as follows:

new radio interface key = KDF (key exchange protocol output, initial shared secret key)

where "key exchange protocol output" refers to the shared secret resulting from the key exchange protocol, and "initial shared secret key" refers to the initial shared secret keys that were in the authentication vector, and were used to authenticate the key exchange.

Editor's note: The following procedure needs to be revised once the authentication and key agreement mechanism in NextGen is defined.

Solution 12.1 in TR23.799 [2] proposed a unified authentication framework for Next Generation network. The unified authentication framework is shown in figure 5.3.4.1.2-2. It consists of supplicant, CP-AU and AAA. Therefore, the DH procedure shall be integrated with the proposed authentication framework.

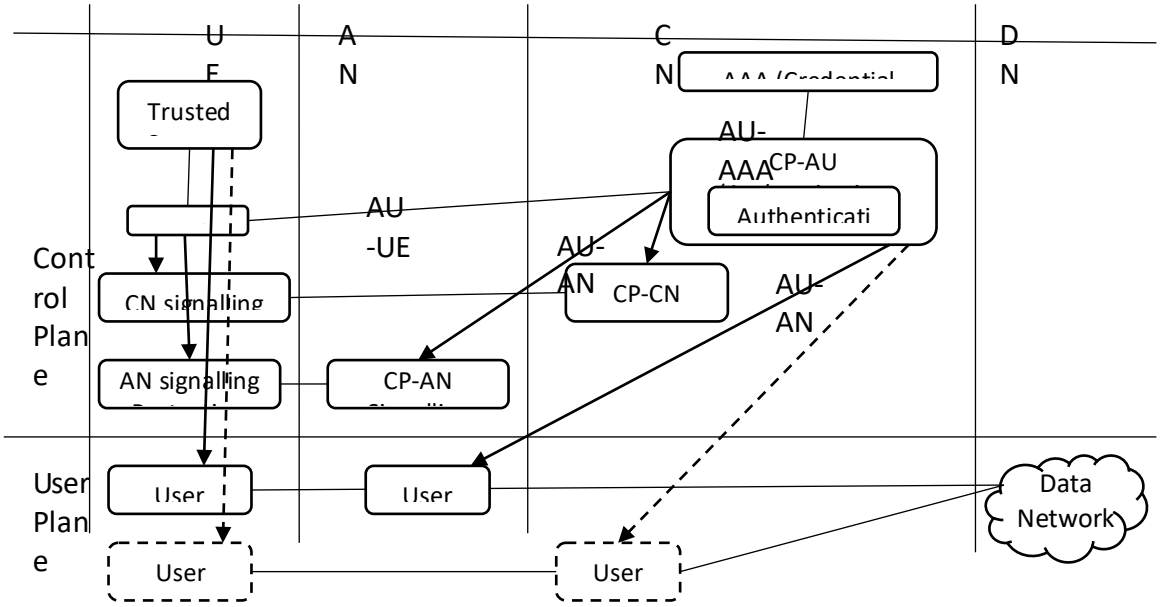


Figure 5.3.4.1.2-2: Unified Authentication Framework for Next Generation Networks

Editor's Note: The figure and the corresponding description should be aligned with SA2.

Lenovo Ex. 1007
Page 256

To integrate the Diffie-Hellman procedure into the authentication and key agreement protocol for session key enhancement, we proposed a possible procedure which is compatible to the Next Generation Systems unified authentication framework. The procedure is as follows:, .

1. UE sends attach Request to UE in which contains indicators of UE D-H capability groups. A D-H capability group indicator indicates a pair of large primes that are pre-configured.

2. UE and SEAF perform mutual authentication.

3. UE and SEAF derive K1 after mutual authentication. The K1 derived in a similar way to the derivation of K_{ASME} in LTE.

4. SEAF selects a D-H capability indicator based on the D-H capability groups of the UE and the preference list of the SEAF. SEAF generates a private Diffie-Hellman key A_{PRIV} and a corresponding public key A_{PUB} based on the selected D-H capability.

5. SEAF sends message 1 to UE, which contains selected D-H capability indicator, APUB and a MAC computed using K1.

6. UE verifies the MAC, decodes A_{PUB}, and further generates a Diffie-Hellman private key B_{PRIV} and corresponding public key B_{PUB} based on the selected D-H capability. UE also derives a symmetric key KDH from BPRIV and A_{PUB} with Diffie-Hellman procedure. UE derives a session key Ksession from with K_{DH} and K1.

7. UE sends message 2 to SEAF, which contains BPUB and a MAC computed using K1.

8. SEAF verifies the MAC, decodes BPUB, and derives the same a symmetric key KDH from APRIV and BPUB with Diffie-Hellman procedure. SEAF derives the same session key Ksession from KDH and K1.

Both UE and SEAFnow own the same shared session key Ksession. They use Ksession to derive other keys for encryption and integrity protection. The Diffie-Hellman technique used in this authentication protocol can also be Elliptic Curve Diffie-Hellman.

Lenovo Ex. 1007
Page 257

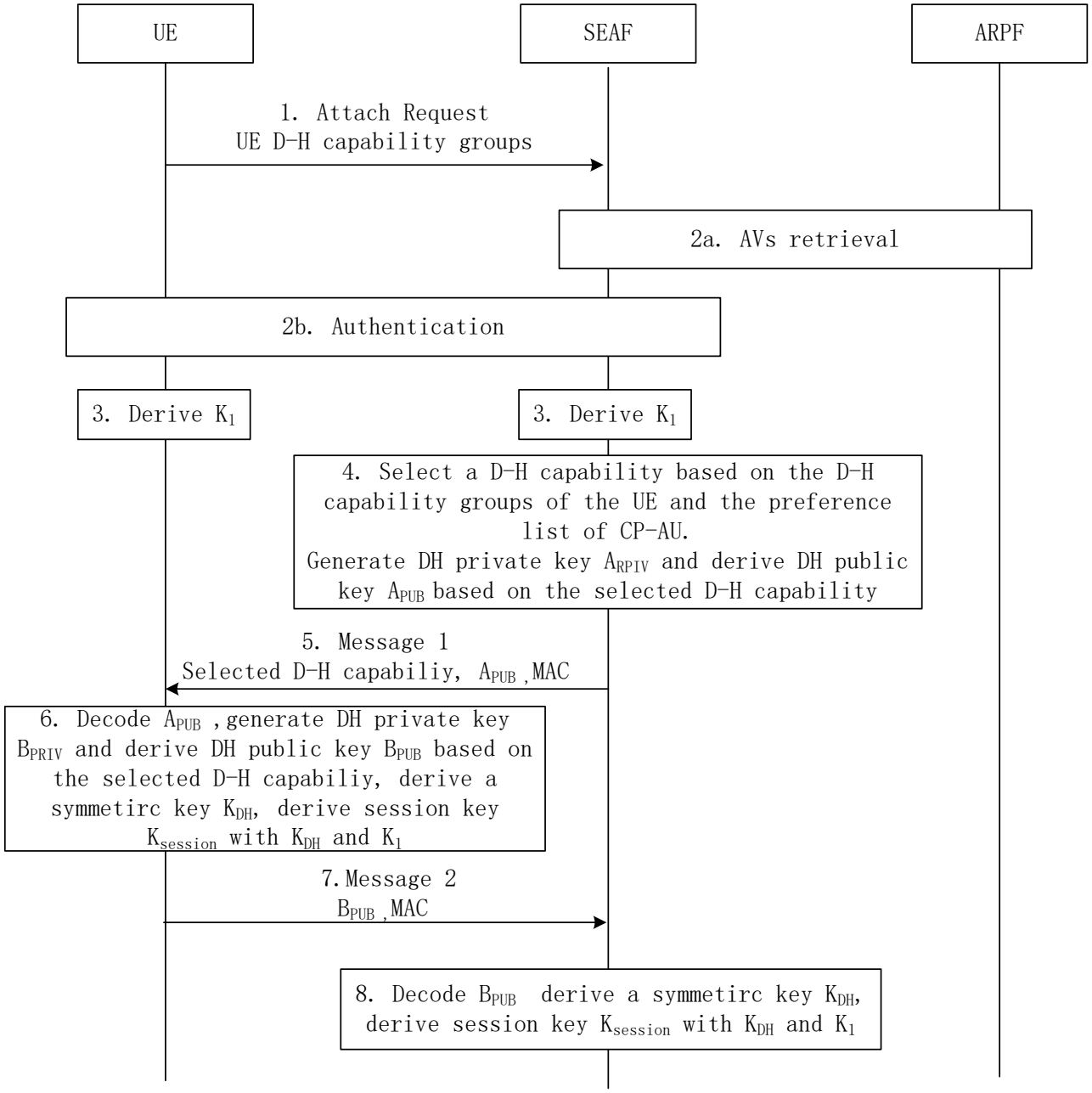


Figure 5.3.4.2.2-3: Integration of Diffie-Hellman procedure with key exchange protocol

5.3.4.1.3 Evaluation

The solution #3.1 described in clause 5.3.4.1 basically consists in applying a Diffe-Hellman handshake after the intermediate key obtained from the authentication vector (e.g a K_{ASME} key) has been successfully established between UE and serving node (e.g. MME). The security context that results from the intermediate key combined with the DH handshake would then be used to derive further keys to protect the radio interface.

We discuss how well the threats described in clause 5.3.3.1.2 are countered by solution #3.1 in the following.

- The first threat described in clause 5.3.3.1.2 seems to be the only attack that solution #3.1 counters reasonably well: as stated in the requirements in clause 5.3.3.1.3, the attacker would indeed have to give up his passivity and become a long term, active man-in-the-middle.

But solution #3.1 seems ineffective against the following attacks:

Lenovo Ex. 1007
Page 258

- Key theft attack 2 means that the authentication vector is sent to the attacker and, hence, not available at any genuine serving node that would perform an Attach procedure with a user. So, the attacker could not sit back, record the encrypted traffic and decrypt later using the knowledge of the eavesdropped key.

  However, the attacker could proceed to impersonate a genuine serving node towards a UE (using one or more false base stations in the vicinity of the victim that would be attached to the serving node). In this way, the attacker could eavesdrop on the UE's traffic for some significant amount of time. The attacker could repeat this attack many times (as long as the attacker would be able to obtain fresh authentication vectors).

  The underlying assumption in the formulation of the requirement in clause 5.3.3.1.3 seems to be that the involvement of the attacker as " long term, active man-in-the-middle " would make the attack unrealistic. But attack 2 can be seen as a false base station attack that would be just as practical as its well-known analogue in GSM (with the difference being that the attack does not exploit a weakness in the air interface security - as in GSM - but in the Interconnection network security).

- Key theft attack 3 is an attack not on SS7 or DIAMETER, but on GTP. It would use e.g. false messages on the NextGen-equivalent of the interface between SGSNs or MMEs. The attacker would record the encrypted communication over the air. The attack on the serving node would only start after the security context, from which the radio encryption and integrity keys were derived, had been established. In particular, it would start only start after the DH handshake proposed in solution #3.1 would have been applied. Hence, solution #3.1 cannot help in mitigating this attack.

- The re-routing attack is an attack exploiting a weakness of the Interconnection network. But it could not be countered by solution #3.1 as the attack does not exploit the knowledge of keys.

Clause 5.3.3.1.1 "Key issue details" states: " The most direct, and clearly recommended industry approach is for operators to improve SS7 / Diameter security, e.g. by introducing SS7 firewalls." This is most certainly true. Solutions approaches can be found in security area#10.

The text in clause Clause 5.3.3.1.1 continues: " But well-designed key management protocols for Next Generation Systems could also reduce the threat significantly." According to the above evaluation, at least solution #3.1 is unlikely to mitigate some common threats seen in today's SS7 networks and could be easily circumvented. It appears that these common threats need to be mitigated by security enhancements to the Interconnection network. But then it is likely that also the only threat, against which solution #3.1 really helps, namely passive eavesdropping on authentication vectors, could be mitigated by similar security enhancements to the Interconnection network.

Conclusion:

Solution #3.1 is costly in terms of performance, especially delay, and it does not help against key theft attacks 2 and 3 nor against the re-routing attack.

5.3.4.2 Solution #3.2: UE can request a radio interface key refresh

5.3.4.2.1 Introduction

This solution addresses key issue #3.2.

5.3.4.2.2 Solution details

Editors' note: more details are needed here

Signalling messages should be defined to allow a UE to request the visited network to carry out a radio interface key refresh. (This may equate to a reauthentication, but we don't know that yet for Next Generation.) It is too early to say exactly whether a new message type will need to be defined, or an existing message type adapted; and it is too early to say which node in the visited network will be the recipient of this message. If this were being retrofitted to LTE, however, then a natural approach would be to introduce a new set of parameter values and new cause code in the Tracking Area Update and/or Routing Area Update messages.

Such request messages are defined for every type of session key used to protect communication or signalling between the UE and any serving network node.

While the architecture of NextGen is being developed, it is difficult to draw final conclusion on the best approach. A UE sends a key refresh message to the parent node of the node that the UE wants to reauthenticate (this request may

Lenovo Ex. 1007
Page 259

possibly travel via other nodes if the UE does not have a direct signalling connection with). In case of the UE re-authenticating a NextGen access node (AN), e.g., gNB, the UE sends the key refresh request to the control-plane entity in the core network which derives the AS key (e.g., KAN which is equivalent to KeNB in LTE) for the access node. The key refresh request is sent using a NAS message. It would also be expected NAS messages would reach entities that can also refresh the NAS security and trigger re-authentication of the whole key hierarchy. Therefore it seems likely that a NAS message would be the appropriate place to carry a key refresh request and such a request would be able to request different levels of key refresh.

Note that this is a request that the visited network may (and normally will) fulfil – not a demand that it must fulfil. This means that the visited network retains ultimate control.

A possible, optional extension is that the UE drops the connection if the request is not fulfilled.

Note that this in no way reduces the network's ability to reauthenticate / update keys whenever its policy requires.

5.3.4.2.3 Evaluation

This solution clearly addresses Key Issue #3.2. The solution is, necessarily, described only at a rather high level, because the detail depends on other choices concerning the session key management architecture and protocols. Nevertheless, it seems very likely that this solution will be achievable and applicable, no matter what key management architecture and protocols are chosen.

5.3.4.3 Solution #3.3: Security Context Management for UE with Multiple Access Technologies

Editor's note: The terminology used in this solution needs to be updated (e.g.it should use the terms "equipment" or "equipment identifier" instead of "device" or "device identifier".

5.3.4.3.1 Introduction

The next generation network system will support multiple access technologies, including previous generation radios, next generation radio, Wi-Fi access technologies, etc. Many of the UE support multiple access technology and UE may establish multiple connections simultaneously to the network with the same 3GPP credentials after the initial authentication based on unified authentication framework. In TR 23.799 [1], a solution (6.12.1) in key issue 12 for authentication framework has been included. It includes a uniformed authentication framework and a security context structure at the network side. But a security context structure has not been defined for UE yet. Therefore, we proposed a security context structure at UE side with the uniform authentication framework and network side security context structure taken into consideration.

5.3.4.3.2 Solution details

With the Next Gen system, a UE may have several simultaneous connections to the network. Different connections may utilize different access technologies. However, different access technology may authenticate with network using the same 3GPP credentials. This solution outlines how the UE authenticates with network and derives security context for each access technology.

In this solution, different access technology shares the same supplicant at UE side. The supplicant is responsible for the authentication for different access technologies.

- When the supplicant performs mutual authentication with authentication unit at the network side (CP-AU), if an authentication security context has not been established at the supplicant, then the UE establish a security context within the supplicant.

Editor notes: UE, device and supplicant need further clarification with SA1 and SA2 respectively

- If the supplicant already has an established authentication security context, then the UE can use the existing authentication security context for mutual authentication with the network authentication entity. If the authentication succeeds, then both the Supplicant and CP-AU update the authentication security context.

- Supplicant transmits the derived security context to the relevant access technology module for the protection of communications.

Lenovo Ex. 1007
Page 260

Editor notes: Use of term security context in various places need ffs.

Figure 5.3.4.3.2-1 shows an example structure of the security context.

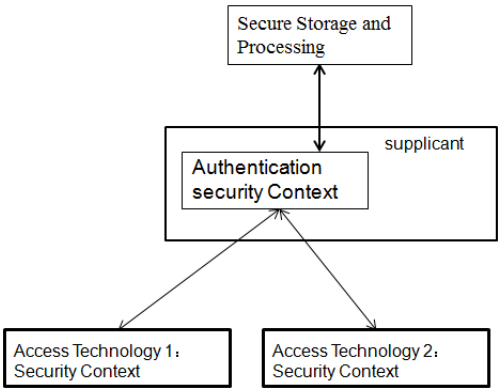


Figure 5.3.4.3.2-1: Security Context Structure for UE with Simultaneous Connections

Figure 5.3.4.3.2-2 shows the detailed procedure for UE with two different access technologies to establish security context with the uniform authentication framework and the security context derivation method proposed above:

1. Supplicant authentication with AUSF within the core network, during which supplicant communicates with Secure Storage and Processing at UE side and CP-AU communicats with ARPF at network side for authentication vectors respectively（2a and 2b）.
2. Supplicant and AUSF establish Authentication Security Context with both CP-AU and Supplicant (3a and 3b)
3. Supplicant and AUSF transmit security context to the relevant device at the UE side and Access Newtork at network side.
4. Both devices and AN installs the security context and use them for data/signalling protection.
5. Supplicant authentication with AUSF within the core network. The authentication procedure reuses the security context established through the authentication for the first access technology.
6. Supplicant and AUSF update Authentication Security Context.
7. Supplicant and AUSF transmit security context to the relative device (device with access technology 2) at the UE side and Access Newtork at network side.
8. Both devices and AN installs the security context and use them for data/signalling protection.

Lenovo Ex. 1007
Page 261

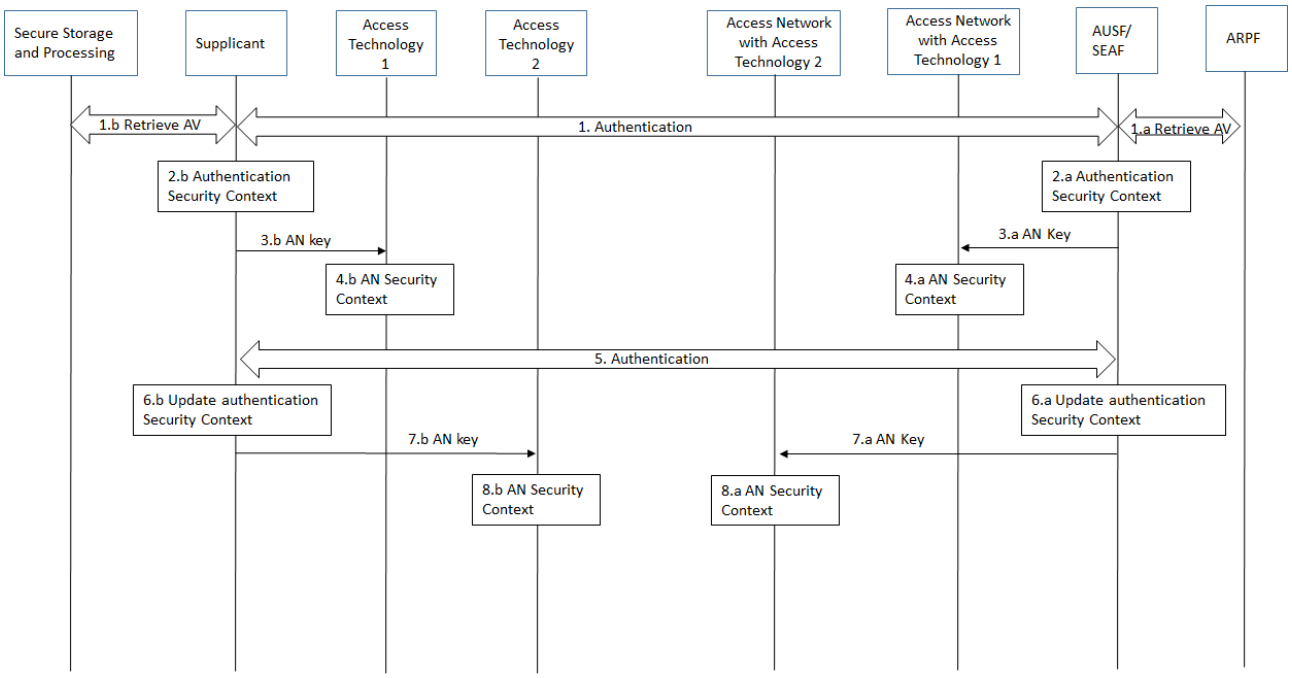


Figure 5.3.4.3.2-2: Authentication and Security Derivation with Simultaneous Connections.

Authentication Security context:

- Kauth: key derived after authentication procedure
- Counter: maintained at both supplicant and CP-AU per authentication security context. It is increased by one after each authentication.
- Fast Reauthentication ID: an ID used by supplicant to perform fast reauthentication.
- Timer: a value specifies the validity of the keys

Editor Notes: Counter and fast authentication ID need for further clarification

After the authentication is finished successfully, the supplicant needs to derive security context for an individual access technology. To isolate the authentication security context from access technologies, the authentication security context is protected and is inaccessible to the individual acces technology. A key derived from Kauth is transmitted to an access technology for data and signalling protection. An example key derivation can be as follows:

- KAT = KDF(Kauth, counter)

The Kauth is always kept within the supplicant and only the KAT is passed to the access technology. Therefore, the session key for an individual access technology is securely isolated from each other.

5.3.4.3.3 Evaluation

Tba

5.3.4.4 Solution #3.4: void

5.3.4.5 Solution #3.5: Trusted non-3GPP access

5.3.4.5.1 Introduction

This solution addresses key issue #3.10 on "Trusted non-3GPP access". It also relates to key issue #2.1 "Authentication framework".

Lenovo Ex. 1007
Page 262

The key issue states: " It is recognized that detailed specifications for trusted access networks in 4G are currently only available for Trusted WLAN (TWAN)... The key issue should therefore explore the security aspects of the NG equivalent of TWAN as well as the need for similar specifications for other access network types. "

The present version of the solution focuses on the NG equivalent of TWAN, i.e. it focuses on trusted WLAN access to the NG core.

Editor's note: The need for specifications similar to the NG equivalent of TWAN for other access network types is ffs.

5.3.4.5.2 Solution details

Architectural aspects:

- We name the NG equivalent of TWAN "NG-Trusted WLAN Access Network" (NG-TWAN). The NG-TWAN forwards IP packets between the UE and the NG core.

The NG-TWAN has the following interfaces:

- The NG-TWAN forwards signalling messages between the UE and one or more control plane functions in the NG core. For simplicity, for the purposes of the present solution we subsume these control plane functions under the name Core Control Function (CCF). The CCF, in general, includes Mobility Management Function (MMF), Session Management Function (SMF), Security Anchor Function (SEAF), and Security Context Management Function (SCMF).

Editor's Note: This solution does not take a stance on whether reference points should be defined between the various functions subsumed under CCF. This is for SA2 to decide.

Editor's Note: It is for SA2 and CT1 to decide how the signalling messages are carried over the TWAN.

- The NG-TWAN forwards user data over IP between the UE and the user plane function NG-UPF in the NG core.

Editor's Note: It is up to SA2 to choose a different name for the user plane function NG-UPF.

Protocol aspects:

- UE authentication is achieved using EAP methods.
- In particular, authentication-related signalling messages in the form of EAP messages need to be forwarded between UE and NG core before IP connectivity over the TWAN is established.
- It is expected that NAS message are sent between UE and CCF after the establishment of an WLAN security association, in particular session management messages (in analogy to WLCP in 4G).

Editor's Note: In 4G, WLCP terminates in the TWAG, which is part of the TWAN. However, in the interest of an access-agnostic session management framework, it is assumed for the present solution that the NG equivalent of WLCP terminates in the CCF (SMF). This needs to be decided by SA2, though.

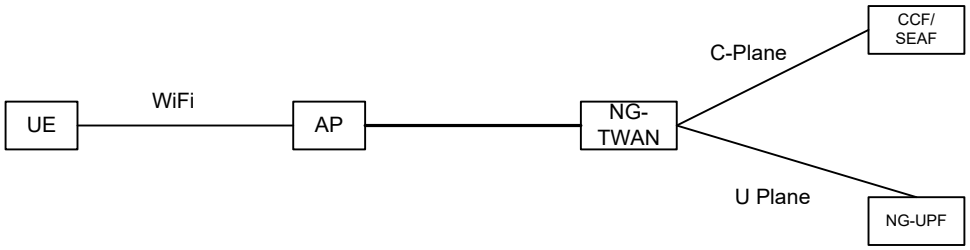


Figure 5.3.4.5.2-1:

Procedural aspects:

- The UE determines that the access network is trusted.

Lenovo Ex. 1007
Page 263

NOTE: Rules for such a determination can be found in TSs 33.402 and 23.402.

- The UE initiates communication with the NG-TWAN.
- The NG-TWAN triggers the UE to send an EAP Identity Response message to the NG-TWAN, which the NG-TWAN forwards to the CCF.

Editor's Note: The above bullet expresses the security needs. In the interest of an access-agnostic mobility management framework, this initial message sent from the NG-TWAN to the CCF could take the form of a generic Attach request. This is, however, for SA2 to decide. In this context, it must be taken into account that a WLAN complying with IEEE 802.1X will let only EAP messages pass until authentication has been completed, so that the information that can be sent before completing authentication is very limited.

- The CCF forwards the EAP Identity Response message to the SEAF.
- The SEAF performs the functions of a 3GPP AAA proxy, as defined in TS 23.402, as far as proxying EAP messages between NG-TWAN and AUSF (which takes the role of EAP server) is concerned.
- At the end of the EAP authentication process, the SEAF sends (possibly via another function in the CCF) the EAP Success message and a key to the NG-TWAN.
- The NG-TWAN uses this key to establish WLAN security according to IEEE 802.11i with the UE.
- IP packets protected between the UE and the NG-TWAN can now be exchanged between the UE and the NG core. These include user plane packets as well as NAS messages sent over IP.

Security context management aspects:

- The SEAF, by its definition, receives the MSK key from the AUSF. This MSK is the anchor key, from which further keys are derived.
- The SEAF takes an active role in key delivery: when the SEAF receives the MSK from the AUSF, the SEAF requests the SCMF to derive a key MSK' from MSK and return it to the SEAF. MSK' is bound to the identity of the NG-TWAN. The key delivered to the NG-TWAN, together with the EAP Success message, is MSK', and not MSK.

NOTE: For the purposes of WLAN security between UE and NG-TWAN, MSK' takes the role that MSK takes in TS 33.402, clause 6.2.

Editor's Note: Re-use of MSK over multiple instances of trusted access is ffs. One solution to consider is EAP-Re-authentication (ERP).

- The UE performs a corresponding key derivation of MSK' from MSK.
- Protection of NAS message that are sent between UE and CCF after the establishment of an WLAN security association, in particular session management messages (in analogy to WLCP in 4G):
    - Use of NAS layer security: The SCMF derives NAS keys from the anchor key MSK and delivers the NAS keys to the MMF and SMF, as appropriate. This would be in line with an access-agnostic handling of NAS security.

Editor's Note: The possiblity of protecting NAS messages by some form of IP address binding is ffs.

Editor's Note: In case SA2 decides to have an NG equivalent of WLCP terminating in the NG-TWAN further key derivations and a security protocol for the NG equivalent of WLCP need to be studied.

Lenovo Ex. 1007
Page 264

5.3.4.5.3 Evaluation

5.3.4.6 Solution #3.6: Next Generation Key Set Identifier

5.3.4.6.1 Introduction

This solution addresses the key issue on "5G security key and context identification" in security area #3: Security context and key management.

Editor's note: Terminology needs to be fixed if security architecture is finalized. Currently a mix of potential 5G terms and LTE terms (e.g. NAS SMC) is used.

5.3.4.6.2 Solution details

Since the NextGen system is being designed to have unified authentication framework to support multiple access technologies such as NextGen (NR), LTE, trusted non-3GPP access, trusted 3GPP access etc., keys need to be derived to support access from any of these access technologies.

For managing and accessing the security context and the key hierarchy in 5G and to identify the 5G security context a new parameter will be needed, which is called Next Generation Key Set Identifier (NG-KSI) in the following. The NG-KSI is a parameter which is associated with a master key derived during an authentication and key agreement protocol.

NOTE 1: Similar to LTE, from the master key, a set of keys will be derived for securing NextGen NAS control plane signaling as well as user plane data terminated directly on the user plane Gateway (UPGW). Subsequent to the successful authentication of the UE and the master key (e.g. similar to K_ASME) keys to protect the access stratum (NextGen AS) will be derived.

NOTE 2: NG-KSI in the clear does not present a significant privacy threat if reasonable short (e.g. three or four bits).

The NG-KSI consists of a value and a type of security context parameter indicating whether an NextGen security context is a native NextGen security context derived out of NextGen authentication of the UE or a mapped NextGen security context derived out of LTE authentication of the UE. NG-KSI will be stored in the Security Anchor Function (SEAF), which may be part of the CCNF (common control function). At the end of successful authentication and verification of the UE, the NG-KSI will be assigned and sent to the UE instructing it to begin a NAS context with index NG-KSI as shown in Figure 5.3.4.6.2-1.

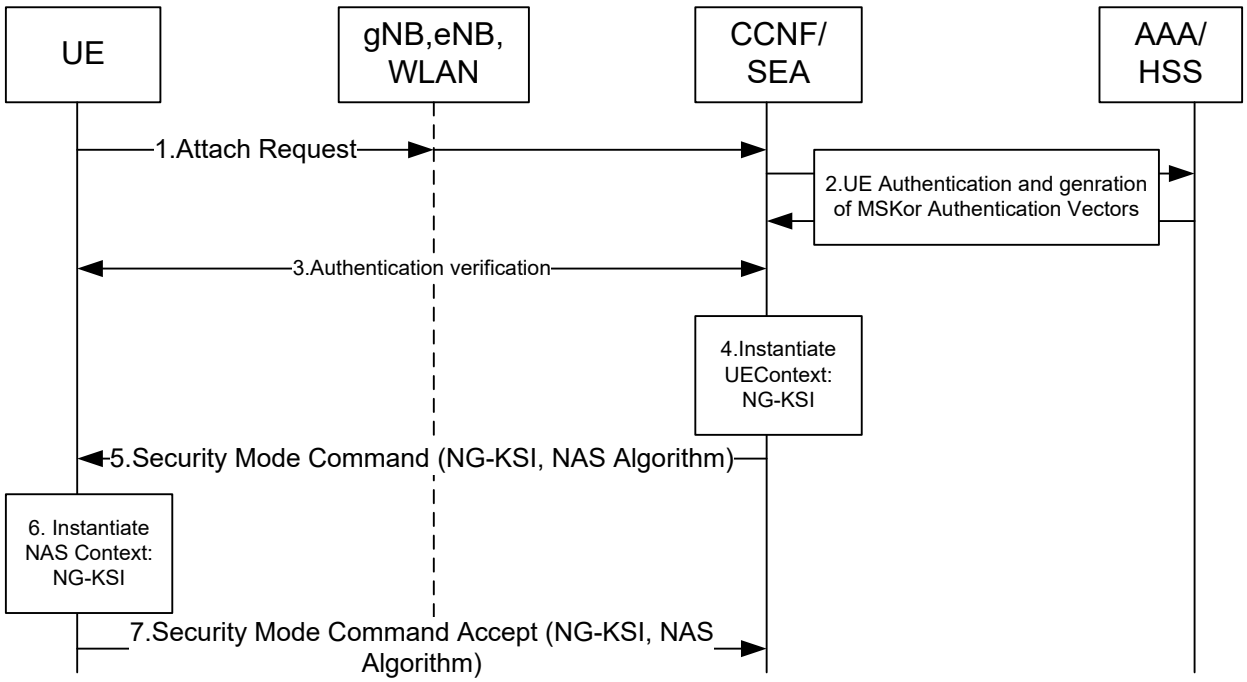


Figure 5.3.4.6.2-1 UE Authentication and Security context instantiation with NG-KSI assignment.

Lenovo Ex. 1007
Page 265

Editor's note: Figure needs to be fixed.

Step 1: The next generation UE, NG UE, does Attach Request to the NextGen system. Attach Request can be made through any of the radio access technologies supported in the NextGen system.

Step2: The Common Control Network Function (CCNF) or the Security Anchor Function (SEAF) of the visited network performs UE authentication in conjunction with the AUSF and the ARPF, and, if authentication is successful, the authentication parameters/vectors are received at the CCNF/SEAF.

Step3: The CCNF/SEAF and UE run NextGen AKA and the authentication request is verified.

Step4: The CCNF/SEAF instantiates a security context for the UE. It assigns a key set identifier NG-KSI for the NextGen system security context. NG-KSI helps the UE and the NextGen system to identify correctly the security context during mobility events.

Step 5: The CCNF/SEAF sends NextGen NAS Security mode command to instruct the UE to instantiate the NextGen NAS security context and the NG-KSI. The message contains additional parameters to secure the NAS communication between the UE and CCNF, to which the SEAF is belonging, such as selected algorithms, NAS counters etc.

Step 6: The UE receiving the NextGen NAS security mode command, instantiates NextGen NAS security context with NG-KSI as the index.

Step 7: UE sends NAS Security mode command to convey the CCNF/SEAF that it has instantiated the NAS security context.

Editor's Note: Depending on SA2 architecture decision, the 5G architecture terminology and functional element names are FFS.

Editor's Note: Impact of the split of MM and SM functions into different nodes is FFS.

Editor's Note: Exact definition and structure of NG-KSI is FFS in CT WGs.

Editor's Note: How the NG-KSI is integrated in the new security messages between 5G system and NG UE, e.g. equivalent to NAS in 4G, is FFS in CT WGs.

5.3.4.6.3 Evaluation

NG-KSI allows the NG-UE and the CCNF/MMF to identify the security context and the correct master key. If such parameter is used, NG-UE and the dedicated network entity storing the NG-KSI do not need to invoke the authentication procedure during a subsequent set-up of the connection during mobility events from LTE to NextGen system or when a connection is changed from one access technology to another within the NextGen system.

5.3.4.7 Solution #3.7: Algorithms Negotiation Procedure

5.3.4.7.1 Introduction

This solution address the key issue 3.3.

The key issue states: "The network (access network entity or core network entity) shall take the final decision on which security features and algorithms will be used, taking into account what the UE has signalled and potential additional information in the subscriber profile."

This solution provides an algorithm negotiation mechanism for the NextGen network.

5.3.4.7.2 Solution details

In LTE, MME is the security anchor to perform algorithms selection and negotiation, while in NextGen the SEAF is the function directly connecting with the NG UE and MM, may also indirectly connect with SM.

In this solution, SEAF is the anchor to perform algorithm negotiation.

Figure 5.3.4.7.2-1 shows the basic call flow for algorithm negotiation.

Lenovo Ex. 1007
Page 266

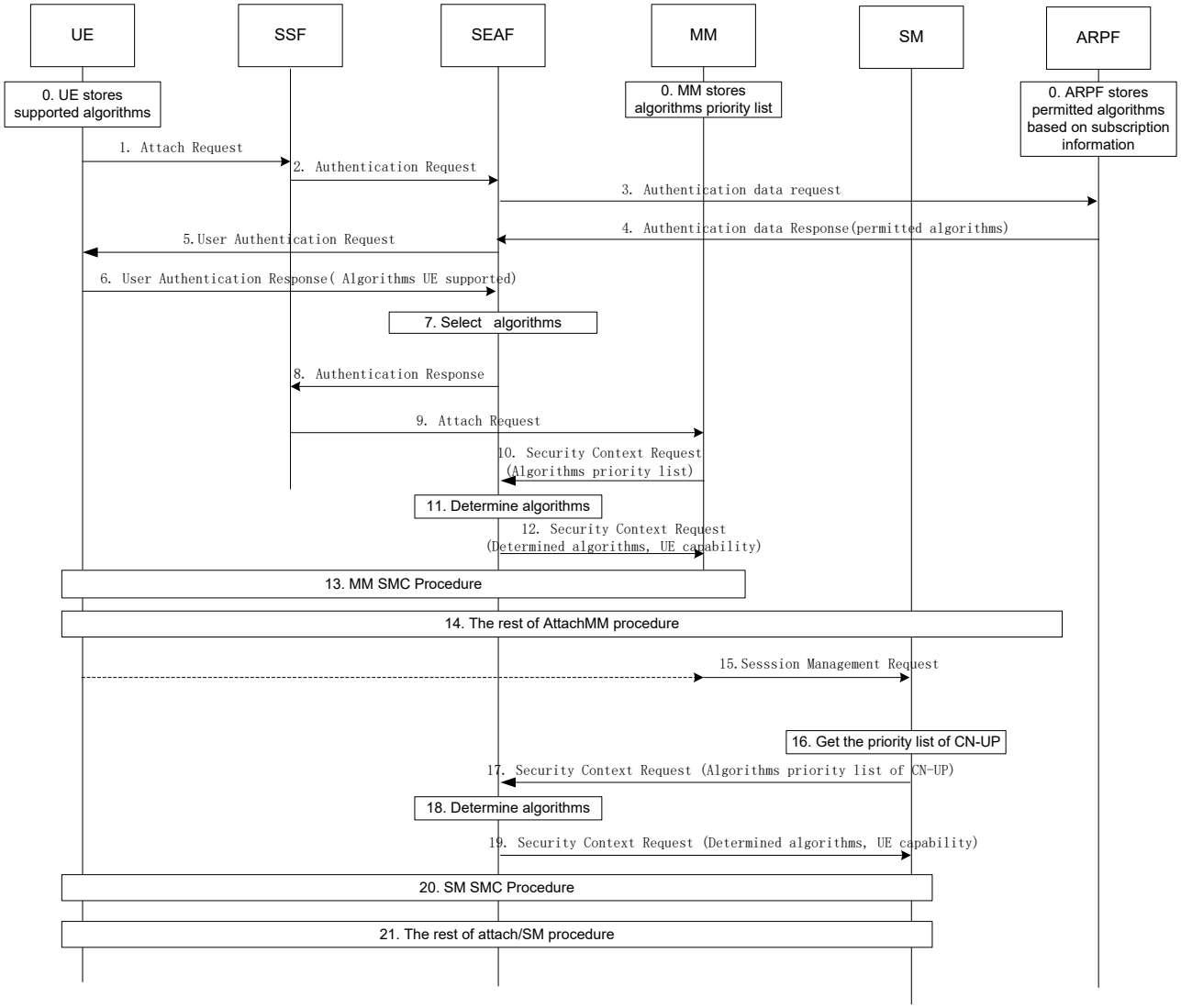


Figure 5.3.4.7.2-1 algorithm negotiation

0. UE stores supported algorithms that is part of the UE security capability, the MM stores an algorithm priority list and the ARPF stores permitted algorithms based on the subscription profile information.

1. UE sends an Attach Request to SSF

2. SSF sends an Authentication Request to SEAF.

3. SEAF sends an authentication data request to ARPF, which shall at least include the IMSI.

4. The ARPF response with authentication data response message. The permitted algorithms may be included in this message. The permitted algorithm is selected by ARPF based on the current UE's profile, e.g. the type of UE.

Editor's Note: It is ffs what information should be used for ARPF determining the permitted algorithms.

5. The SEAF sends User Authentication Request message to UE to perform mutual authentication.

6. After the UE authenticates the network, it will send User Authentication Response message to SEAF.This message also contains the algorithms UE supported.

7. The SEAF selects algorithms based on the UE supported algorithms and the permitted algorithms received from ARPF.

8. SEAF informs SSF the result of authentication.

Lenovo Ex. 1007
Page 267

9. The SSF forwards the attach request message to MM.

10. MM sends Security Context Request message to SEAF. The message at least includes the algorithms priority list belonging to MM and the UE identity.

11. SEAF compares the preferences of the MM and the selected algorithms from step7 to get the determined algorithms for MM which include one ciphering algorithms and one integrity algorithms.

12. SEAF responds to MM with Security Context Request message which includes determined algorithms and the UE security capability.

13. MM perform MM SMC Procedure with the NG UE. The messages shall be protected by keys and the determined algorithms.

14. UE and MM perform the rest of Attach MM procedure.

15. If the initial attach indicates that the SM procedure needs to be executed, the MM will forward the Session Management Request to the SM. If the initial attach does not contain SM procedure, then UE will send Session Management Request to SM some time later.

16. The SM gets the algorithm priority list of CN-UP.

NOTE: The current call flow assumes that the UP security terminates at CN-UP.

17. The SM sends Security Context Request message to SEAF including algorithms priority list of CN-UP.

18. SEAF compares the preferences of the CN-UP and the selected algorithms from step7 to get the determined algorithms for CN-UP which includes one ciphering algorithm and one integrity algorithm.

19. SEAF responds to SM with Security Context Request message which includes determined algorithms for CN-UP and the UE security capability.

20. SM performs SM SMC to enable UP security protection. At this point, all messages are integrity and confidentiality protected by keys just derived using the agreed upon algorithms.

21. The SM performs the rest of SM procedure or the rest of the attach procedure.

Editor's Note: Where NAS traffic terminates in the network should be aligned with SA2 architecture.

Editor's Note: It is FFS why put the UE security capability in UE authentication response message.

Editor's Note: It is FFS whether SEAF needs to keep status of UE supported algorithm list to server MM-SMC and later SM-SMC.

5.3.4.7.3 Evaluation

5.3.4.8 Solution #3.8: Key negotiation of dual connectivity to deal with the leakage of secret key

5.3.4.8.1 Introduction

This solution addresses the key issue #4.3 "Security aspests of dual connectivity" and key issue #2.2 "Reducing the impact of secret key leakage".

It refers in the key issue #4.3 that "an attacker may eavesdrop on traffic involved in dual connectivity", and requires in the key issue #2.2 that "anti-passive attack capabilities shall be provided if the pre-shared root key K_i is stolen". Therefore, this proposal provides a new solution to key negotiation in dual connectivity.

5.3.4.8.2 Solution details

This solution proposes a D-H based key negotiation between UE and gNB. Figure 5.3.4.8.2-2 shows the procedure of key negotiation.

Lenovo Ex. 1007
Page 268

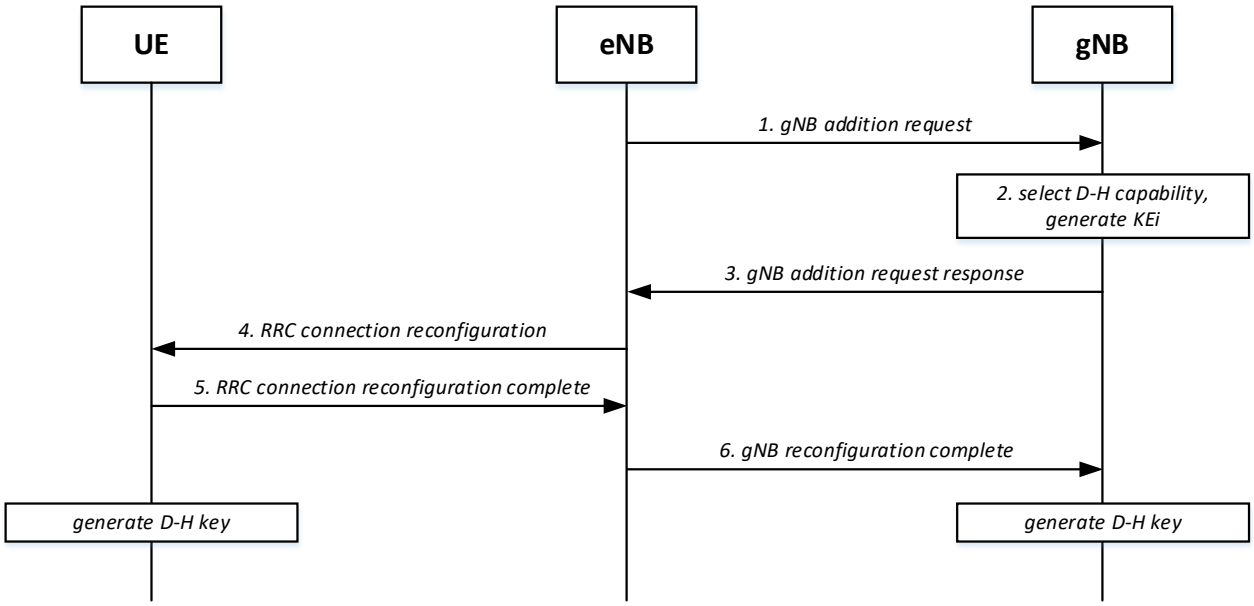


Figure 5.3.4.8.2-2: the procedure of the key negotiation

1. eNB sends a gNB addition request to gNB containing the D-H capability groups of UE.

2. gNB selects the D-H capability according to its pre-determined priority D-H capability list and UE supported D-H capability groups, and then generates KE_i the interim session key generated by gNB based on selected D-H capability.

3. gNB sends a gNB addition response to eNB containg the selected D-H capability and KE_i.

4. eNB sends the RRC connection reconfiguration containing the selected D-H capability and KE_i.

5. UE generates KE_r, the interim session key generated by UE, based on the selected D-H capability, and then sends a RRC connection reconfiguration complete containing KE_r to eNB. Meanwhile, UE can derive D-H key using KE_i and KE_r.

6. eNB sends the gNB reconfiguration complete containing KE_r to gNB with which gNB can derive the same D-H key.

Editor's Note: It is ffs how to use D-H key.

Editor's Note: How random numbers are transferred is FFS.

5.3.4.8.3 Evaluation

Editor's Note: Computational overhead aspect needs to be considered in the evaluation.

tba

5.3.4.9 Solution #3.9: Security Key Refresh Triggered by UE

5.3.4.9.1 Introduction

This solution addresses Key Issue #3.2.

5.3.4.9.2 Solution details

UE is equipped with a key refreshing policy. The policy indicate the risk level of the visited network, different risk level will trigger the refresh of different keys. Four risk levels are considered in the policy: High, Middle, Low, None. Three key refresh scenarios are introduced. These include reauthentication, main key refresh and CP/UP key refresh. When the risk is High, the UE will trigger reauthentication, and then refresh all the interface keys. When the risk is Middle, the UE will trigger main key refresh. CP/UP key will be refreshed if the risk is Low, and no key will be refreshed if the risk is None.

Lenovo Ex. 1007
Page 269

More specifically, detailed scenarios of different risk levels are discussed here.

- Once UE moves to a visited network with lax security policy. With high probability, the main key will be compromised if the key is used for a long time. In this situation, the risk is High, UE will trigger reauthentication periodically, to keep the main key fresh.
- In a visited network, if the key is used for a long time, the attackers recover the air interface key from the UE or AN. In such situation, the UE will trigger the main key refresh key procedure to refresh all the air interface keys.
- In a visited network, the attackers monitor the air interface of the UE and try to figure out the air interface key from the data transimitted. In this case, the risk is Low, and UE needs to refresh the air interface keys periodically.

The policy is defined by the home network and dynamically configured to UE during IAR/IAS in the MASA framework in solution #2.12. **Different levels are defined according to the geographical location of the serving network, the regularity, the home network policy, etc. The policy configure procedure is as follows.**

1-2 These are the original MASA flows that UE sends IAR request to the serving network and forwords it to the home network.

1. HSS define a refreshing policy based on the UE subscribe information, the geographical location of the serving network, the regularity, the home network policy etc.
2. HSS sends back the refreshing policy to the serving network possibly in an encrypted form..
3. The serving network forward the refreshing policy to UE in the IAS

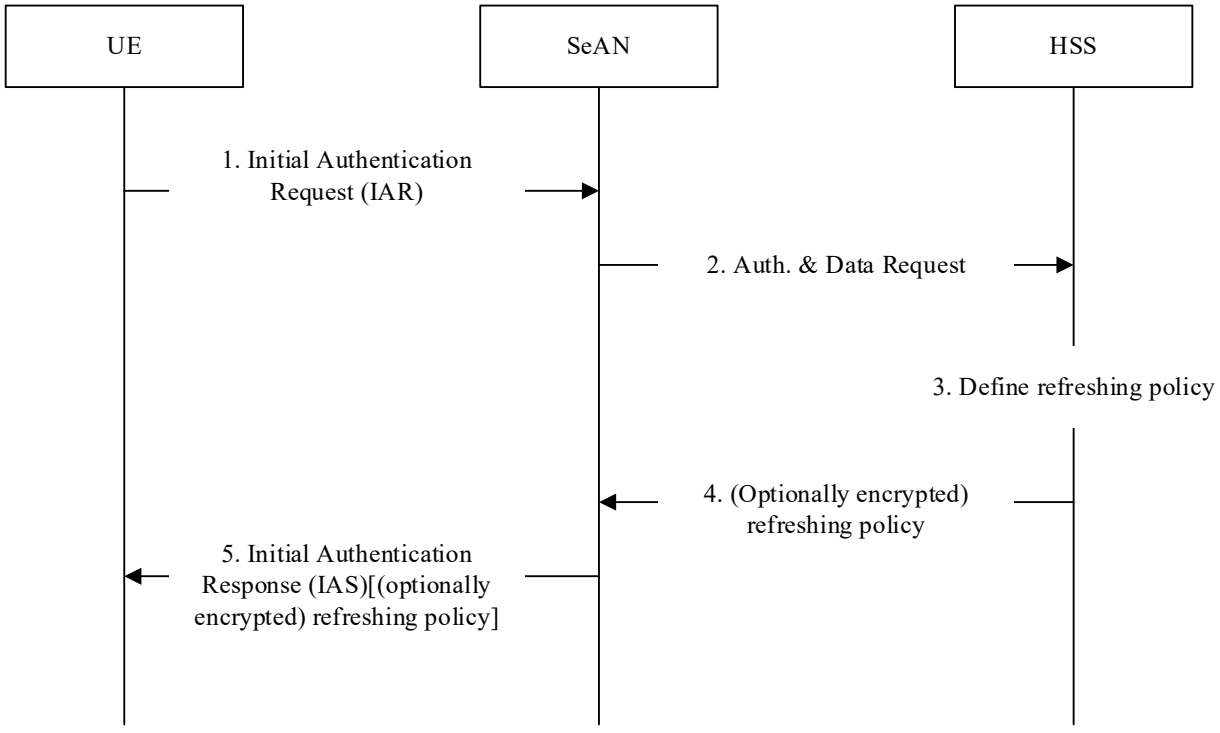


Figure 5.3.4.9.2-1

Editor's Note: Clarification and more details is needed on how the policy is delivered from home network to the NG-UE.

Editor's Note: This solution needs to be evaluated against current OMA DM and USIM OTA provisioning solutions.

The refreshing procedures are as follows:

- **Reauthentication** If the UE roams to a visited network with High risk as defined per the home network policy. UE will trigger the reauthencation procedure and refresh all the interface key.

Lenovo Ex. 1007
Page 270

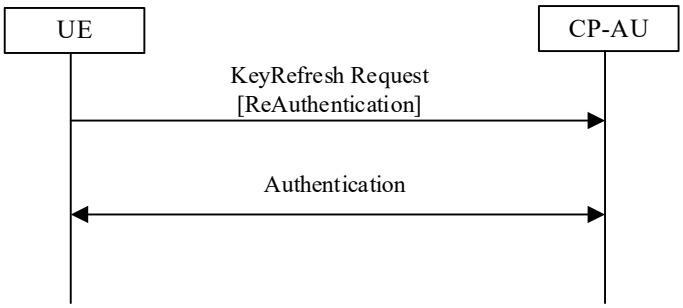


Figure 5.3.4.9.2-2

NOTE 1: The policy also defines a refresh period time X, which means if UE stay in the same visited network all the time, the key refresh procedure will be automatically triggered every time X.

NOTE 2: In case the time of reauthentication arrives and the UE is engaged in some important activities, it is a UE local policy to use a backoff timer to delay the reauthentication until a later time.

NOTE 3: the difference of the reauthentication here between 2/3/4G is that the authentication is initiated by UE and do not need to drop the connection.

- **Main Key Refresh** If the UE roams to a visited network with Middle risk, UE will trigger the main key refresh procedure and refresh all the derived keys from it. **The main key here means Kng in the NextGen key hierarchy or Kasme in 4G.** There are two ways to refresh the main key. One is based on DH key agreement and the other is based on key chain.

  a) The DH based key refresh procedure is according to solution #3.1 and described as follows.

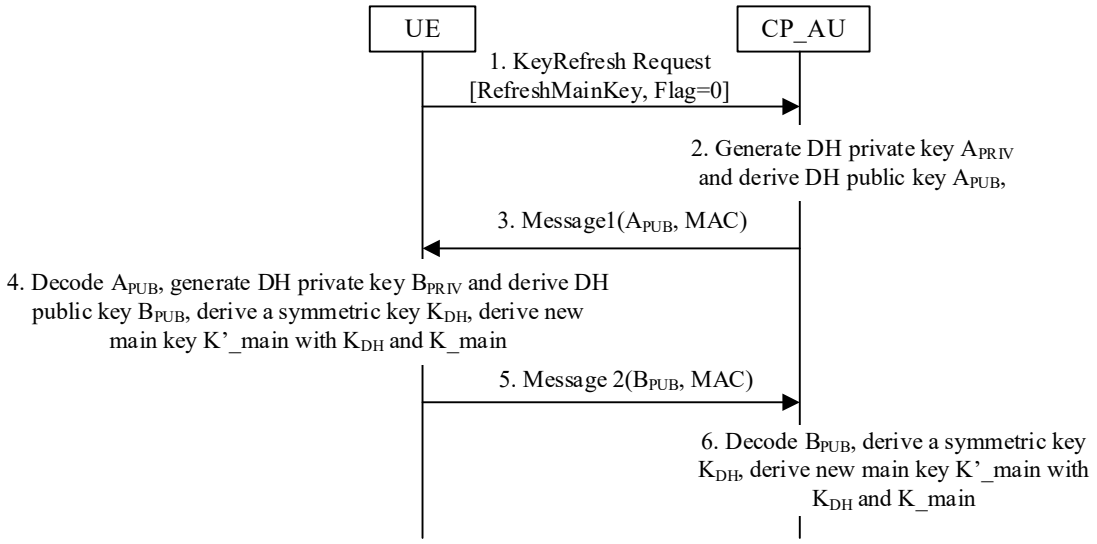


Figure 5.3.4.9.2-3

1. UE sends a KeyRefresh Request to CP-AU and contains indication RefreshMainKey and Flag=0 to use DH agreement protocol.

2. CP-AU generates a DH tuple A_{PUB} and A_{PRIV}.

3. CP-AU computes the MAC of A_{PUB} using the previous main key K_main, and sends A_{PUB} together with the MAC to UE.

4. UE first generates a DH tuple B_{PUB} and B_{PRIV}, then checks the MAC of A_{PUB} and computes the DH key K_{DH}. Finally, it refreshes the main key as K'_main = KDF(K_main, K_{DH}).

5. UE computes the MAC of B_{PUB} using the previous main key K_main, and sends B_{PUB} together with the MAC to CP-AU.

Lenovo Ex. 1007
Page 271

6. CP-AU first checks the MAC of A_{PUB}, and then computes the DH key K_{DH}. Finally it refreshes the key as K'_main=KDF(K_main, K_{DH}).

b) In the chain based procedure, UE and CP-AU maintain a counter MainKeyChainCounter, and the procedure is as follows.

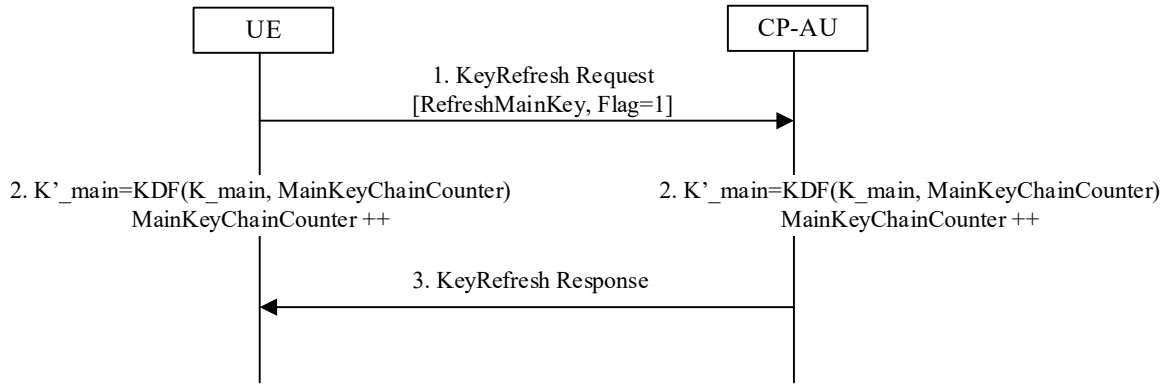


Figure 5.3.4.9.2-4

1. UE sends a KeyRefresh Request to CP-AU and contains indication RefreshMainKey and Flag=1 to use chain based method.
2. UE and CP-AU both refresh the main key as K'_main = KDF(K_main, MainKeyChainCounter), and the counter will add 1 index.
3. CP-AU returns a KeyRefresh Response message to UE.

- **CP/UP key refresh** If the UE roams to a visited network with Low risk, UE will trigger the CP/UP key refresh procedure and refresh all the derived keys from it. There are two ways to refresh the CP/UP key. One is based on DH key agreement and the other is based on key chain.

a) The DH based key agreement protocol is according to solution #3 and is similar to the main key refresh procedure except using the K_CP/K_UP, as follows.

1. The CP case:

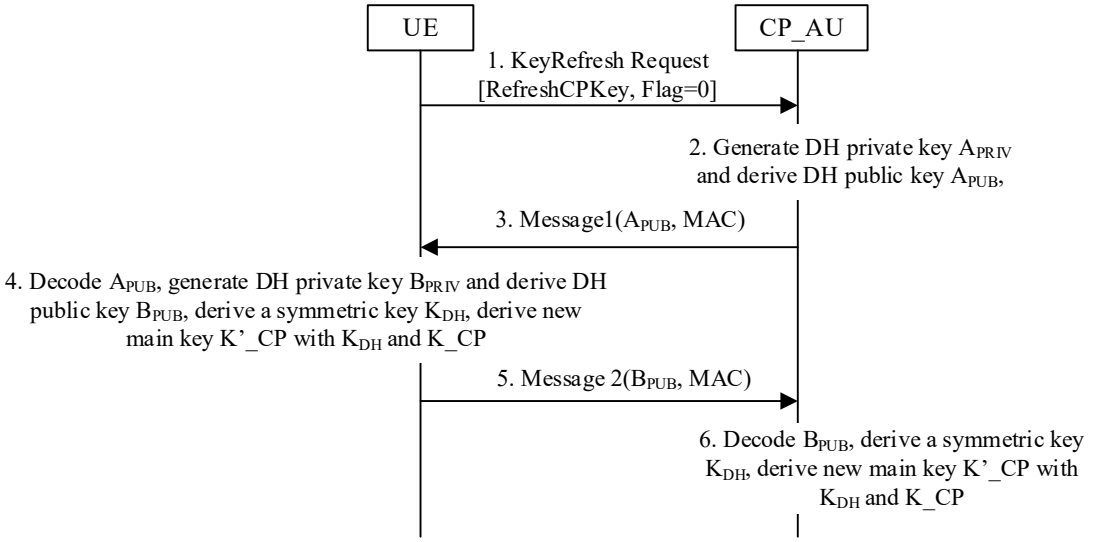


Figure 5.3.4.9.2-5

2. The UP case:

Lenovo Ex. 1007
Page 272

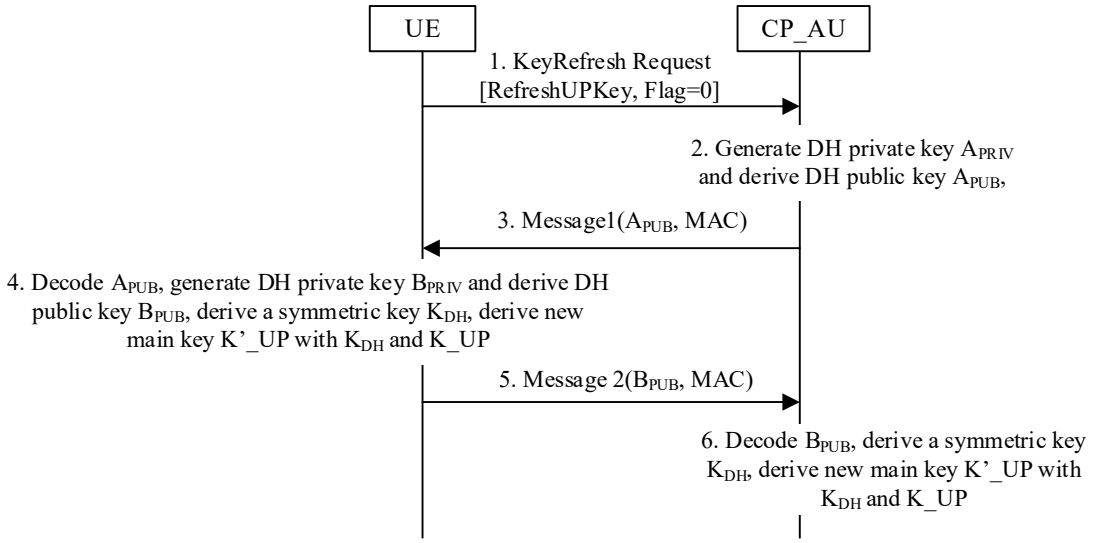


Figure 5.3.4.9.2-6

b) The chain based protocol is similar to the main key refresh procedure except using K_CP, CPKeyChainCounter and K_UP, UPKeyChainCounter, as follow.

1. The CP case:

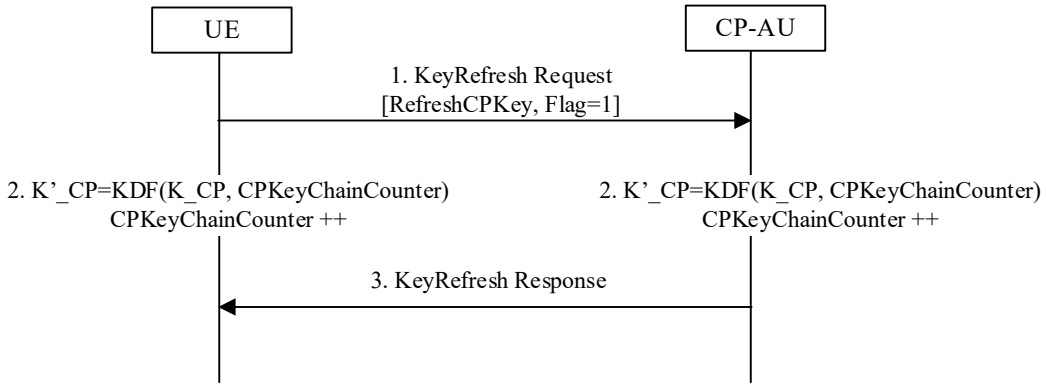


Figure 5.3.4.9.2-7

2. The UP case:

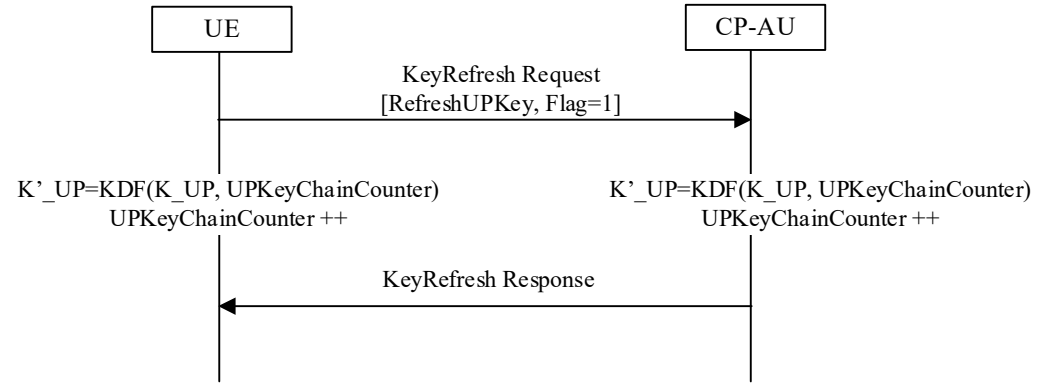


Figure 5.3.4.9.2-8

5.3.4.9.3 Evaluation

tba

Lenovo Ex. 1007
Page 273

5.3.4.10 Solution #3.10: void

5.3.4.11 Solution #3.11: Binding of keys to an authentication session with a serving network in NextGen systems

5.3.4.11.1 Introduction

This solution addresses Key Issue #3.1 (Theft of keys). Keys can be stolen not only by passive eavesdropping of communication links between the home and serving network nodes but also via triggering a genuine serving network requesting the keys from the home network on behalf of the UE when the UE is not present at the serving network. Such stolen keys can be used by an attacker to impersonate the legitimate serving network and intercept UE's communication traffic.

Editor's Note: The threat needs to be clarified: Who triggers? Who is the attacker? If the attacker is not the genuine network how does the attacker get hold of the keys if not by eavesdropping on communication links? If the attacker is the genuine network what exactly is the associated risk? The present solution needs further justification based on a thorough risk analysis.

This solution describes an enhanced authentication protocol that binds an authentication session root key (K_{ASRK}) to the authentication session.

Editor's Note: The notion of authentication session is not defined in TR 33.899 nor in TS 33.401. Who is involved in this authentication session, UE and serving network, or UE, serving network and home network?

Such binding ensures the UE that the current authentication session and corresponding communication with the serving network is authorized by the home network. This binding to the authentication session also has the affect of binding the authentication to a serving network

Editor's Note: It seems that two protocol properties are mixed here: it is easily possible that an MSK is bound to the authentication session (if the meaning is that the MSK was generated after the UE sent a certain freshness parameter), but there is no serving network authentication, cf. example of EAP-AKA. It is the other way around for EPS AKA: the visited network can request an authentication vector independent of any request from the UE, but serving network authentication is guaranteed.

NOTE: The solution ensures the UE that the current authentication session and corresponding communication with the serving network is authorized by the home network when used with EPS AKA. Similarly, it implicitly ensure that the home network that any authentication vector sent can only be used for the present session.

Editor's Note: It needs further clarification whether the home network has any notion of authentication session.

Editor's Note: It is FFS which other authentication methods require the additional mechanisms to bind the key to the authentication session and/or serving network.

5.3.4.11.2 Solution details

Binding an authentication session root key (K_{ASRK}) to a serving network is achived based on an attach request with an information element (IE) that is encrypted by the UE and can only be decrypted by the AUSF in the home network. The encrypted IE contains the serving network identifier (SNID) and a session specific key encryption key (KEK) generated by the UE. The SNID provided by the UE (i.e., not by the serving network) is used by the AUSF to bind a K_{ASRK} to the serving network. The KEK is used to bind K_{ASRK} to the authentication session in such a way that the NG-UE who initially generated the KEK can be confirmed with the knowledge of the KEK by the serving network during the authentication procedure.

Binding K_{ASRK} to the serving network prevents an attacker who acquired the messages exchanged between the AUSF and the serving network from masquerading the serving network identified by the SNID.

Editor's Note: This statement suffers from a lack of clarity in the threat analysis, cf. first Editor's note in 5.3.4.11.1. If the attacker obtains any secret information by eavesdropping then confidentiality protection in the interconnection network would seem sufficient. If the genuine serving network acts as an attacker then there is no issue of masquerading as the serving network cannot masquerade as itself.

Lenovo Ex. 1007
Page 274

And, binding K_{ASRK} to the KEK prevents an attacker who obtains the authentication session root key (or other information used by the serving network to authenticate the NG-UE, e.g., an authentication vector in LTE) from masquerading the serving network after the authentication procedure associated with the KEK has been completed.

Editor's Note: This seems impossible to accomplish as anybody knowing the K_{ASRK} will also know the derived keys and can, hence, e.g. eavesdrop on the radio link long after the authentication procedure has been completed, until the K_{ASRK} is refreshed.

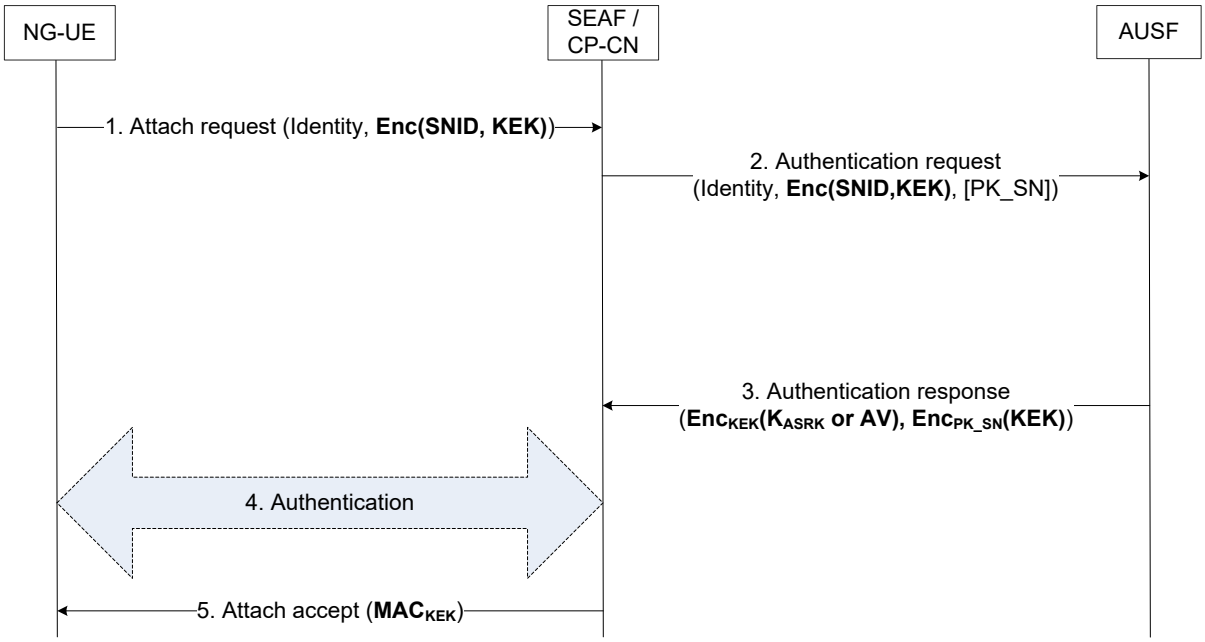


Figure 5.3.4.11.2-1: Attach procedure with intrinsic serving network and session binding when using EPS AKA

1. The NG-UE sends an attach request to the serving network with UE identity and an encrypted information element (IE) that contains the serving network identity (SNID) to which the NG-UE is attaching and a key encryption key (KEK) that is generated by the NG-UE.

NOTE 1: either the AUSF's public key or a shared key between the NG-UE and the AUSF can be used as an encryption key. In case that the AUSF's.public key is used for encryption, the NG-UE shall be provisioned with the AUSF's public key or certificate.

Editor's Note: SEAF and CP-CN are shown in the same box since the interface between them has not been defined.

2. The SEAF/CP-CN adds its certificate (or public key) to the information received from the NG-UE and sends an authentication request to the AUSF. The AUSF obtains the SNID and the KEK by decrypting the authentication request message.

NOTE 2: If the certificate or public key associated with SNID is stored in the AUSF, it need not be included in the authenetication request.

3. The AUSF sends the authentication response that includes an encrypted authentication session root key (K_{ASRK}) and an encrypted KEK. The K_{ASRK} is encrypted using the KEK and the KEK is encrypted using the public key of the serving network.

NOTE 3: Only the serving network (node) that owns the private key associated with the public key used for the KEK encryption can decrypt the KEK and subsequently decrypt the K_{ASRK} using the KEK.

NOTE 4: In EPS AKA, the AUSF includes an authentication vector (AV) in the authentication response so that the serving network can perform authentication with the NG-UE. In this case, the AV is encrypted using the KEK.

The SEAF/CP-CN obtains the KEK using its private key and subsequently AV or K_{ASRK} using the KEK.

Lenovo Ex. 1007
Page 275

4. The SEAF/CP-CN authenticates with the NG-UE based on the AV.

5. The SEAF/CP-CN integrity-protects the attach accept message using the KEK and sends the integrity-protected message to the NG-UE. If the NG-UE successfully verifies the attach accept message, then the NG-UE can be confirmed with the binding of K_{ASRK} to the current authentication session and the binding of the K_{ASRK} to the serving network, based on the SEAF/CP-CN's knowledge of KEK.

NOTE 5: Integrity protection of this message using KEK assures to the UE that the AVs used for the authentication in step 4 is freshly provided by the home network to this serving network for the Attach Request in step 1. The step 5 can be performed as part of the step 4.

5.3.4.11.3 Evaluation

The risk of a genuine serving network obtaining authentication vectors ahead of an Attach request by the UE seems quite limited, as shown by the evaluation section of solution 2.22 Furthermore, even the solution presented in this clause cannot completely mitigate the risk of a genuine serving network abusing authentication vectors or root keys, cf. online variant of the attack in the evaluation section of solution 2.22

The present solution is not needed for AKA-based authentication methods:

It appears that EPS AKA* in solution 2.22 suffices to mitigate the risk of a serving network obtaining authentication vectors when the UE is not present in the serving network.

Even if it is decided that a stronger mitigation of this risk is needed the method of choice would rather be EAP-AKA', a well-proven method, than a totally new protocol that seems to have no stronger security properties than EAP-AKA', but is considerably more complex.

It is also pointed out that, for enhancing EPS AKA according to the intention of the present solution, a much simpler solution would work: the UE includes an unencrypted random value in the Attach request, which the serving network forwards to the home network. The home network then includes this random value in the computation of KASME from CK, IK, together with the serving network identity. This works as CK, IK never leave the home network in EPS AKA.

The present solution is not needed for EAP-based authentication methods:

. For EAP-based authentication methods, the simpler solution 2.19 where the AUSF calculates KSEAF from the EMSK in a way that KSEAF is bound to the serving network identity seems preferable to the present solution for reasons of complexity.

The present solution is therefore potentially useful only for non-AKA, non-EAP authentication methods. However, it is not clear whether 5G authentication will support such methods.

5.3.4.12 Solution #3.12: "Binding a serving network public key into the derivation of the radio interface session keys"

5.3.4.12.1 Introduction

This solution addresses Key Issue #3.1: Interception of radio interface keys sent between operator entities.

5.3.4.12.2 Solution details

The solution is identical to solution 2.6.

5.3.4.12.3 Evaluation

Solution #10.2 "Public-key encryption of keys in authentication vectors" also addresses key issue 3.1. It has the advantage over solution 3.12 that it works under the same prerequisites as, but does not affect the radio interface, which is a scarce resource.

Lenovo Ex. 1007
Page 276

5.3.4.z Solution #3.z: <solution name>

5.3.4.z.1 Introduction

Editor's note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the security area.

5.3.4.z.2 Solution details

5.3.4.z.3 Evaluation

5.3.5 Conclusions

Editor's note: This clause will contain the evaluation between the solutions, and the conclusions made by SA3.

5.4 Security area #4: RAN security

5.4.1 Introduction

The security area "RAN security" can be considered to consist of the high level security models depicted in Fig 5.4.1-1 and Fig 5.4.1-2 based on the New Radio study progress in TR 38.804 [62] and TR 38.801 [72], and from the implicit threat model used in LTE.

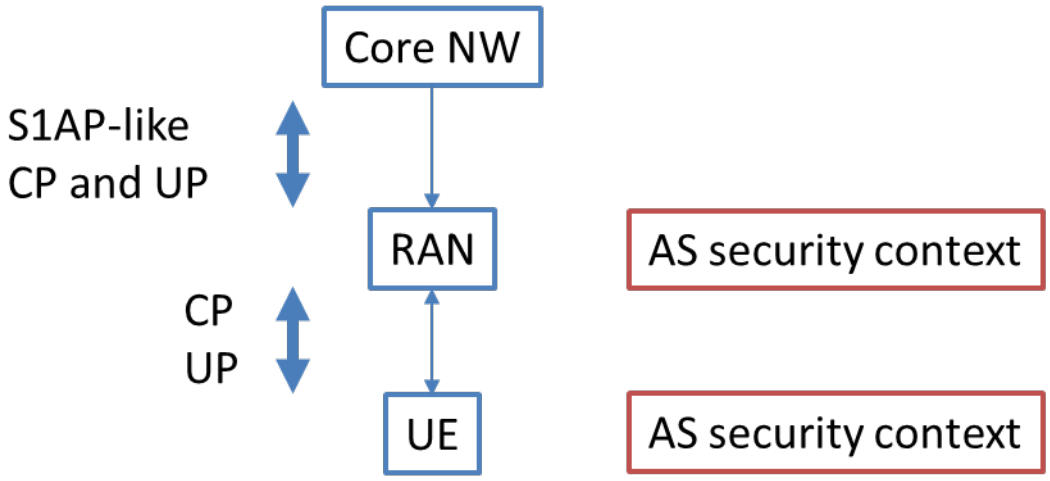


Figure 5.4.1-1. High level static security model of RAN.

Figure 5.4.1-1 depicts a static view of the possibly highest level model of the RAN interacting with the UE and the core network.

Lenovo Ex. 1007
Page 277

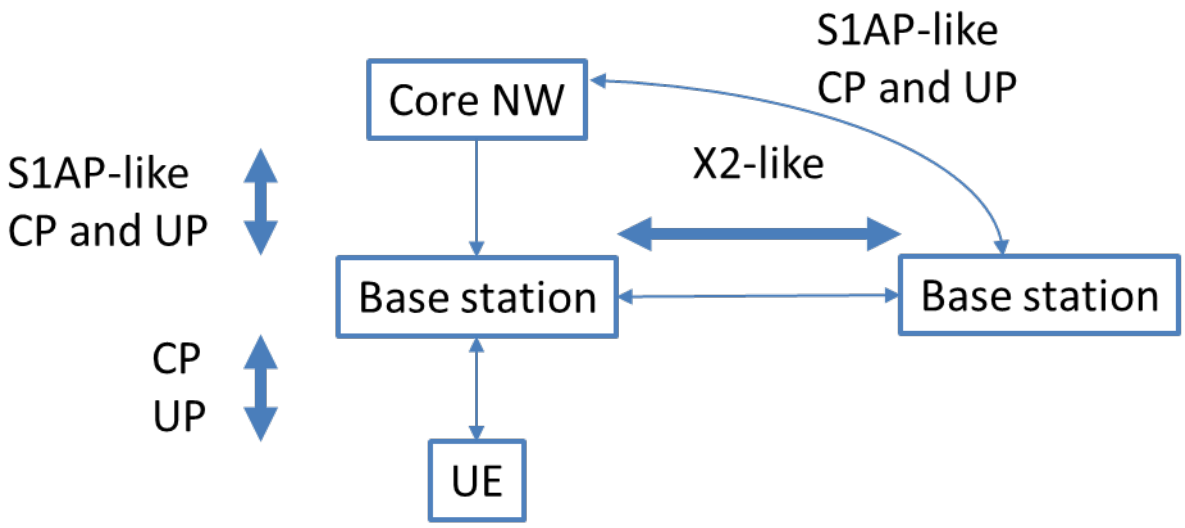


Figure 5.4.1-2. A more granular and dynamic view of the system. The figure does not take into account that base stations may be gNBs or eNBs. Neither does it show whether the UE is connected via NR or (e)LTE.

Figure 5.4.1-2 provides a more granular view of the system. Here, dynamic aspects, such as mobility, appear. The figure shows two base stations, but does not take into account whether they are gNBs or eNBs. Neither does the figure depict whether the UE is connected via NR or (e)LTE radio access.

From these security models it is possible to collect which security functions need to be defined in RAN security area for different functions and events. Some of the security functions may be covered by or may be overlapping with existing key issues and solutions also elsewhere in the TR. This is not seen as a problem as the structure of the TR is such that security are inherently overlapping. The purpose of this introduction is to obtain an overview of what security functions are required, so that it is possible to deduce whether RAN security area has covered the entire problem space, including similar functionality that exists in LTE, but also functionality that is new compared to LTE security.

In particular this security area deals with aspects such as:

- Protection of control plane and user plane between the UE and RAN.
- Protection of control plane and user plane between the RAN and NGC. This is covered by KI 1.5 and 1.6.
- Protection of control plane and user plane between base stations.
- Negotiation of security algorithms for e.g.
  - state changes
  - handovers
  - idle mode mobility
  - dual-connectivity cases
- radio link failure-Handling of AS security context for e.g.
  - state changes
  - handovers
  - idle mode mobility
  - dual-connectivity cases
  - radio link failure
- DoS attacks towards the network infrastructure or against others devices/users, such as

Lenovo Ex. 1007
Page 278

  - the overload of signalling messages.
  - jamming of radio interface

- Privacy aspects, such as:
  - the possibility for an attacker to link temporary identities with real user identities at any time during the network operation
  - the use of predictable radio identities.
  - the persistence of radio identities (not refreshed) when a radio procedure or a state transition occurs.

5.4.2 Security assumptions

Editor's Note: This clause will document security assumptions related to each security area.

5.4.3 Key issues

5.4.3.1 Key Issue #4.1: AS security during RRC idle mode

5.4.3.1.1 Key issue details

In the LTE system, UE obtains some services in the RRC idle state. In the RRC idle state, UE acquires the system information from the camped cell and uses them to receive paging and obtain other services such as MBMS, D2D, etc. in RRC idle state. When the UE select a cell in RRC idle mode, it does not validate whether the eNB is authentic or fake. As a result, UE may camp to a rogue cell leading to denial of services (such as public safety warnings, incoming emergency calls, real-time application server push services, proximity services, etc.).

So far the mobile communication system has been focused on providing AS secure communication in the RRC connected state and security aspects in RRC idle state are not considered. As some services are offered to the UE in the RRC idle mode through System Information Blocks, it is necessary to consider and ensure the security of the messages carrying the service/service information, even when the UE is in RRC idle mode for the next generation systems.

5.4.3.1.1 Security threats

If the UE camps on a fake cell during RRC Idle state (and there is no authenticity verification done), then the attacker can successfully mount DoS attack on the UE for the following services obtained when the UE is in RRC Idle state:

a) Detection of mobile terminated services (for example, incoming calls, connection request from application servers, etc.), system information change;

b) UE interested in the D2D service can acquire the broadcasted system information and uses the radio resources configured via the system information for the D2D discovery/communication transmission/reception;

c) UE interested in the MBMS reception can acquire relevant system information and uses the control information indicated in the system information for MBMS reception.

Mounting of these attacks without knowledge of UE is highly possible, especially in auditoriums, play grounds, shopping malls, corporate buildings, conference venues and theatres. Unless the UE initiates any service, the UE will not come out of the fake cell and all the mobile terminated services and service information are blocked by the fake cell.

5.4.3.1.3 Potential security requirement

- Next generation system should provide a means to ensure a UE in idle state is able to determine the authenticity of a cell.

Editor's Note: It should be studied to have a possible solution for the above requirement with minimal impact to the system.

Lenovo Ex. 1007
Page 279

5.4.3.2 Key issue #4.2: Security requirements on gNB

5.4.3.2.1 Key issue details

The gNB may, in contrast to other nodes, in many cases be located in a vulnerable location. Hence security requirements on the gNB may be in scope of 3GPP, even if security requirements on other nodes are up to implementation.

In the LTE system, there are a number of security requirements on the eNB, covered in clause 5.3 of [a]. There are security requirements for eNB setup and configuration, for key management inside eNB, for handling User plane data and Control plane data, and for the secure environment of the eNB.

Possible security requirements on the gNB depend on the NG architecture. The security requirements on gNB may be similar to the security requirements on eNB, but differences between the EPS and the NG architecture may also result in different requirements for gNB compared to eNBs. Furthermore, according to TR 38.801[72] clause 5.3, co-sited deployment of eNB and gNB is also possible, either as part of the same base station or as multiple base stations at the same site. For deployments where eNB and gNB are the same base station, the security requirements on eNBs and gNBs may be both relevant, and even identical.

Security requirements on the gNB should take possible virtual deployments into account and be formulated in a way that is applicable for both virtual and non-virtual deployments.

5.4.3.2.2 Security threats

An attacker may modify the gNB's setting or software configurations via local or remote access.

An attacker may obtain keys, user data or user identifiers from the gNB.

5.4.3.2.3 Potential security requirements

Editor's Note: The potential security requirements are ffs.

Editor's Note: The requirements in the present clause needs to take in consideration requirements in clause 5.3 of TS 33.401 as the architecture for NextGen system becomes more complete.

- gNB configuration management, whether local or remote, shall be authorized.
- gNB shall ensure boot and run-time integrity of its platform.
- gNB software updates shall be applied only after successful integrity and origin verification.
- Secure storage and processing of sensitive data in gNB shall be assured.

5.4.3.3 Key issue #4.3: Security aspects of dual connectivity

5.4.3.3.1 Key issue details

5.4.3.3.1.0 General security aspects of dual connectivity

The next generation system is expected to cover different cases of dual connectivity. The purpose of this key issue is to study security aspects of dual connectivity in the next generation system.

Dual connectivity in the next generation system may involve not only next generation nodes, but also LTE radio access and possibly also the EPC. The options that may be relevant to study are listed in Table 5.4.3.3.1-1.

Lenovo Ex. 1007
Page 280

Table 5.4.3.3.1-1: Architecture options for dual connectivity

Option	Main node	Secondary node	Core network
2	gNB	gNB	NextGen core
3	eNB	gNB	EPC
4	gNB	eNB	NextGen core
5	eNB	eNB	NextGen core
7	eNB	gNB	NextGen core

Note: Option 3 refer to Option 3 and its variants

Most of the scenarios involve both the LTE system and the next generation system. Similarities and differences between the systems will hence influence the study of the security aspects of dual connectivity. For example, the following aspects may have an influence:

- Similarities and differences in the PDCP layer of LTE and corresponding layer(s) in the next generation system;
- The endpoint of user plane data encryption in the next generation system; and
- Possible user plane integrity protection in the next generation system.

The study of the security aspects of dual connectivity will of course also depend on the technical work on dual connectivity.

5.4.3.3.1.1 Security aspects for deployment scenario of option 3

Figure 5.4.3.3.1.1-1 shows the deployment scenario of Option 3 in which the eNB is the main node and gNB is the secondary node, and both are connected to the EPC. This option is being discussed in key issue and solution 18 "Interworking and Migration", Annex J "Deployment Scenarios" of TR 23.799 and section 7.1 "Tight interworking between new RAT and LTE" of TR 38.801. In option 3, a UE, which has dual connectivity to eNB in LTE and gNB in NR (NextGen Radio), accesses EPC network.

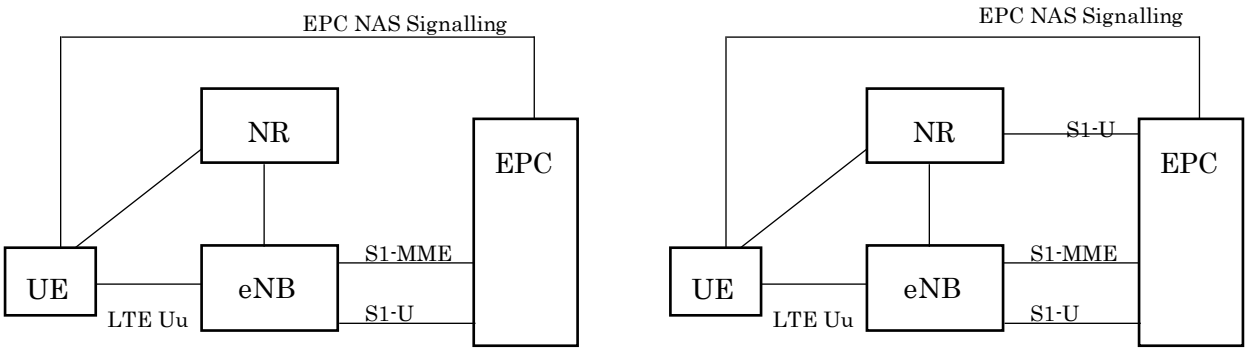


Figure 5.4.3.3.1.1-1: Deployment Option 3 (TR 23.799 v 2.0.0)

5.4.3.3.2 Security threats

- An attacker may eavesdrop on traffic involved in dual connectivity at the secondary eNB or gNB.
- An attacker may impersonate an eNB, gNB or UE involved in dual connectivity at the secondary eNB or gNB.
- An attacker may attack a dual connectivity traffic flow by injecting wrong packets in to a traffic flow.
- U-plane traffic sent through NR could be compromised.
- The communication between EPC and NR, i.e. between gNB and EPC via eNB or directly, can be compromised.

Editor's note: It's FFS whether U-plane security termination point is in NR or SGW.

Lenovo Ex. 1007
Page 281

5.4.3.3.3 Potential security requirements

- The offloaded link on the secondary eNB or gNB should have the same or better level of protection compared to the main link of the UE. For this reason, it shall be possible for the master eNB or gNB to control the security keys and security parameters for the dual connectivity link.
- It shall be possible for the master eNB or gNB to indicate the type of protection ie integrity or encryption to be applied on a DRB basis to the secondary eNB whenever new DRBs are added .
- The security keys (integrity and encryption keys) on the same secondary eNB or gNB should not be predictable between different instances of dual connectivity while the UE remains connected to the same main eNB or gNB.
- It shall be possible to update the security keys on the secondary eNB or gNB when the main eNB or gNB meets the trigger conditions or when secondary eNB or gNB meets the trigger conditions.
- Authorization mechanism for UE to access NR network shall be provided.
- Integrity, confidentiality and replay protection shall be provided for communications between NR and EPS nodes.

5.4.3.4 Key issue #4.4: Security aspects of inactive mode mobility

5.4.3.4.1 Key issue details

The Next Generation system may include inactive mode UE mobility. The scope of this Key issue is the security aspects of this mobility procedure.

Editor's Note: It is ffs in RAN2 whether there will be an ECM-CONNECTED/RRC_INACTIVE state. Hence, it is ffs whether security aspects of inactive mode mobility need to be studied as well.

5.4.3.4.2 Security threats

5.4.3.4.3 Potential security requirements

5.4.3.5 Key issue #4.5: Security aspects of RAN-WLAN aggregation/integration

5.4.3.5.1 Key issue details

The Next Generation system is expected to include WLAN aggregation. See clause 4.1.3 in TR 38.804 [62] and especially Figure 4.1.3-1 in the same clause for possible deployment scenarios. The scope of this key issue is the security aspects of WLAN aggregation.

Editor's Note: In RAN working groups, interworking/aggregation with WLAN is down-prioritized until March 2017.

5.4.3.5.2 Security threats

5.4.3.5.3 Potential security requirements

5.4.3.6 Key issue #4.6: User plane DoS attacks

5.4.3.6.1 Key issue details

NextGen systems are expected to host diverse services and to provide connectivity/services to a massive amount of devices simultaneously. Such devices include IoT devices that send small amount of data *infrequently*. The key issue in subclause 5.4 of TR 23.799 [2] is on session management for those IoT devices.

NOTE: This attack was not dealt with in LTE, but the introduction of user plane integrity in NextGen allows the possibility to protect against this attack.

Lenovo Ex. 1007
Page 282

Some solutions in TR 23.799 are proposing the absence of user plane AS security. However, in the absence of user plane AS security, the network may be exposed to denial of service (DoS) attacks. It is desired for the NextGen systems to have a way to deter or filter bogus user plane packets injected by unauthorized devices or applications (e.g., malware). At the same time, in the normal operations (i.e., in case of no identified ongoing attacks), the NextGen network should support efficient transmission of small data by IoT devices as intended.

5.4.3.6.2 Security threats

In the absence of integrity protection being provided by AS security, attackers can launch DoS attacks on the user plane against the NextGen network by sending bogus packets to the network. Though the bogus packets may be identified and filtered at the network node that can verify packets based on the security context of a device, the path towards the network node can still be flooded by bogus packets. This would lead to denial of service or at least throughput degradation caused by congestion to devices whose traffic shares the same network links as that of the bogus packets.

5.4.3.6.3 Potential security requirements

The NextGen system should support an efficient method to filter bogus user plane packets at an access node to prevent DoS attacks for uses cases where there is no per UE AS layer user plane security context.

5.4.3.7 Key Issue #4.7 Key handling in RRC inactive state to RRC active state transition

5.4.3.7.1 Key issue details

In additional to RRC idle and RRC connected, inactive connected state has been introduced into the new RAN. In the inactive connected state, the connection (both CP and UP) between RAN and Core should be maintained, and the AS context should be stored in RAN and the UE. As forward security defined in TS 33.401, for a eNB with knowledge of K_{eNB}, shared with a UE, it shall be computationally infeasible to predict any future K_{eNB}. Similar with LTE, the next generation network also needs forward security during RRC state transition. Consequently, key handling mechanism in RRC inactive connected state to RRC connected state transition is needed.

5.4.3.7.2 Security threats

For a gNB with knowledge of K_{AN}, shared with a UE, if it can predict any future K_{AN} that will be used between the same UE and another gNB, the confidentiality of messages may be broken.

5.4.3.7.3 Potential security requirements

If a UE transits to RRC connected state from RRC inactive connected state when connecting a new (another) gNB, new K_{AN} shall be derived between the UE and the new gNB.

5.4.3.8 Key issue #4.8: void

5.4.3.9 Key issue #4.9: Security aspects of NG2 handover

5.4.3.9.1 Key issue details

The logical nodes in the new RAN of the NextGen system are interconnected with each other through a new RAN interface named the Xn interface. The control plane interface of these RAN nodes with the Next Generation Core (NGC) is named the NG2 interface.

During handover from one RAN node to a different RAN node, the two RAN nodes may not be interconnected via the Xn interface. In such case it is expected that a NG2 handover take place where the NGC needs to be involved, similar to the S1 handover in LTE. Further, the NG2 handover might involve the change of the NGC node (e.g., AMF) as well.

At S1 handover in LTE, backward and forward securities are achieved as follows [TS 33.401 [y]]:

LTE-RAN:

Supports both backward and forward security:

Lenovo Ex. 1007
Page 283

-Target eNB has no knowledge of the security keys (KeNB and keys derived from it) used in source eNB.
-Source eNB has no knowledge of the security keys (KeNB and keys derived from it) used in target eNB.

EPC-Core Network:

-Source MME transfers the Kasme and a fresh {NH, NCC} pair to target MME. There is no support of 1 hop forward security.
-Target MME has knowledge of the Kasme and the derived NAS keys from it, used in source MME. There is no support of 1 hop backward security

It is important for the NextGen systems to maintain or improve (if necessary) the existing protection mechanism in the LTE.

NG Systems:

One difference in NG Systems is related to handover scenarios involving AMF changes. In fact, in legacy systems, the MMEs are trusted and hence during MME change, the UE security context is handed over unchanged from the source and the target MME. The target MME may though select other NAS algorithms but this change does not affect the AN security context and will be taken to use during a NAS SMC procedure following the handover completion.

Based on the above description:

1. First the security handling in legacy systems is based on the assumption that the MME is the trust anchor in the core network.

2. Second, a change in the NAS algorithms is only effective after the NAS SMC procedure.

3. Third, a NAS SMC is only possible upon completion of the handover and requires the target MME and the UE to undertake a tracking area update procedure.

It is worth noticing, that in NG Systems a SEAF function has been introduced to cater for the flexibility in the deployment of AMFs. In other terms, from a security perspective, AMFs might be deployed in domains where the risk of compromise, e.g. because of exposure, could vary. This implies that AMFs might not qualify as true security anchor in the same way as the MME does in legacy systems. Therefore, other mechanisms than in 1 should be investigated in order to take into account this aspect. In relation 2 and 3, it is worth the effort to investigate how the legacy mechanism can be improved in order to avoid running a NAS SMC-like procedure after the handover. This would save on signaling.

This key issue concerns the security aspects of the NG2 handover.

5.4.3.9.2 Security threats

If the NG2 interface is not security protected, then an attacker could eavesdrop or insert or modify the security key and the security parameters transferred on the NG2 interface.

If the target AMF is compromised and the UE security keys do not have the property of backward security, then an attacker would be able to decrypt the previous data exchanged between the UE and the network.

If the source AMF is compromised and the UE security keys do not have the property of forward security, then an attacker would be able to decrypt the future data exchanged between the UE and the network.

5.4.3.9.3 Potential security requirements

Editor's Note: It is FFS if forward security is achievable or even necessary in this scenario.

- The 5G key transferred from source AMF to target AMF (similar to Kasme in LTE) shall have property of backward security.

- Integrity, confidentiality and replay protection shall be provided for communications on the NG2 interface.

Lenovo Ex. 1007
Page 284

5.4.3.10 Key issue #4.10: Security aspects of sidehaul interfaces

5.4.3.10.1 Key issue details

This key issue covers the security aspects of the sidehaul interfaces in the Next Generation systems, which include the following interfaces [TR 38.801]:

- Xn interface: It denotes the interface between the NGC-connected RAN nodes, either gNBs or eLTE eNBs.
- Xx interface: It denotes the interface between the EPC-connected gNB and NGC-connected eLTE eNB.

5.4.3.10.2 Security threats

- If the Xn/Xx interfaces are not confidentiality protected, an attacker could eavesdrop on the control/user plane traffic transferred on them.
- If the Xn/Xx interfaces are not integrity protected, an attacker could modify the control/user plane traffic transferred on them.

5.4.3.10.3 Potential security requirements

- Integrity, confidentiality, and replay protection shall be provided for communications on the Xn/Xx interface.

5.4.3.11 Key issue #4.11: Flexibility to retain or to change AS security keys

5.4.3.11.1 Key issue details

In LTE systems, the root key for AS security is called K_{eNB}, which is derived by the MME and is given to the eNB. The actual AS security keys for encryption and integrity-protection, i.e. K_{RRCenc}, K_{RRCint}, and K_{UPenc}, are derived from the K_{eNB}. Every time the K_{eNB} is refreshed, new K_{RRCenc}, K_{RRCint}, and K_{UPenc} are generated. The refreshment of the root key can be triggered by one of the following events:

- Radio link failure (RLF);
- RRC state transition (e.g., UE transitions from RRC IDLE to RRC CONNECTED); and
- Handover (UE is in and remains in RRC CONNECTED).

It is expected that there will be also AS-like security keys in the NextGen system. This key issue addresses the refreshment of these security keys.

An important security practice is to avoid using the same security keys for a long period of time. Therefore, the AS security keys need to be regularly refreshed. However, refreshing the security keys does have impact on performance, e.g. time delay, buffering requirements, radio resource usage etc. In fact this is the case when refreshing AS security keys in LTE systems. Because it is not practically feasible to start encrypting the downlink data upon "departure to L1", i.e. when the MAC scheduler determines which queue to serve, downlink data is encrypted and queued in advance in the eNB. Therefore, a key-refresh implies that the queued data that was already encrypted with the old key must be decrypted and re-encrypted with the new key.

In the case of an intra-eNB HO, i.e. handover between the cells belonging to the same eNB, decryption and re-encryption within the same eNB does not serve any security purpose. But a key-refresh is done anyway in the LTE system at intra-eNB HO. Such unnecessary key-refresh could be an issue in NextGen systems due to higher throughput and lower latency requirements.

Another motivation is related to the centralized RAN deployment (Figure 5.3.3.11.1-1) and co-sited deployment scenarios, described in the 3GPP TR 38.801. In relation to this, all the agreed options for the functional split between the central and the distributed units do place both the RRC and PDCP layers in the central units. These are the layers handling the security for the UP and CP traffic with the UE.

There could be scenarios where the Central Unit is placed in a secure location. In such cases, refreshing the keys for a handover that does not require a Central Unit change is not really needed and hence is not worth the additional processing burden. Therefore, unnecessary key-refresh is an issue that needs optimization in the NextGen system.

Lenovo Ex. 1007
Page 285

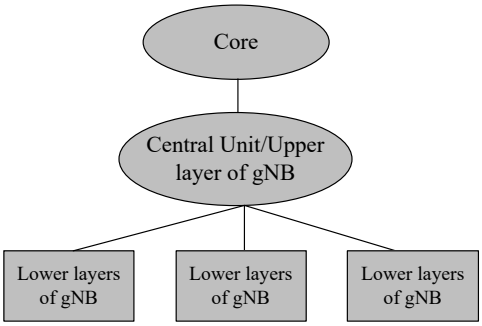


Figure 5.4.3.11.1-1: Centralized RAN deployment scenario in the NextGen

In summary, a flexible mechanism of key-refresh could be useful in the NextGen system. This mechanism should allow the network to control when to perform the key-refresh, for example depending on the type of the deployment, the location of the Central Unit, etc. As a consequence, the network would be able to avoid unnecessary key-refresh and perform necessary key-refresh only when there are security reasons.

5.4.3.11.2 Security threats

- If AS security keys are not refreshed when required, the confidentiality and integrity of the AS messages could be compromised.
- If AS security keys are always refreshed even when not required, then performance of RAN could be degraded (i.e., operational inefficiency).

5.4.3.11.3 Potential security requirements

- The NextGen RAN shall support a flexible mechanism for the refreshment of the security keys.
- The NextGen RAN shall allow the network to control when to refresh the security keys.

5.4.3.12 Key issue #4.12: Changing AS security keys on-the-fly

5.4.3.12.1 Key issue details

In LTE systems, the security keys used for the protection of the radio interface communication are known as access stratum (AS) keys. The clause 7.2.9 of the 3GPP TS 33.401 describes the mechanism in LTE systems for changing the LTE AS keys on-the-fly. The change of LTE AS keys on-the-fly is accomplished using a procedure based on intra-cell handover (HO), shown in Figure 5.4.3.12.1-1.

The LTE intra-cell HO procedure is logically an X2 HO procedure where both the source eNB and the target eNB are the same. The eNB instructs the UE to perform HO by sending the RRC Connection Reconfiguration message (described in 3GPP TS 36.331). The UE detaches from the eNB and again performs RACH procedure (described in 3GPP TS 36.321) with the same eNB. After the completion of the RACH procedure, the UE confirms the completion of the HO by sending RRC Connection Reconfiguration Complete message (described in 3GPP TS 36.331) to the eNB.

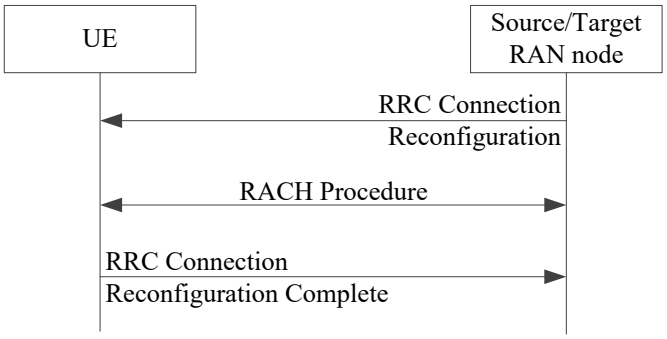


Figure 5.4.3.12.1-1: LTE intra-cell / intra-eNB HO that is also used for changing keys on-the-fly.

Lenovo Ex. 1007
Page 286

The main motivation of using this RACH procedure in this case is to synchronize the key-change between the UE and the eNB. In other words, the UE and the eNB use the old AS keys for all signalling and data transmissions prior to the RACH procedure, and the new AS keys for all signalling and data transmissions after the RACH procedure. Doing so means that the UE and the eNB need to flush or clear any data currently stored in RLC/MAC transmit/receive buffers at the time of the RACH procedure, so that this data can be sent/resent from the PDCP layer using the new key.

Security awareness is one of the increasing trends in society as reflected by the high expectations on the security in Next Generation systems. This is will not only drive continuous improvements in security standards but will also motivate for enforcing better security practises and stricter security policies, e.g. increasing the refresh frequency of security keys.. Furthermore, the number and the types of devices served by Next Generation systems is expected to dramatically increase. This implies that the consumption of radio resources because of additional RACH-like procedures for each key-change will get worse. Finally, the Next Generation systems are expected to support services with very strict performance requirements, e.g. low latency or high reliability, which clearly will benefit from avoiding undertaking unnecessary RACH-like procedures and RLC/MAC buffer flushes.

Therefore, for the Next Generation systems, it is desirable to analyse potential enhancements to existing mechanism of changing AS keys on-the-fly.

5.4.3.12.2 Security threats

- In absence of efficient mechanism of changing AS keys on-the-fly, if the AS security keys are not refreshed (to save radio resource or to improve latency), the confidentiality and integrity of the AS messages could be compromised.

5.4.3.12.3 Potential security requirements

- The NextGen RAN should have efficient mechanism (e.g., in terms of radio resource and latency) to change the AS keys on-the-fly.

5.4.3.13 Key issue #4.13: Dealing with radio jamming

5.4.3.13.1 Key issue details

This key issue covers the problem of radio jamming attack and the aspects of what Next Generation systems could do to deal with it.

One way to mitigate, if not to prevent, the effect of the radio jamming attack is to use frequency hopping over a large set of frequencies. Doing so could be a feat available today to military systems, but not to civilian cellular systems because of the limited available spectrum. It might also be unfeasible, if possible, to provide effective resilience against high power radio jamming in the vicinity of the receiver.

Nevertheless, it is important and worthy to develop potential solutions for the Next Generation systems, that are first, feasible or practical, and second, improve resilience compared to the LTE systems such as:

- resilience against low power jamming;
- network-based (and/or UE-assisted) detection of jamming that enables the MNO and LEA to search for and stop unlawful radio jamming; etc.

Editor's Note: It is FFS whether it is technically feasible to address low power jamming and whether it is in scope of SA3 in the first place.

5.4.3.13.2 Security threats

- Radio jamming interrupts the normal service and in absence of its detection/resilience, there could be serious impacts on vehicular safety, critical infrastructures, MNO's reputation, etc.

5.4.3.13.3 Potential security requirements

- The network should support detection of radio jamming.
- The network may support resilience to low power jamming.

Lenovo Ex. 1007
Page 287

5.4.3.14 Key issue #4.14: Privacy aspects of RAN level temporary identifiers

5.4.3.14.1 Key issue details

In LTE systems, the identifier called the "C-RNTI" is used in the RAN level for various purposes, e.g., the eNB scheduling data transmission to the UE, the UE sending scheduling requests to the eNB, etc. The C-RNTI is assigned by the eNB during RRC connection establishment. The C-RNTI can be re-assigned using RRC Connection Re-configuration message (e.g. at handover).

When the C-RNTI is assigned by the eNB during RRC connection establishment that uses contention based random access (CBRA) procedure, the C-RNTI is visible over-the-air. If S-TMSI was used in the RRC connection request message, then the C-RNTI and the S-TMSI are linkable to each other. However, there does not seem to be a significant privacy issue because first, the S-TMSI itself is temporary identifier (i.e., the actual subscriber is unknown), and second, the C-RNTI is short-lived (i.e., during a particular RRC connection) and changes during handover and RRC state transitions.

It is also not feasible for the eNB to deliberately keep assigning the same C-RNTI, even if it wanted, to the same subscription because the C-RNTI is assigned during the RACH procedure (i.e., in random access response (RAR) message) while the S-TMSI is known only after the RACH procedure (i.e. in RRC connection request message). The only apparent privacy issue is that an attacker can guess the presence of some subscriber based on the UL/DL traffic when the RRC connection is very long-lived.

During handover (HO), when the C-RNTI is securely assigned by the target eNB during RRC connection re-configuration after which the UE uses contention free random access (CFRA) procedure, the C-RNTI is not visible over-the-air. There does not seem to be any privacy issue.

This key issue deals with the privacy aspects of the RAN level temporary identifiers of the Next Generation systems, i.e. whether the future RAN level temporary identifiers introduce any new privacy issue and if yes, how to solve it.

The scope of this key issue also covers any possible enhancements that would benefit the NR architecture/requirements and possibly enhance the privacy aspects.

NOTE: Privacy aspects of CN level identifiers (e.g., IMSI, GUTI) are covered in security area #7 (i.e. Subscriber Privacy).

Editor's Note: The severity of the privacy threat is FFS.

5.4.3.14.2 Security threats

- The mechanism to handle the RAN level temporary identifiers in the Next Generation systems could introduce new privacy issues that were not present in LTE.

5.4.3.14.3 Potential security requirements

- The mechanisms to handle RAN level temporary identifiers in next generation system shall not introduce new privacy issues (e.g. exposing subscription identifiers).

5.4.3.15 Key issue #4.15: Security aspects of Xn handover

5.4.3.15.1 Key issue details

According to the TR 38.801 [72], the logical nodes in the new RAN of the NextGen system are either gNBs or eLTE eNBs. The New RAN architecture is shown in Figure 5.4.3.15.1-1 and different architecture options are shown in Figure 5.4.3.15.1-2.

Lenovo Ex. 1007
Page 288

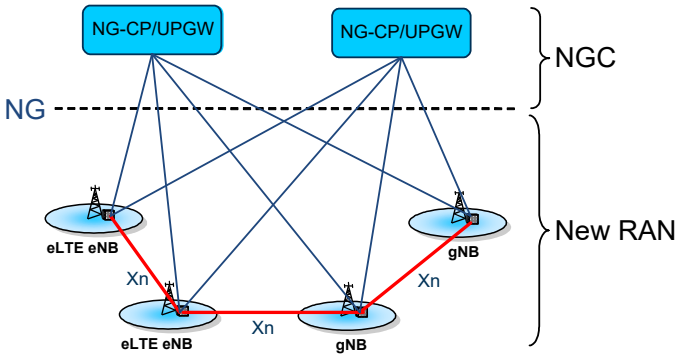


Figure 5.4.3.15.1-1: New RAN architecture

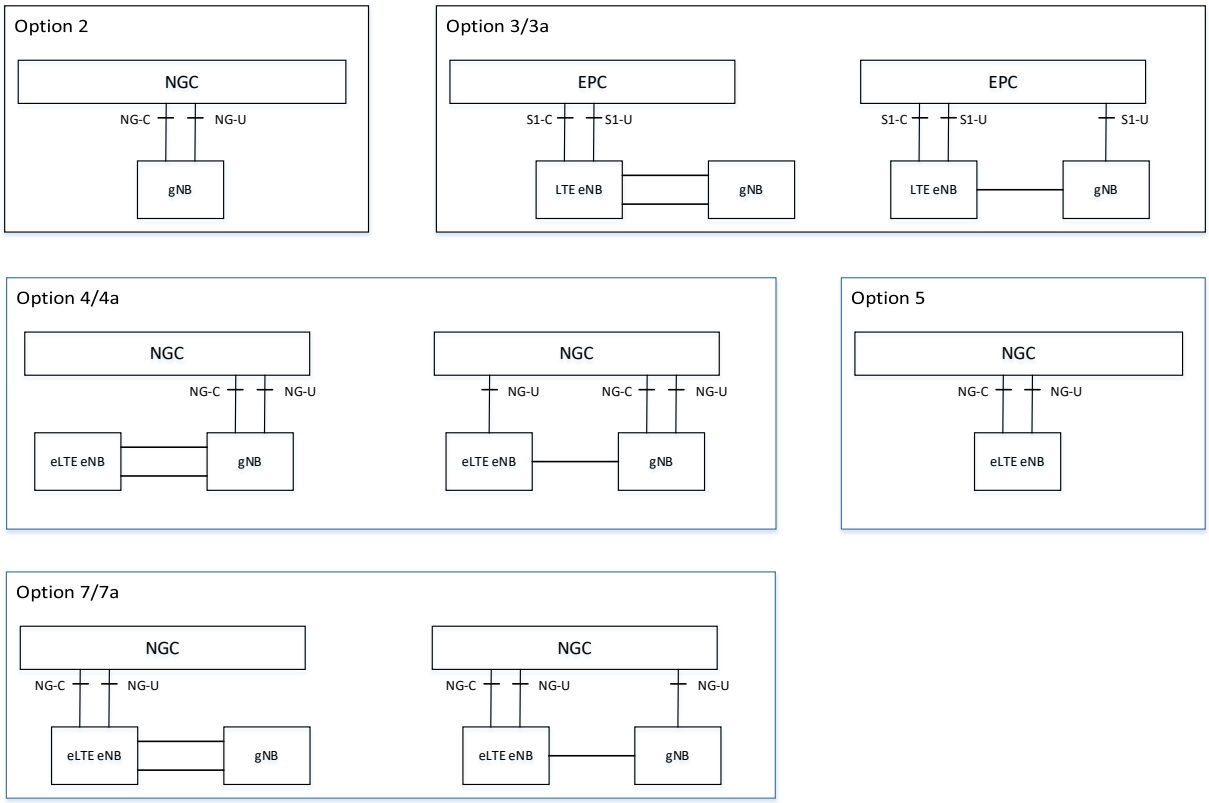


Figure 5.4.3.15.1-2: New RAN architecture options

The logical RAN nodes (eLTE eNB and gNB) are connected to the Next Generation Core (NGC) via the NG interface, and are interconnected with each other through a new RAN interface named the Xn/Xx interface. The New RAN functions and the Xn interface are described respectively in the clauses 6.2 and 7.3.1 of the TR 38.801. It is clear that the Xn interface will support Xn handover, both NR-NR (between two gNBs), E-UTRA-E-UTRA (between two eLTE eNBs) and E-UTRA-NR (between eLTE eNBs and gNBs).

The Option 3/3a is not relevant to Xn handover because the RAN nodes are connected to the EPC rather than to NGC. In Option 4/4a, the LTE eNB is connected as a non-standalone RAN node and cannot act as source or target in Xn handover. Similarly, in Option 7/7a, the gNB is connected as a non-standalone RAN node and cannot act as source or target in Xn handover. The architecture options that are relevant to our study are listed in Table 5.4.3.15.1-1 (the term "same NGC" is used because there is no NGC change during the Xn handover).

Lenovo Ex. 1007
Page 289

Table 5.4.3.15.1-1: Architecture options for Xn handover

Options	Source node	Target node	Core network
gNB-A and gNB-B connected to same NGC (option 2/4 of RAN arch.)	gNB-A	gNB-B	NextGen core
gNB and eLTE eNB connected to same NGC (option 2/4 combined with option 5/7/7a of RAN arch.)	gNB	eLTE eNB	NextGen core
eLTE eNB-A and eLTE eNB-B connected to same NGC (option 5/7/7a of RAN arch.)	eLTE eNB-A	eLTE eNB-B	NextGen core
eLTE eNB and gNB connected to same NGC (option 5/7/7a combined with option 2/4 of RAN arch.)	eLTE eNB	gNB	NextGen core

In the LTE, the X2 interface (corresponding to Xn interface) is protected using the NDS/IP as specified in TS 33.210. Similarly, during the X2 handover in the LTE (corresponding to Xn handover), the backward and forward securities are achieved as follows [TS 33.401]:

- The source eNB derives a new KeNB called KeNB* from the old KeNB or a fresh NH (received from the MME). This new KeNB* is transferred together with the corresponding NCC to the target eNB. The KeNB* provides 1 hop backward security because the target eNB has no knowledge of the security keys used in source eNB.

- The target eNB uses the KeNB*, that was sent by the source eNB, as its KeNB. The source eNB knows this KeNB (i.e. same as KeNB*) used in the immediate target eNB. But the source eNB will not know the future KeNBs used in the new target eNBs because of future handovers. Therefore, there is 2 hop forward security. However, it is recommended that the target eNB initiates an intra-cell handover with the UE as soon as possible (meaning that the target eNB manually triggers a vertical key derivation) so that the source eNB no longer knows the latest KeNB.

It is important for the NextGen systems to maintain or improve (if necessary) the existing protection mechanism in the LTE. Therefore, this key issue concerns the security aspects of the Xn handover, especially the backward/forward security of the security keys.

NOTE: Security of Xn/Xx interface is covered in key issues #4.10 (i.e., Security aspects of sidehaul interfaces).

5.4.3.15.2 Security threats

If the target RAN node is compromised and the UE security keys do not have the property of backward security, then an attacker would be able to decrypt the previous signalling and user plane data exchanged between the UE and the source RAN node.

If the source RAN node is compromised and the UE security keys do have the property of forward security, then an attacker would be able to decrypt the future signalling and user plane data exchanged between the UE and the target RAN node.

NOTE: Key issues #4.10 shall be referred to, for security of Xn interface.

5.4.3.15.3 Potential security requirements

- The Access Stratum (AS) security keys shall have property of forward security.

- The Access Stratum (AS) security keys shall have property of backward security.

NOTE: Key issues #4.10 shall be referred to, for security of Xn interface.

5.4.3.16 Key issue #4.16: Security algorithm negotiation between UE and RAN

5.4.3.16.1 Key issue details

According to the TR 38.801 [72], the logical nodes in the new RAN of the NextGen system are either gNBs or eLTE eNBs. The New RAN architecture is shown in Figure 5.4.3.16.1-1.

Lenovo Ex. 1007
Page 290

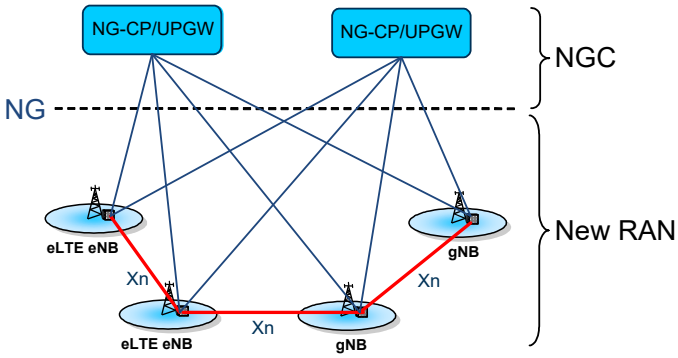


Figure 5.4.3.16.1-1: New RAN architecture

Both gNB and eLTE eNB are expected to support the RRC protocol or a modified RRC protocol, similar to in LTE. The RRC protocol exchanged between the RAN and UE requires both integrity protection and confidentiality protection. In order to establish security between the RAN and the UE, it is expected that security algorithm negotiation is required between the UE and the RAN, similar as in LTE.

5.4.3.16.2 Security threats

- In lack of a secure security-algorithm negotiation, an attacker could perform bidding down attacks on the security algorithms negotiated between the UE and the RAN.

5.4.3.16.3 Potential security requirements

- It shall be possible to do secure negotiation of security algorithms between the UE and the RAN.

5.4.3.17 Key issue #4.17: Supporting integrity protection of UP

5.4.3.17.1 Key issue details

Integrity protection of UP data between UE and core network was introduced for enhanced-GPRS for IoT devices in 3GPP Rel-13. The support of Integrity protection of UP data for enhanced-GPRS was optional in the UE but mandatory in the network.

Such a feature for IoT devices is expected to be very useful as well in Next Generation. Especially, if the security between UE and gNB is similar to AS security in EPS, then the question could be about activating the existing integrity protection from the control plane also for user plane and about re-using existing mechanism of distributing keys, negotiate the security algorithms, refresh of security context or re-using the fields in the existing PDCP protocol.

Support of UP integrity in gNB and device may be simple to add if its specified as a mandatory feature already in Phase 1. If the feature is added later e.g. in Phase 2, then it may become complex as legacy network nodes needs to be considered and taken care of in the solution. From deployment point of view, adding integrity protection of UP to the RAN would need to be done in phase 1. Adding such protection at upper layer may be easier later.

Editor's Note: Its FFS whether LTE eNB's connected to a Next Generation core should support UP integrity protection between the UE and LTE eNB as well.

If support of UP integrity protection is introduced in gNB and devices, then it is expected that the use of UP integrity protection needs to be negotiated between the UE/device and core network in NAS layer. The core network would need to inform the gNB via NG2 interface and the UE whether to enable UP integrity protection or not.

This key issue concerns the security aspects of the support of UP integrity protection in gNB and device, and the impacts on mobility (e.g. NG2-handover procedure and Xn-handover) and Dual Connectivity.

Introduction of UP integrity protection to gNB (using a method similar to the one used in enhanced-GPRS) could require at least the following:

- The UE would need to indicate the support of the UP integrity protection feature to the CN in a secure way.
- The CN would need to make a policy decision of activating the UP integrity for the UE.

Lenovo Ex. 1007
Page 291

- The CN would need to inform gNBs about the policy decision.
- gNBs would need to indicate the usage of the feature to the UE.
- gNBs would need to inform each other about the policy decision when the UE is moving or dual connectivity is activated.

5.4.3.17.2 Security threats

- In lack of a secure way of indicating that the UP integrity protection shall be used, an attacker could perform bidding down attacks to disable UP integrity protection in the UE.

5.4.3.17.3 Potential security requirements

- It shall be possible for the network to securely indicate to the UE that the UP integrity protection is to be used.
- It shall be possible for the network nodes to securely inform each other about the UE's integrity protection (e.g., when the UE is moving or dual connectivity is activated).

5.4.3.y Key issue #4.y: <key issue name>

5.4.3.y.1 Key issue details

5.4.3.y.2 Security threats

5.4.3.y.3 Potential security requirements

5.4.4 Solutions

5.4.4.1 Solution #4.1: Network signs selected signalling messages

5.4.4.1.1 Introduction

This solution addresses key issue #4.1.

Editor's note: The impact of global certificates is for ffs.

Editor's note: the operational impacts of these solutions (e.g. managing PKI) are ffs.

5.4.4.1.2 Solution details

5.4.4.1.2.1 Background

In this solution, NextGen networks need to have private keys, and UEs can obtain the corresponding public keys and verify their authenticity. The network then uses the private key to append a digital signature to sensitive (broadcast or UE-specific) downlink signalling messages, and the UE can verify the authenticity of those messages. This prevents a false network from spoofing those messages successfully.

Editor's note: It is ffs which messages should be signed. It is also ffs how exactly message formats should be adapted to accommodate an appended signature.

The mechanism is mandatory to implement and mandatory to use in networks. It is optional to support and optional to use in UEs. Legacy UEs, or UEs for which signature verification would be in some sense too demanding, can ignore the appended signatures and treat all network messages as genuine.

5.4.4.1.2.2 Provisioning and management of keys

This solution requires one or more global Certification Authorities (CAs). Each network needs to have a root key pair, with the public key certified by one of the CAs.

Lenovo Ex. 1007
Page 292

NOTE: An alternative approach, avoiding centralised CAs, would be to have every home network sign visited network certificates to be used by the home network's own subscriptions. The list of visited network certificates available to a subscription could be maintained by an OTA mechanism. This alternative seems harder to maintain, however.

All CA root public keys should be programmed into each UE that supports the present solution. These root keys could in principle be either in the USIM (or its NextGen equivalent) or in the ME. The solution proposed is as follows:

- The UE first looks for three lists on the USIM:
  - A list of Permitted CA Certificates. Each entry on this list is a full root certificate.
  - A list of Forbidden CA Certificates. Each entry on this list is an unambiguous certificate identifier.
  - A list of Forbidden Network Certificates. Each entry on this list is an unambiguous certificate identifier.
- Dependent on what lists are present on the USIM, then UE may also look for lists on the ME, as follows:
  - If there are no Permitted CA Certificates listed on the USIM (either no file or an empty file) then the UE looks for a list of Permitted CA Certificates on the ME.
  - If there are no Forbidden CA Certificates listed on the USIM (either no file or an empty file) then the UE looks for a list of Forbidden CA Certificates on the ME.
  - If there are no Forbidden Network Certificates listed on the USIM (either no file or an empty file) then the UE looks for a list of Forbidden Network Certificates on the ME.

By initially including a dummy Forbidden CA Certificate on the USIM, the MNO can in effect indicate to the UE that it (via OTA to the USIM) will manage the Forbidden CA Certificate list. Similarly, by initially including a dummy Forbidden Network Certificate on the USIM, the MNO can in effect indicate to the UE that it (via OTA to the USIM) will manage the Forbidden Network Certificate list. (An alternative would be to have a flag on the USIM indicate this intention to the UE.) Otherwise, the two forbidden certificate lists can be managed in ME software updates.

Each NextGen network generates one or more (Network Private Key, Network Public Key) pairs, and obtains corresponding Network Certificates signed by one of the global CAs. The Network Private Key is not used directly for signing signalling messages. Instead, individual network nodes generate or are provided with (Network Node Private Key, Network Node Public Key) pairs, with the Network Node Public Key signed by a Network Private Key in a Network Node Certificate.

Network Node Certificates have a relatively short duration, e.g. one day. The UE should cache at least the most recently seen Network Node Certificate, and may cache more.

The Network Node Private Key is then used to sign messages. The network node broadcasts its Network Node Certificate, which the UE will be able to verify. Having verified the Network Node Certificate, the UE will also be able to verify signatures on signalling messages.

5.4.4.1.2.3 Revocation

There are three levels of certificate: Global CA Certificates, Network Certificates, and Network Node Certificates.

Revocation of Global CA Certificates is managed by the use of Certificate Revocation Lists on the UE. The home network can send OTA messages to update the list of Forbidden CA Certificates, or the list of Permitted CA Certificates, or both. Device vendors may also update the ME-based list of Forbidden CA Certificates and/or the ME-based list of Permitted CA Certificates in software updates. Trusted online revocation servers may also be used, in which case the UE will check the revocation server periodically, and use relevant information found there to update its own local list of Forbidden CA Certificates.

Revocation of Network Certificates is also managed by the use of Certificate Revocation Lists on the UE. The home network can send OTA messages to update the list of Forbidden Network Certificates. Device vendors may also update the ME-based list of Forbidden Network Certificates. Trusted online revocation servers may also be used (in particular, managed by the CAs that issued the Network Certificates), in which case the UE will check the revocation server periodically, and use relevant information found there to update its own local list of Forbidden Network Certificates.

Network Node Certificates are not revoked – just allowed to expire, and not renewed.

Lenovo Ex. 1007
Page 293

5.4.4.1.2.4 Signature algorithms and algorithm selection

UEs supporting this solution must support the ECDSA signature algorithm [32].

NOTE: An alternative signature algorithm would be RSASSA-PSS (specified in PKCS #1 v2.2 and RFC 3447).

Editor's note: It is ffs how best to support new algorithms in future, such as quantum computing resistant algorithms. Options include

(a) New algorithms are supported by new UEs, and where possible in current UEs via patching; new algorithms are mandatory to support in networks, and network appends multiple signatures computed using all available algorithms. The UE pays attention only to the "best" algorithm that it supports. The biggest downside of this approach are that all networks must be upgraded before a new algorithm can be introduced on the UE side.

(b) Networks broadcast which algorithms they support, and the UE chooses the "best" algorithm that it has in common with the network. The network appends multiple signatures computed using all available algorithms. The biggest downside of this approach is that a false network can say that it only supports the weakest algorithm.

(c) A list on the UE, updated by the home network, tells the UE which visited networks support the new algorithm(s). An attacker who can't break the new algorithms then can't pose as one of those networks, but can pretend to be another network instead.

5.4.4.1.2.5 UE actions

A UE supporting this solution will reject a signalling message that it expects to be signed, unless the following conditions are all true:

- the message has a signature that the UE can verify using a Network Node Public Key;
- the Network Node Public Key has a certificate that the UE can verify a Network Public Key;
- the Network Public Key has a certificate that the UE can verify using a root CA certificate in its Permitted CA Certificates list;
- the root CA Certificate is not in the UE's Forbidden CA Certificates list;
- the Network Certificate is not in the UE's Forbidden Network Certificates list.

If the UE rejects a message then it does so silently, with no error message being returned.

5.4.4.1.3 Evaluation

1. Description of attack on Broadcast messages with Digital Signature: If an attacker obtains a log of the broadcasted MIB and SIBs with time stamp, digital signature, SFN etc for 24 hrs from a valid network node, with all the parameters, he is in possession of the system information matching time stamp and digital signature. The attacker can masquerade as the original cell, its cell Id, frequency parameter etc and broadcast the same MIB/SIB information. All he needs to do is to synchronize his broadcast with the time stamp in his log file to match the original cell. If this is an attack on idle mode UEs, the attacker need to operate the fake cell in the same tracking area (TA), to match the TAC.

If the idle mode UE, entered idle mode in the same tracking area as the attacker is broadcasting with tracking area code (TAC) in the MIB, the idle mode UE will pass the digital signature check. The idle mode UE has the public key ($K\text{-}SIG_{Public}$) for the tracking area, if the UTC time matches the signature verification will be successful. Whether the content of the system information, whether it is MIB or any of the SIBs, is it actual or replayed, the UE will not be able to make out because the signature matches. The end result is that the idle mode UE camps on a fake eNB. The UE would loose all the valid paging messages, broadcast messages by camping on it.

If the UE is trying to do a fresh Attach to a fake network, it will be fooled by the replayed signed system broadcast messages since the signed broadcast messages will pass verification. UE will send the subscription identity (e.g such as IMSI or P-IMSI) to the network. The attacker succeeds in extracting the identifier (IMSI/PMSI/GUTI etc) from the UE, the signature verification will fail only in the subsequent messages.

If the UE gets attached to a genuine network, then security mechanisms specified at the NAS and AS protocol layers makes it difficult to spoof the UE specific messages in the DL and UL.

Lenovo Ex. 1007
Page 294

Draw back of the current solution: In the current solution, *"Each NextGen network generates one or more (Network Private Key, Network Public Key) pairs, and obtains corresponding Network Certificates signed by one of the global CAs. The Network Private Key is not used directly for signing signalling messages. Instead, individual network nodes generate or are provided with (Network Node Private Key, Network Node Public Key) pairs, with the Network Node Public Key signed by a Network Private Key in a Network Node Certificate.*
Network Node Certificates have a relatively short duration, e.g. one day. The UE should cache at least the most recently seen Network Node Certificate, and may cache more.
The Network Node Private Key is then used to sign messages. The network node broadcasts its Network Node Certificate, which the UE will be able to verify. Having verified the Network Node Certificate, the UE will also be able to verify signatures on signalling messages. "

If the Network Node Certificates have a relatively short duration, e.g. one day, the signature of all system broadcast messages may repeat for the duration of the day. That means an attacker can copy and replay these messages. The UE is expected cache the most recently seen Network Node Certificate, and may cache more. The Network Node Private Key is then used to sign messages. The network node broadcasts its Network Node Certificate, which the UE will be able to verify. Having verified the Network Node Certificate, the UE will also be able to verify signatures on signalling messages.

Observation1: It is possible to mount a successful attack on UEs within a tracking area even with the solution described in 5.4.4.1 against system broad cast messages from a valid cell/network node.

Observation 2: Based on the validity of certicate, signature will remain steady or repeats. Replay attacks are possible based on signature steady and repeat cycle.

Observation 3: To avoid the replay attacks completely calendar+UTC time stamp (as specified in RFC3339) is needed as parameters in signature calculation.

Observation 4: Even with Calendar+UTC time stamp, (near) realtime replay attacks are possible, to avoid this GPS coordinates of the cell are also needed and the UE need to verify its GPS coordinates with that of the cell.

Observation5: If the UE was power cycled totally it would be difficult for UE to know the local time or UE without learning from the SIB.

Observation6: With Digital Signature and Timestamp, GPS parameters, the size of protected System Info can get significantly larger.

2. Attack on Unicast messages to a UE with Digital Signature: An attacker can replay signed system broadcast messages from a real gNB and fool the UE to since send the Attach Request with subscription identity (e.g such as IMSI or P-IMSI) to the network. The attacker succeeds in extracting the identifier (IMSI/PMSI/GUTI etc) from the UE. The attacker can also replay valid reject/fail messages signed by a valid network, which he may have extracted previously. Most of the reported hackings on the LTE networks has been on the unprotected initial messages like Attach Request/ Attach Reject (EMM error codes), Tracking Area Update Reject etc. In the replayed system response scenario, since the message is signed by the system the UE will pass the message correctly and will behave according to the instruction. The attack succeeds.

Observtaion 7: UE may need to include a freshness parameter NONCE in addition to the UE ID to the network in case of Attach Request/ Re-attach etc. The network should send back the integrity protected NONCE in the response message to avoid replay attacks. This should be the case for all messages until umutual authentication between UE and network takesplace.

3. Protection of Unicast messages after mutual authentication: Unicast messages to a UE after successful mutual authentication between the UE and the gNB are integrity protected using the key derived from the AS and NAS context keys, hence they do not need additional protection using certificate/private keys. Such protection only adds to additional overheads to signaling messages.

Observation 8: Messages that need protection are unicast messages to the UE before the UE is authenticated and not being protected with AS and NAS security context.

5.4.4.2 Solution #4.2: Verification of authenticity of the cell during RRC idle mode

5.4.4.2.1 Introduction

This solution addresses key issue # 4.1.

Lenovo Ex. 1007
Page 295

A cell periodically broadcasts synchronization signals and system information (SI). UE detects a cell based on the synchronization signals. If the signal quality of detected cell is above a defined threshold then UE determines whether the cell is authentic or not, to camp on it. A cell is authentic, if the authenticity verification of the system information received from the cell is successful.

5.4.4.2.2 Solution details

5.4.4.2.2.1 System Information verification using Digital Signatures

This solution is applicable only for verification of authenticity of the cell during Idle mode cell reselection.

In order to enable the UE to validate the authenticity of received system information, the NR digitally signs the broadcasted system information as shown in Figure 5.4.4.2.2.1-1. System information to be broadcasted, Private security key ($K\text{-}SIG_{Private}$) and Time Counter are input to security algorithm to generate the digital signature. The generated DS together with some least significant bits of Time Counter is added to the system information before transmitting over the air. $K\text{-}SIG_{Private}$ is specific to the Tracking area. The private key ($K\text{-}SIG_{Private}$) is provisioned in the NR by the MNO. The public $K\text{-}SIG_{Public}$ key is provisioned by the core network to the UE, when performing location update procedure, as shown in Figure 5.4.4.2.2.1-2. Time Counter is maintained based on UTC time (number of UTC seconds in 10 ms units since 00:00:00 on Gregorian calendar date 1 January, 1900 (midnight between Sunday, December 31, 1899 and Monday, January 1, 1900), similar to the mechanism used in ProSe Discovery protection TS 33.303) and can be units of milliseconds or seconds or minutes. The gNB obtains a value for a UTC-based counter associated with a transmission slot based on UTC time. The UE may obtain UTC time from any sources available, e.g. the RAN (via SIB, as in LTE via SIB16), NITZ, NTP, GPS (depending on which is available). The Time Counter input to the security algorithm is the value of counter corresponding to time slot in which system information is transmitted. The usage of Time Counter ensures that received system information cannot be replayed. There can be differences in the Time Counter maintained in the UE and the AN because of different UTC source or implementation errors. To take care of these errors least significant bits of Time Counter are also transmitted along with system information.

On receiving the system information the UE generates digital signature. The system information with digital signature received, public security key ($K\text{-}SIG_{Public}$) and Time Counter of the time slot in which system information is received are used to check the authenticity of the SI. If authenticity verification is successful, then the system information is authentic and the UE considers the cell as authentic.

The size of the digital signature leads to increase in the signalling overhead. In order to reduce the overhead, digital signature can be generated for multiple system information together instead of generating the digital signature for each system information. System information is periodically broadcasted, in order to reduce the overhead; protection can be applied once every 'N' period instead of every period. Mechanisms to reduce the overhead are detailed in the clause 5.4.4.2.2.3 of this TR.

Editor's note: The solution to be revised to update the Tracking Area equivalent for NextGen System based on the progress in other working groups.

Editor's Note: It is FFS to determine if provisioning multiple K-SIG-Pubs in UE is feasible.

Editor's Note: Provisioning of K-SIG-Priv needs to be clarified. And it is FFS to determine if provisioning K-SIG-Private in multiple NRs during each TAU is feasible.

Editor's Note: It is FFS whether the K-SIG-Priv of all eNBs within a TA are same or different. The possible key leakage if the same K-SIG-Priv is shared by all eNBs needs to be considered.

Lenovo Ex. 1007
Page 296

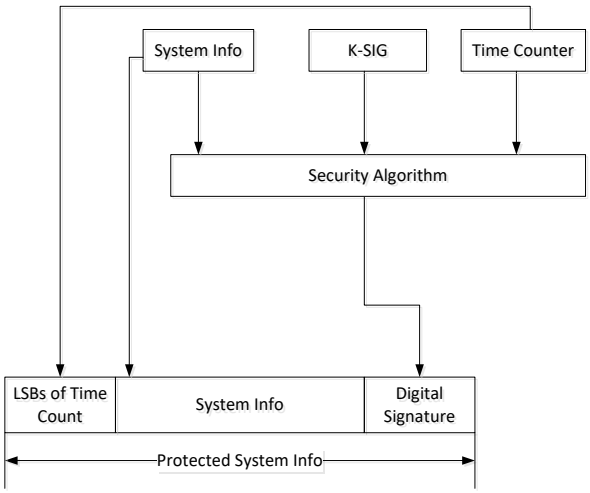


Figure 5.4.4.2.2.1-1: System Information verification using Digital Signatures

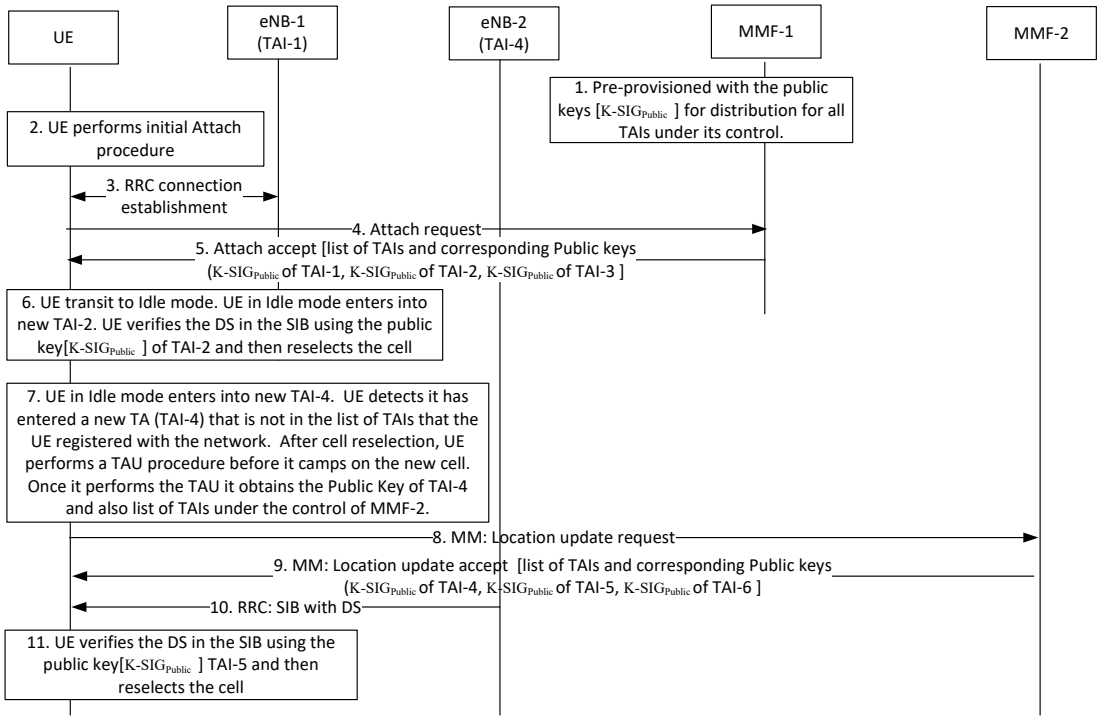


Figure 5.4.4.2.2.1-2: Provisioning of Public Keys to the UE

5.4.4.2.2.2 System Information verification using Identity Based Cryptography

The network provisions UEs and NR with a set of credentials for Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI), as defined in IETF RFC 6507 [33] along with the public key of the CN. Furthermore, UEs are provisioned with the Public Validation Token (PVT) specific to each cell and the NR are configured with the Secret Signing Key (SSK) associated with its cell identity. In order to verify the authenticity of the cell, the NR act as "signer" and the UE act as the "verifier" (according to the definitions in RFC 6507). The NR uses SSK associated to the cell to sign the system information, and the UE uses the public key of the CN and the cell ID specific PVT to verify the signature.

As mentioned in the clause 5.4.4.2.2.1, the time counter is used as the input for signature generation and also to reduce the overhead; digital signature can be generated for multiple system information together and protection can be applied once every 'N' period instead of every period. Mechanisms to reduce the overhead are detailed in the clause 5.4.4.2.2.3 of this TR.

Lenovo Ex. 1007
Page 297

5.4.4.2.2.3 Optimization of SI verification using the other SI

5G SI is divided into minimum SI and other SI [62]. The other SI may either be broadcast, or provided in a dedicated manner by the gNB, triggered either by the network or upon request from the UE [62]. The authenticity verification information can be classified into the other SI. The gNB generate the digital signature with the minimum SI broadcasted, Private security key ($K\text{-}SIG_{Private}$) and Time Counter as input (as shown in Figure 5.4.4.2.2.1-3) and provides the digital signature in the other SI (as a separate SI) either periodically or upon request from the UE (as shown in Figure 5.4.4.2.2.1-4). As the UE needs to verify the authenticity of the gNB, only signing of the minimum SI is performed in order to reduce the overhead in the UE and in the gNB.

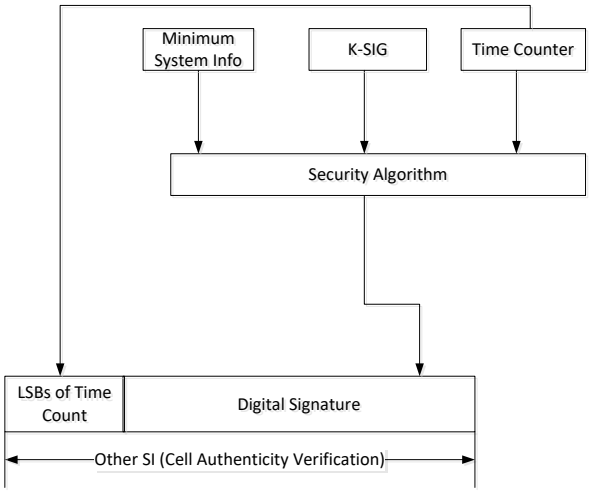


Figure 5.4.4.2.2.1-3: Cell authenticity verification using other SI

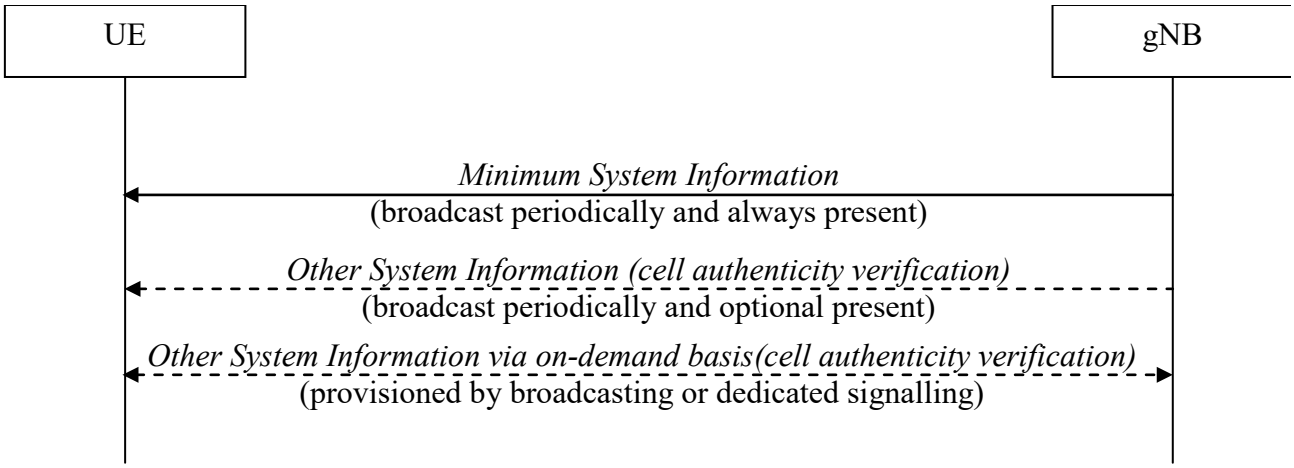


Figure 5.4.4.2.2.1-4: Transmission of cell authenticity verification using other SI5.4.4.2.3 Evaluation

Observation X: With Digital Signature and Timestamp parameters, the size of protected System Info can get larger and size impact needs evaluation.

Lenovo Ex. 1007
Page 298

5.4.4.3 Solution #4.3: Dual Connectivity Solution based on Offload counter

5.4.4.3.1 Introduction

5.4.4.3.2 Solution details

Editor's Note: In this solution gNB is expected to have the same protocol stack as eNB. In case the protocol stacks are different, the impact of that in this solution is FFS.

This solution is based on the principles of existing Dual Connectivity solution in LTE. The solution can be applied uniformly in different tight interworking scenarios between NR and E-UTRA, option 3/3a/3x, 4/4a and 7/7a/7x being considered as deployment options by RAN groups.

- E-UTRA-NR DC via EPC where the E-UTRA is the master (Option 3/3a/3x in TR 38.801 section 10.1.2);
- E-UTRA-NR DC via 5G-CN where the E-UTRA is the master (Option 7/7a/7x in TR 38.801 section 10.1.4);
- NR-E-UTRA DC via 5G-CN where the NR is the master (Option 4/4A in TR 38.801 section 10.1.3).

The eNB or gNB who is acting as the master MCG maintains an offload counter to derive security keys for the SCG. The counter is common for all types of SCG whether they are eNB or gNB.

When executing the SeNB Addition procedure (i.e. the initial offload of one or more radio bearers to the SeNB), or the SeNB Modification procedure requiring an update of S-K_{eNB}, the MeNB shall derive an S- K_{eNB} using a Offload counter which results in a fresh S-K_{eNB}. The MeNB shall forward the generated S-K_{eNB} to the SeNB during the SeNB Addition procedure or SeNB Modification procedure requiring key update.

The SeNB based on its protocol stack shall derive RRC security keys KRRCint and KRRCenc and user plane keys K_{UPenc} and K_{UPint} from the received S-K_{eNB} and use it for either integrity protection or encryption of radio bearer as indicated by the MeNB.

The general scheme for key derivation is given below.

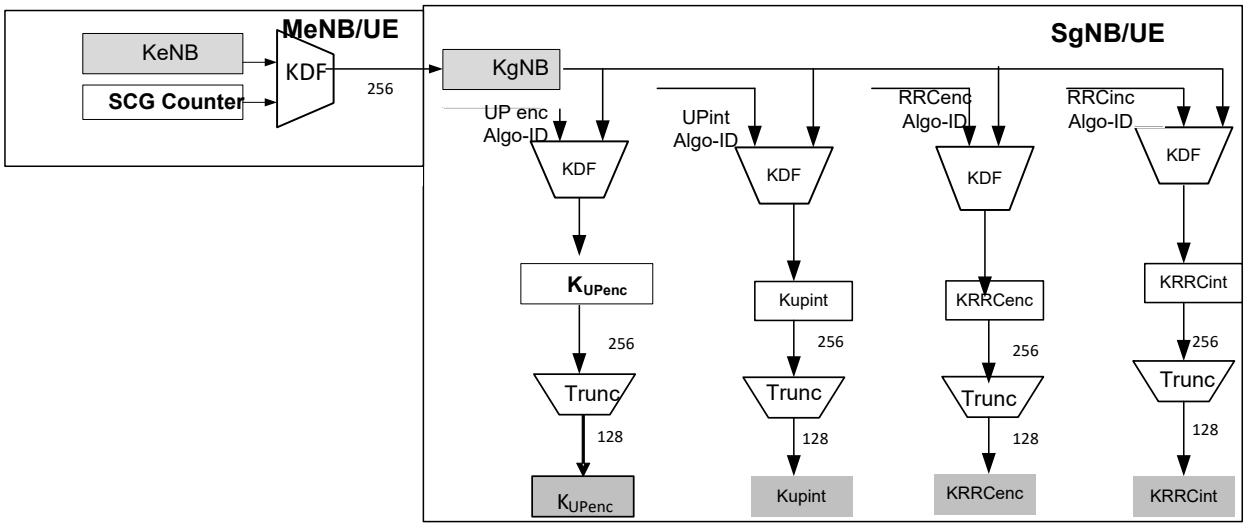


Figure 5.4.4.3.2-1: Key derivation scheme for tight interworking

Editor's Note: Key names need to be adapted for KeNB and gNB.

Editor's note: It should be further studied whether adding an RRC control function to the SgNB and deriving its protection keys from the S-KgNB introduces new threats. If so, these threats needs to be dealt with.

Lenovo Ex. 1007
Page 299

5.4.4.3.3 Evaluation

Solution is common across all tight interworking scenarios irrespective of the MCG or SCG type.

Solution maintains parity with existing LTE dual connectivity solution.

5.4.4.4 Solution #4.4: Fake gNB detection using UL traffic monitoring and System Query

5.4.4.4.1 Introduction

For the verification of authenticity of the cell during RRC idle mode, two solutions are given, which when combined can always verify the gNB.

5.4.4.4.2 Solution details

1) **Fake gNB detection using UL traffic monitoring:** In this method , the UE in Idle mode, when other conditions for Cell reselection and camping are met UE scans and monitor whether the cell has live UL link traffic. For this purpose, UL receiver is implemented in all NextGen UEs. If the UE can monitor and detect that there is UL traffic, that is reliable indication that the gNB is serving multiple UEs. For this the UE need to monitor the Uplink control channel PUCCH, where the UEs transmitting on the uplink put the indication so that gNB can decode it accordingly.

Editor's Note: This method will work only if the UE has capability to receive the UL traffic and able to receive UL from other UEs in any geographical location within the cell. If other UEs are close to BS than the monitoring UE and monitoring the UE's UL receiver is limited to certain range, then this solution may not be feasible. It is FFS to study this aspect.

As defined in TS 36.300 PUCCH contains information on ,

"Physical uplink control channel (PUCCH)

- *Carries Hybrid ARQ ACK/NAKs in response to downlink transmission;*
- *Carries Scheduling Request (SR);*
- *Carries CSI reports."*

Any fields present on the PUCCH channel is a good indication that the cell is serving UEs, but may not be serving genuine UEs.

Editor's Note: It is FFS which uplink channels are reliable for monitoring and conclude the authenticity of a cell without attack from fake UEs..

NOTE: Other UL channels like PUSCH or PDCCH also can be candidates for monitoring to determine the cell is serving active and genuine. Assuming UL receiver is implemented in all NextGen UEs and a mechanism is available for the monitoring UE to verify that the UL is from genuine UEs.

Editor's Note: It is FFS how complex is this UL monitoring for the UE in TDD and FDD systems.

2) UE verifies gNB with 'System Query' message:

In this procedure, the UE in Idle mode, when other conditions for Cell reselection and camping are met, will send a short System Query message to the gNB (or the Common Control Function (CCNF) where the NAS context of the UE is held). The UE includes a freshness parameter NONCE in the System Query message.

The Response to the System Query is generated by the Serving System network element (gNB or CCNF). The Response is digitally signed by using the Private Key of the Serving System. When digital signature is computed, the NONCE received from the UE is also used as a part of signed contents. To prevent any replay attacks of the message from the serving network, the GPS coordinates of the cell/gNB is also included as part of the signed contents. The presence of GPS cordinates of the gNB helps the UE to compare its own coordinates to make sure that it is within the expected coverage of the gNB or any of its cell sectors. The associated Public Key of the Serving System is signed in advance by the Trusted CA – an entity which is known and trusted by the HPLMN of the UE, and whose Trust Root

Lenovo Ex. 1007
Page 300

(Public Key of Trusted CA) is provisioned into the UE when subscription is set up. This signed Public Key of the Serving System is also included in the Response message.

Effectively, the System Query Response would contain at a minimum the following information:

- Cell-id or CCNF-id
- GPS coordinates of the Cell
- NONCE initially received from the UE
- Serving System Public Key and its Digital Signature computed in advance and provided by the Trusted CA: [PuK_SS][SIG1(PuK_SS)$_{PrK\_CA}$]
- Digital signature of all above elements computed using the Private Key of the Serving System: {SIG2[Cell_id/CCNF_id],[NONCE],[Cell GPS coordinates], [PuK_SS][SIG1(PuK_SS)$_{PrK\_CA}$]}$_{PrK\_SS}$

When the UE receives the Query Response message, it does the following:

1. UE uses the pre-provisioned Public Key of Trusted CA to validate the SIG1, and once it is validated, the UE accepts the Public Key of the Serving System as trusted.
2. Then, the UE verifies that the received NONCE is the one associated with the query that it sent.
3. Then the UE uses the received and validated Public key of the Serving System to validate the signature SIG2. Once this signature is validated, the UE gets assured of the legitimacy of the system that sent the Query Response.

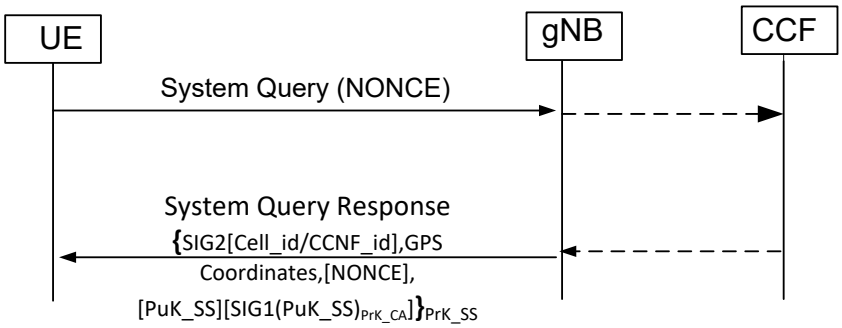


Figure 5.4.4.3-1 Idle mode UE doing a System Query to gNB/CCNF to verify the gNB.

Real time attacks with system query method: Real time attacks are possible even with the System Query method. If GPS coordinates are given to the UE, the UE can use its own GPS data and calculate the distance to the center of the Cell pointed by the GPS data. The UE can independently calculate distance to the Cell using radio link parameters, roundtrip time/ time of arrival and verify that this distance it finds in the communication matches with the distance based on GPS coordinates. But UE cannot figure out the actual GPS cordinates of the cell. Hence if the real time attacker happens to be in the same radial distance as the Cell center, the UE would not make out the difference and the attack would succeed. However matching the distance is very difficult to achieve and in any case the attack is limited only this same radial distance.

Editor's Note: It is FFS how to address the real time replay attacks in the system query method or it need not to be addressed since it is a very difficult attack to mount.

Editor's Note: It is FFS whether the neighbour list in the SIB can be used to enhance this method or neighbour list need to be added in the System Query message to help the UE evaluate the neighbour gNBs it should be seeing.

5.4.4.4.3 Evaluation

Draw back of UL traffic monitoring method: This method though reliable when the PUCCH indication is available, has a drawback. The limitation is that a genuine cell may not be always serving UEs on the Uplink and the serving UEs are not always under the proximity of the monitoring UE. There may not UEs transmitting all the time in every frame or sending ACK/NACK or CSI in every radio frame. Hence every radio frame may not carry PUCCH indications from UEs, particularly at late night or early morning hours. Hence this method could be used during day time or when available but needs an alternate way of verification if this step is inconclusive. Further UL traffic monitoring is power consuming for UE in idle. Also UE may not have RF/baseband receiver to monitor UL. Currently, UL receiver is implemented only in the BS (NBs, eNBs), hence additional HW needed in the UE. Even if the UE

Lenovo Ex. 1007
Page 301

receives the UL signaling, it is required to have a mechanism to check the validity of the UL signaling whether it is from genuine UE or from the fake BaseStation/UE.

Advantage of UL traffic monitoring method: UE in Idle mode can decide on the validity of the cell without anything transmitted. No DL replay attacks are possible in this method, since this channel carries indications from multiple UEs in the ULThere are no privacy issues since this is a physical layer channel.

Advantage of System Query method: System is verified using a query, hence doesn't overload the SIB/MIB. In fact the scheme could be extended to cover SIB information in general rather than always broadcast over the air. UE uses the pre-provisioned Public Key of Trusted CA to validate the signature, and once it is validated, the UE accepts the Public Key of the Serving System as trusted.

Drawback of system query method: An Idle mode UE is made to transmit a query message to verify the gNB thus losing power.

Editor's Note: It is FFS how the UE can determine the correct coverage area of the gNB.

Editor's Note: It is FFS whether it can be required that the UE has a GPS receiver.

Editor's Note: It is FFS whether solution 1 can be defeated by using fake UEs in addition to a fake gNB or whether the fake gNB could generate UL traffic posing as a UE.

5.4.4.5 Solution #4.5: Prevent User Plane DoS Attack over Air Interface for Small Data

5.4.4.5.1 Introduction

This solution addresses key issue #4.6

In key issue 5.4.3.6 of TR 33.899, it discussed about the user plane DOS attack that might be caused by the small data from UE. It mentioned that, in TR 23.799, some solutions for infrequent small data transmission are proposing the absence of user plane AS security. However, in the absence of user plane AS security, the network may be exposed to denial of service (DoS) attacks. Therefore, for the NextGen systems, the AS layer should have a way to deter or filter bogus user plane packets injected by unauthorized devices or applications (e.g., malware). At the same time, in the normal operations (i.e., in case of no identified ongoing attacks), the NextGen network should support efficient transmission of small data by UE as intended.

In this solution, we proposed to use Identity-based public technology to solve the DOS attacks that may appear in the AS layer and also allow the normal UE to transmit small data. To use the Identity-based technology for signature generating and verifing according to RFC 6507 [33], the sender need to be provisioned with a SIGN-Key, (PVT, SSK), which are generated according to its ID and KMS parameters, and are also provisioned with the KMS Public Authentication Key (KPAK). The sender can sign the message with the SSK, and KPAK. A verifier need to be provisioned with the KPAK. The sender needs include its ID, PVT together with the data and a signature generated. A receiver can verify the message with its KPAK and the received ID, PVT, data and signature.

5.4.4.5.2 Solution details

In this solution, we propose to use the Identity-based public technology to filter out bogus data packets injected by unauthroized users. We assume that the Credential Repository play the role for KMS and generate Identity-based SING-Keys for UE. KMS of different operator may use different KMS public authentication keys. At the same time, it allows normal users to transmit there data to the network. The proceduers are as follows:

1. RAN is provisioned with Identity-based KMS public key for signature verification

   1.1 RAN is provisioned with Identity-based KMS Public Authentication Key (KPAK).

   1.2 RAN stores the KPAK. KPAK is used by RAN to verify the signature contained in the small data packet from the UE.

2. UE is proviseioned with Identity-based Keys

   2.1 UE perform a mutual authentication with AUSF/SEAF and sets up a secure connection with the core network.

Lenovo Ex. 1007
Page 302

2.2 AUSF/SEAF notify the KMS of the authentication results

2.3 KMS provision UE with Identiy based keys, including UE's temporary ID (ID_UE), PVT_{ID_UE}, SSK_{ID_UE}, and KPAK.

2.4 UE stores the ID_UE, SSK_{ID_UE}, PVT_{ID_UE}, and KPAK.

2.5 UE shall release the connection with the network.

NOTE: ID-based keys can be used for certain period, e.g. one week, after the connection is released. A new key can be provisioned after the current key expires.

3 UE using the Idenity-based SING-Keys to sign the small data

3.1 When UE receives data from upper layer, it finds KPAK, PVT_{ID_UE}, and SSK_{ID_UE} and computes signature for the data with above parameters.

3.2 UE transmits data message that contains ID_UE, PVT_{ID_UE}, timestamp, data and the generated signature to the RAN. The timestamp is used to prevent replay attack.

3.3 After receiving the data from UE, the RAN Verify the signature of data with UE_ID, PVT_{ID_UE}, and KPAK. If the data passes the verification, then RAN forward the data message to the core network, else, it drops the data.

3.4 UE transmit the data to the core network handling function for further processing.

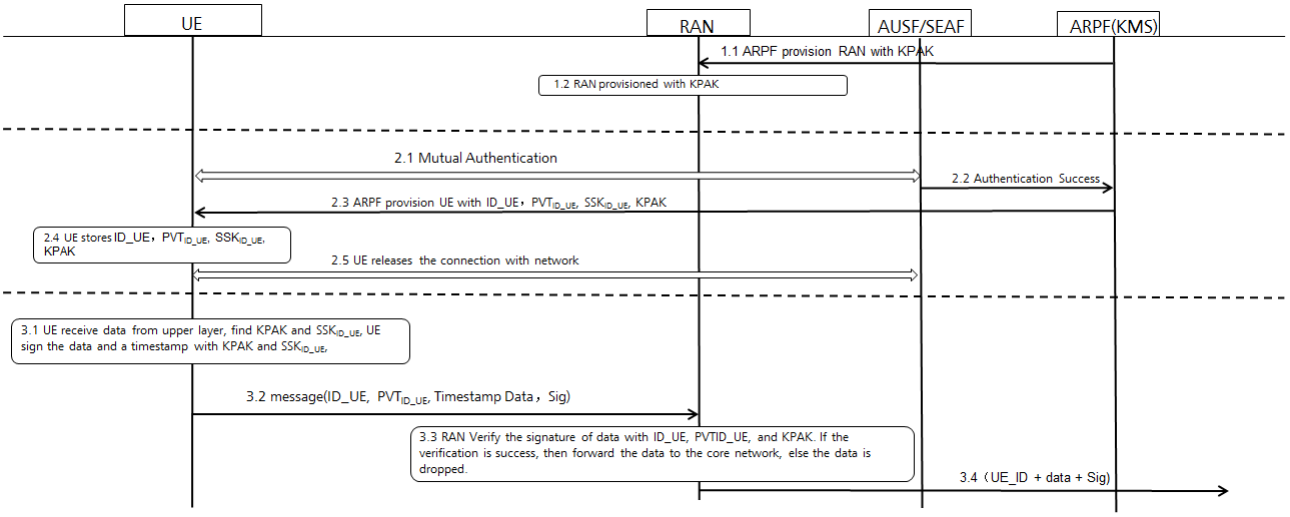


Figure 5.4.4.5.2-1: UP plane data verification using Identity-based Digital Signatures

Editor's note: The roaming case needs to be described more. E.g. how can a home operator know which network the user will roam to.

5.4.4.5.3 Evaluation

DOS attack at air interface: with the proposed solution, the RAN needs to verify the signature of the small data. However, considering that the small data is transmitted with low frequency, and each RAN only allocate part of its radio resource for small data transmission, therefore, the verification of signature for small data is unlikely cause DOS attack. On the other hand, with the signagure verification, the RAN can prevent UE from perfoming DDOS attack to core network nodes.

Editor's Note: It is ffs performance impact of ID based signature verification on UE and RAN

Editor's Note: It is ffs security aspects of storing Identity based private key (SST). This is closely tied to decisions taken in security area 8.6.5

Lenovo Ex. 1007
Page 303

5.4.4.6 Solution #4.6: Security mechanism for deployment scenario of option 3

Editor's Note: The SA3 study of security aspects of dual connectivity should be aligned with progress in the on-going study of dual connectivity in RAN2 and RAN3

5.4.4.6.1 Introduction

This solution addresses key issue #4.8 "Security aspects for deployment scenario of option 3".

5.4.4.6.2 Solution details

Security mechanism is provided for deployment scenario of option 3 with the following points.

- UE's authorization to access NR (New Radio) is checked
- UE's capability to access NR is checked before starting security procedure to select appropriate security algorithm
- Information on UE's capability and authorization to access NR is stored in initial attach phase in eNB to make security procedure efficient

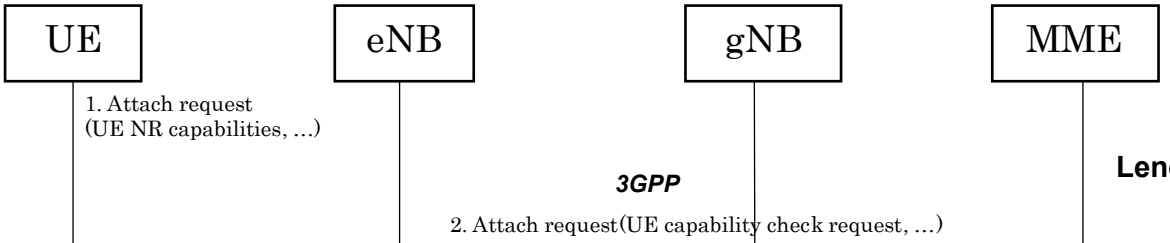
Procedures of initial attach and gNB addition for option 3 with security mechanism are shown in Figures 5.4.4.6.2-1 and 5.4.4.6.2-2, respectively.

Initial attach procedure is carried out with the following steps:

1. Attach request with UE NR capability is sent from UE to eNB.
2. eNB sends the attach request from UE to MME.
3. MME checks UE's capability and subscription to access NR.
4. MME sends attach response to eNB with the check results of the information.
5. eNB sends the attach response from MME to UE.
6. eNB stores the information on the UE capability.

gNB addition procedure is carried out with the following steps:

1. RRC connection is established during which IDs of security algorithm and KDF (Key Derivation Function) for U-Plane protection between UE and gNB requested by UE and UE capability are sent to eNB.
2. eNB checks that the UE is authorized to access gNR based on the stored information whether the UE is authorized to access gNB.
3. eNB derives a key (K_{AN}) for U-plane protection between UE and gNB.
4. eNB sends gNB addition request with K_{AN}, IDs of security algo./KDF and UE capability to gNB.
5. gNB decides security algo./KDF based on the received information.
6. gNB sends the IDs of decided algo./KDF to eNB. If the decided algo./KDF is different from the ones requested by UE, eNB derives K_{AN} using the decided ones and send K_{AN} to gNB again.
7. eNB sends RRC connection reconfig request to UE with IDs of the decided algo./KDF.
8. UE sends RRC connection reconfig response to eNB.
9. eNB sends gNB Reconfiguration complete message to gNB.
10. Activation of encryption/decryption is carried out in UE.
11. Activation of encryption/decryption is carried out in gNB.



3GPP

Lenovo Ex. 1007
Page 304

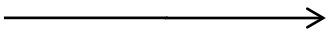


Figure 5.4.4.6.2-1: Initial attach procedure for option 3

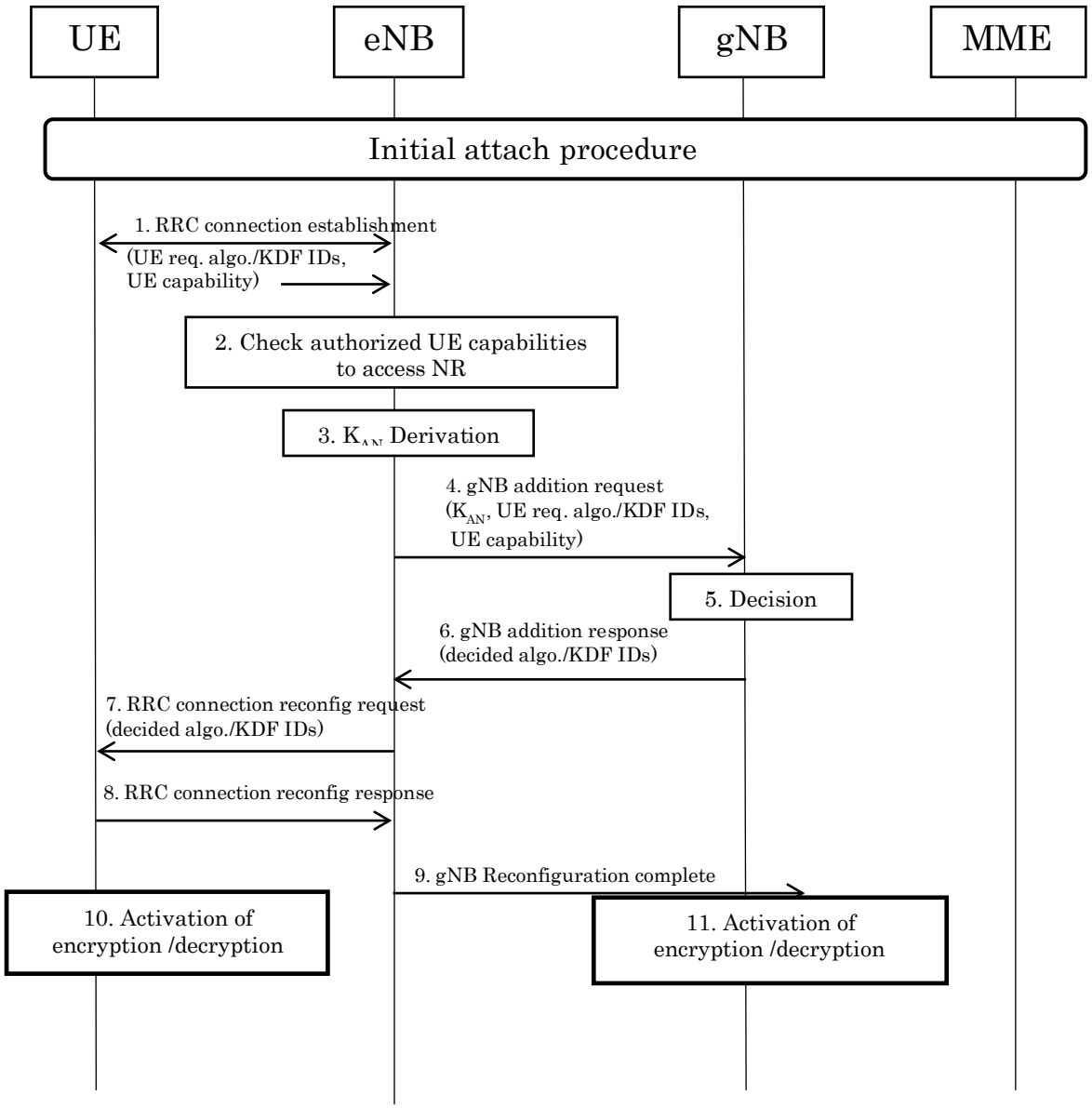


Figure 5.4.4.6.2-1: gNB addition procedure for option 3

5.4.4.6.3 Evaluation

FFS

5.4.4.7 Solution #4.7: Handover procedure for Intra NG (R)AN

5.4.4.7.1 Introduction

This solution proposes the Handover procedure for Intra NG (R)AN scenario where UE moves from one cell to another cell within same NG (R)AN.

Lenovo Ex. 1007
Page 305

5.4.4.7.2 Solution details

Figure 5.4.4.7.2-1 shows the handover procedure for Intra NG (R)AN of non-roaming scenario. This solution assumes that the similar service capability is available across all the cells serviced by the given NG (R)AN.

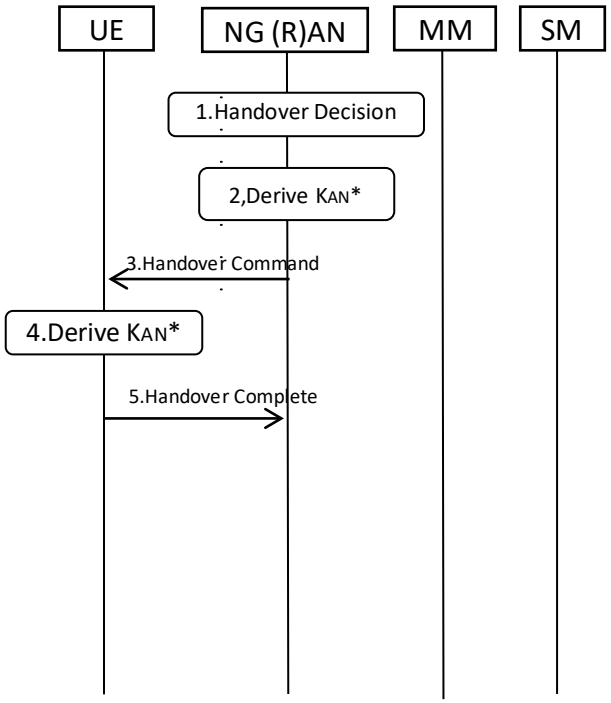


Figure 5.4.4.7.2-1 Call flow for Handover procedure of Intra NG (R)AN

29. When handover within the NG (R)AN is required, the NG (R)AN makes the handover decision.
30. It refreshes the AN keys (derives KAN* and the subsequent RRC and UP integrity and encryption keys).
31. NG (R)AN sends the handover command to the UE
32. Using the parameter sent in the Handover Command, the UE derives the KAN* and the subsequent RRC and UP integrity and encryption keys.
33. UE sends the handover complete to NG (R)AN

Editor's Notes: Mandatory key changes at handover is FFS.

Editor's Notes: Terminology needs to be aligned with RAN2 and RAN3

5.4.4.7.3 Evaluation

FFS

5.4.4.8 Solution #4.8: Fake gNB Detection using Identity Based Signature

Editor's Note: It is FFS to check if solution addresses the general case of the key issue.

5.4.4.8.1 Overview

The proposed solution tries to solve following key issue section 5.4.3.1 as follows:

"

In the LTE system, UE obtains some services in the RRC idle state. In the RRC idle state, UE acquires the system information from the camped cell and uses them to receive paging and obtain other services such as MBMS, D2D, etc. in RRC idle state. When the UE select a cell in RRC idle mode, it does not validate whether the eNB is authentic or fake. As a result, UE may camp to a

Lenovo Ex. 1007
Page 306

rogue cell leading to denial of services (such as public safety warnings, incoming emergency calls, real-time application server push services, proximity services, etc.).

"

If the UE camps on a fake cell during RRC Idle state (and there is no authenticity verification done), then the attacker can successfully mount DoS attack on the UE.

One of the example of RRC idle mode bidding down attack where a UE is camps with fake gNB and UE is redirected to another GSM network, 2G network with lower security. Following Figure 5.4.4.8.1-1 shows one of the possible ways an unprotected RRC connection release message from a fake 5G eNB/gNB with redirection to another GSM network, 2G network with lower security.

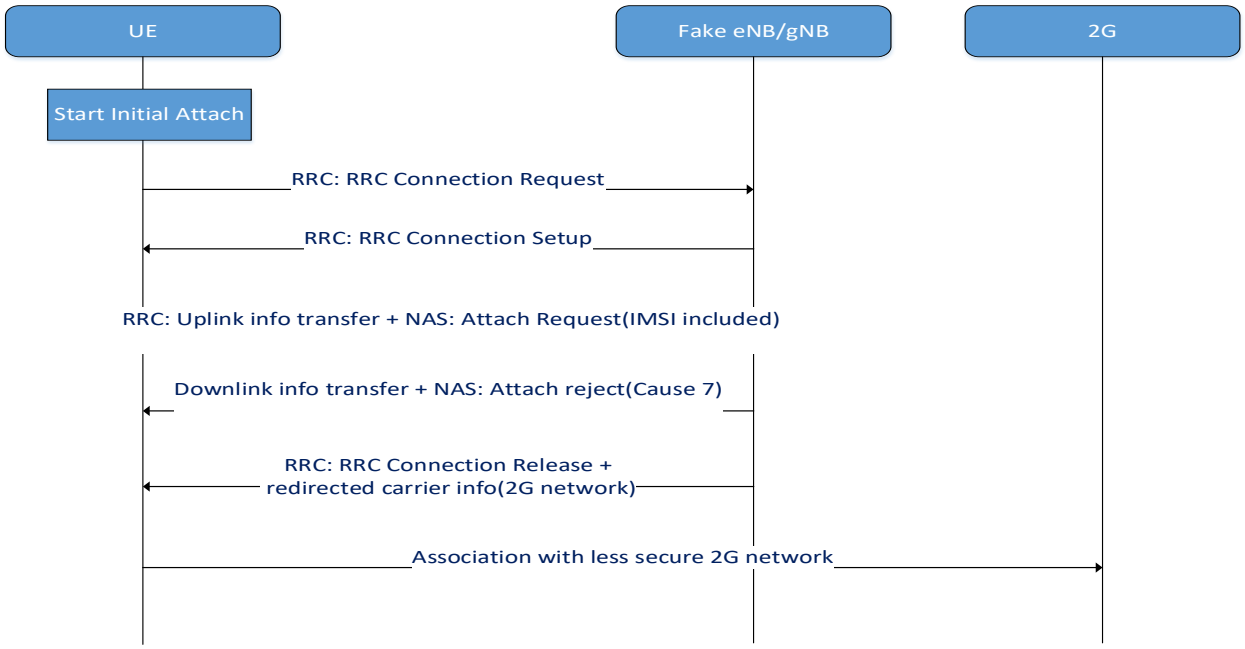


Figure 5.4.4.8.1-1: Bidding Down Attack

In this proposed solution, we use an Identity based authentication and encryption enabling UE to verify authenticity of the the eNB/gNB that it is going to connect during Cell reselection or cell redirection. The Identity based mutual verification system can achieve detection of fake gNB/eNB.

When UE receives a cell redirection message, the UE may verify the authenticity of eNB/gNB. This is achieved by executing Verify-Request and Response message exchange protocol between UE and eNB/gNB.

5.4.4.8.2 Solution Details.

Following pre-conditions are assumed:

1. The UEs and eNB/gNBs are provisioned with the required credentials (as defined in RFC 6507 [14] and RFC 6508[24) in advance when the UEs have secure access to their Key Management Server (KMS).

2. The KMS, common root of trust for the UEs, eNB/gNB, provisions the UEs with a set of credentials for ECCSI and SAKKE schemes.

3. Upon successful provisioning for ECCSI, each UE and eNB will be configured with the public key of the KMS, and a set of credentials associated with the UE's identity, which is:

Lenovo Ex. 1007
Page 307

Secret Signing Key (SSK) and Public Validation Token (PVT). The UE must act as "signer" and "verifier." As a signer, the UE uses its SSK to sign a message, and when acting as a verifier, the UE uses the public key of the KMS and the signer's PVT to verify the signature.

4. Upon successful provisioning for SAKKE, each UE will be configured with the public key of the KMS, and a Receiver Secret Key (RSK) which is associated with the UE's identity. The sender UE uses the eNB/gNB identity (receiving entity for SAKKE payload) and the public key of the KMS to create an encrypted SAKKE payload. The eNB/gNB uses its identity, its Receiver Secret Key and the public key of the KMS to decrypt SAKKE payload.

5. The public identity of a UE may be encoded in any format that is compatible with the guidelines provided in RFC 6509 [12]. For example, the public identity of a UE may be a concatenation of a fixed part (in the form of IMSI, SIP URI, TEL URI, other user@domain types of URI, etc.) and a varying part (in the form of a timestamp). RFC 6509 provides some examples, like IMSI:expiration-date@domain.com

6. To avoid signaling overhead concern, this Verify-Request, Verify-Accept does not need to be performed all the time. One optimization may be to send Verify-Request only during the RRC Connection Release message with Cell-Redirection is received by UE.

Figure 5.4.4.8.2-1 shows high-level steps.

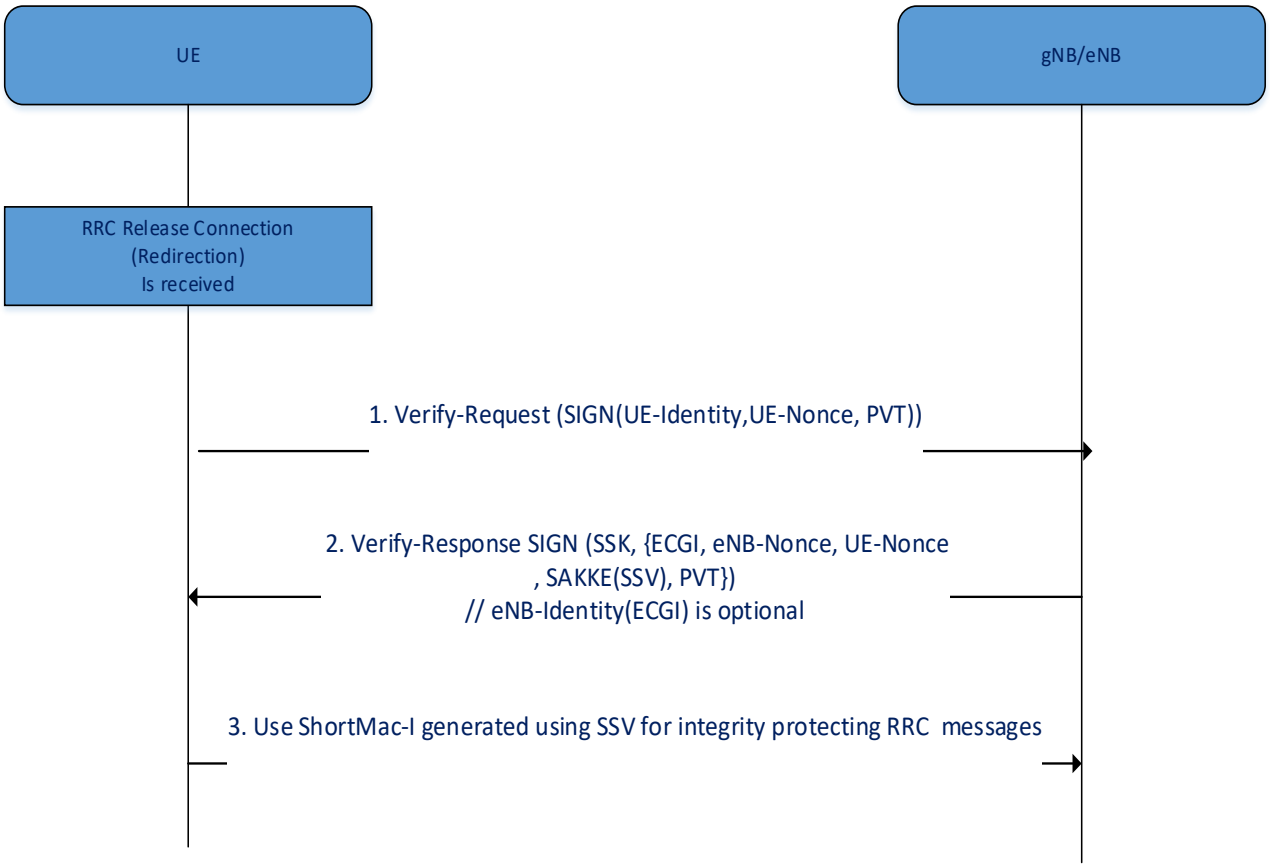


Figure 5.4.4.8.2-1: Fake gNB detection using IBS

1. UE sends Verify-Request message to the eNB (or the Common Control Function (CCNF) where the NAS context of the UE is held).

Lenovo Ex. 1007
Page 308

i. Verify-Request message includes the following parameters:

1. UE Identity
2. UE Nonce
3. PVT (Public Verification Token)
4. SIGN – an ECCSI signature is computed over the UE Identity and UE-Nonce.

2. Verify-Response is generated by the Serving System network element (eNB or CCNF). Upon reception of the Verify-Request message, eNB verifies the signature payload SIGN in the verify-request message. If the verification test is successful, eNB sends a Verify-Accept message including the following parameters:

i. eNB Identity = This information is used to derive the Signer's identifier (used by ECCSI). eNB identity is optional.

ii. eNB Nonce

iii. UE Nonce

iv. PVT (Public Verification Token)

v. SSV (Shared Secret Value) generated by eNB and encrypted using SAKKE

vi. SIGN – an ECCSI signature of the Verify-Response message. The signature is computed over the User of eNB Identity, Nonce-UE, Nonce-eNB and the SAKKE parameters (Shared Secret Value as follows).

3. Upon receipt of the Verify-Response message, the UE verifies the signature payload SIGN. If the verification test is successful, it decrypts SAKKE payload to extract the SSV which is used as a security association key between the UE and eNB. The UE and eNB use this key to derive integrity key for integrity protecting RRC messages.

4. Upon successful verification, UE may use the derived integrity key to protect RRC messages until the UE authenticates with eNB.(i.e. until AS Security context is established at EPC and UE).

5.4.4.8.3 Evaluation

This solution does not address the key issue #4.1. UEs in IDLE mode are not prevented from camping onto false base station.

5.4.4.9 Solution #4.9: Security of Access Stratum (AS) keys on Xn handover

5.4.4.9.1 Introduction

This solution addresses the key issue #4.15, "Security aspects of Xn handover" and covers the security of AS keys with respect to the backward/forward security.

Lenovo Ex. 1007
Page 309

5.4.4.9.2 Solution details

This solution proposes to re-use the security mechanism present in the X2 handover of the current LTE systems as much as possible, with some modifications. In the following text, the security keys used in the eLTE eNB and the gNB are respectively denoted as KeNB/KeNB* and KgNB/KgNB*.

NOTE: It is yet to be decided whether the keys used in eLTE eNB and the gNB will be same or have the same format, because the Next Generation Core (who may assign these keys) may not need to know if the RAN node is an eLTE eNB or a gNB.

Re-using existing mechanism/properties: The following mechanisms/properties are proposed to be adapted from the X2 handover of the current LTE systems:

- horizontal key derivation
- vertical key derivation with the help of Next Generation Core
- use of the target RAN node's properties for the derivation of the security keys (e.g., E-ARFCN and PCI in case of eLTE eNB) so that it is possible to prepare multiple target RAN nodes with different security keys
- 1 hop backward security
- 2 hop forward security
- support for deriving both 128-bit encryption/integrity keys and 256 bit encryption/integrity keys from the KeNB/KgNB
- support for the target node to select different encryption/integrity algorithms compared to the source node

Potential new mechanisms/properties: The following new mechanisms/properties are proposed to be considered in the Xn handover of the NextGen systems:

- support for retaining the security key (i.e., not refreshing the security key when not needed)
- enhancements to key refresh mechanism (e.g., allowing RAN nodes to trigger key refresh regularly without excessive signalling or computational overhead)

5.4.4.9.3 Evaluation

TBD

5.4.4.10 Solution #4.10: UE-assisted false base station detection

5.4.4.10.1 Introduction

This solution relates to the key issue #4.1, i.e. "AS security during RRC idle mode".

The issue of an UE selecting a false base station to camp on, during IDLE mode, could be addressed in following two ways:

- Type 1: Prevent the UE from camping on a false base station in the first place.
- Type 2: Let the UE camp on a false base station. But, detect that the UE camped on a false base station when the UE connects back to the genuine network.

This solution is of Type 2. Questions like whether the Type 1 solutions (currently proposed for #4.1), are feasible or not and whether the proposed Type 2 solution is sufficient or not are discussed in the evaluation clause.

Editor's Note: This solution does not prevent UE from camping on a fake cell.

5.4.4.10.2 Solution details

This solution builds upon the existing measurement report mechanisms described in the TS 36.331.

Lenovo Ex. 1007
Page 310

When the UE is in RRC_CONNECTED mode, the gNB sends configuration information to the UE in a protected RRC message, asking the UE to perform and log measurements when the UE is later in RRC IDLE mode. The existing "Logged Measurement Configuration" procedure may be used for doing so. It is left up to the implementations to decide for which UEs or in which tracking areas (TAs) the measurements are activated. For example, during some important social event, the network may choose to activate the measurements only for vulnerable subscriber's UEs and in the areas close to the event location.

When in RRC_IDLE mode, the UE builds the measurement reports according to the configuration information that was sent by the gNB. The existing "MeasResults" message may be used for the same purpose This already allows to obtain various information relevant for false base station detection, e.g. identifier and received-signal strength information of the cell that the UE camped on, and detailed location information of the UE. In addition to the existing information, it is proposed that the following new information (belonging to the cell that the UE camped on) is included in the report:

- mib_info = hash of the MIB; and
- sib_info = list of {SIB number, hash of the SIB}.

When the UE transitions later to RRC_CONNECTED mode, the UE sends the measurement reports in a protected message to the gNB. A transition to the RRC_CONNECTED mode means that a successful security activation has taken place and the UE is connected to a genuine gNB. The existing "Measurement Reporting" procedure may be used for doing so.

The gNB, possibly with assistance from the core network or neighbouring gNBs, detects the false base station by determining if the hashes of the MIB and the SIBs are correct; the reported received-signal strength of the cell matches the reported location of the UE; or the UE did not respond to the Paging message even when the UE was successfully camping.

Editor's Note: Privacy aspects related to measurement and location reports are FFS.

Upon detection of the false base station, the operator can take further actions, e.g. informing legal authorities; or contacting the victim subscriber.

It is proposed to leave it open to the implementations to use other techniques on using the measurement reports and on taking actions, than mentioned above.

5.4.4.10.3 Evaluation

Two types of solutions, Type 1 and Type 2 were mentioned in the introduction clause.

The Type 1 solutions that have been proposed so far for key issue #4.1 seem to be unfeasible or impractical to achieve without having considerable impact on the existing system.

- One proposal (solution #4.2) to achieve the Type 1 solution is that the network signs its broadcast messages, i.e. MIB and SIB. In order to mitigate the replay attack, the timestamp is used as one of the parameters to generate the signature and that timestamp needs to be transmitted along with the message. Further, to prevent the size of message from growing large, only some LSBs of the timestamp value are transmitted with the message, thereby allowing the network and the UE to be off-time within some limit, usually in the order of seconds. However, the MIB/SIB are transmitted more frequently than a second. For example, in LTE, the MIB is broadcasted every 40ms (repeated every 10 ms) and the SIB1 is broadcasted every 80 ms (repeated every 20 ms). Therefore, signing the broadcast message and including some LSBs of timestamp does not seem to be preventing the replay attack, meaning that the false base station attack is still possible.

NOTE: The above mentioned replay attack may not be applicable, when the digital signature is provided over the Other System Information (SIs). Whether those "Other SIs" are always mandatory for cell reselection or whether they are conditional depending upon network configuration is yet to be confirmed.

- Another proposal (first part of solution #4.4) is that the UE detects the uplink traffic towards the base station before camping on that base station. That approach has a serious security flaw because the UE is not able to detect genuine uplink traffic and hence the false base station can still trick the UE by generating fake UL signals. Further, that approach requires the UE to have an uplink (UL) receiver.
- Yet another proposal (second part of solution #4.4) is that the UE verifies the authenticity of the gNB by sending a new "System Query" message. Doing so defeats the purpose of the IDLE mode since it requires some level of activity form the UE.

Lenovo Ex. 1007
Page 311

The Type 2 solution that is proposed seems to be simple and sufficient.

- The proposal of Type 2 solution that uses already existing measurement reporting mechanisms [TS 36.331] has only a minimal impact on the system. The necessity of having minimal impact is stated as an Editor's Note in the requirements sections of the key issue #4.1.
- Detecting the false base station seems to be a sufficiently good enhancement, which can help the legal authorities to track and actually locate the attackers.
- The network is able to activate the measurement reporting on selected UEs or in selected areas, which means efficiency in signalling and computation.
- Allowing the network to collect the information and to use the information in implementation specific way, enables the network to adapt quickly to the evolving attack methods.

5.4.4.11 Solution #4.11: Security of sidehaul interfaces

5.4.4.11.1 Introduction

This solution addresses the key issue #4.10, "Security aspects of sidehaul interfaces".

5.4.4.11.2 Solution details

It is proposed that the protection of the Xn and Xx interfaces in the Next Generation systems are based on the similar solution in the LTE systems, i.e. using NDS/IP as specified in TS 33.210.

5.4.4.11.3 Evaluation

TBD

5.4.4.12 Solution #4.12: Security Aspects of Option 3/3a/3x or EN-DC

5.4.4.12.1 Introduction

This solution addresses Key Issue 4.3 for the Dual Connectivity (DC) architecture options 3/3a/3x (Non-Standalone NR with LTE anchor, EPC connected) or E-UTRA-NR Dual Connectivity (EN-DC)

5.4.4.12.2 Solution details

Options for Data Radio Bearers or DRB termination:

The protocol architecture for Option 3 (MCG split bearer) / 3a (SCG bearer) is shown in the below figure.

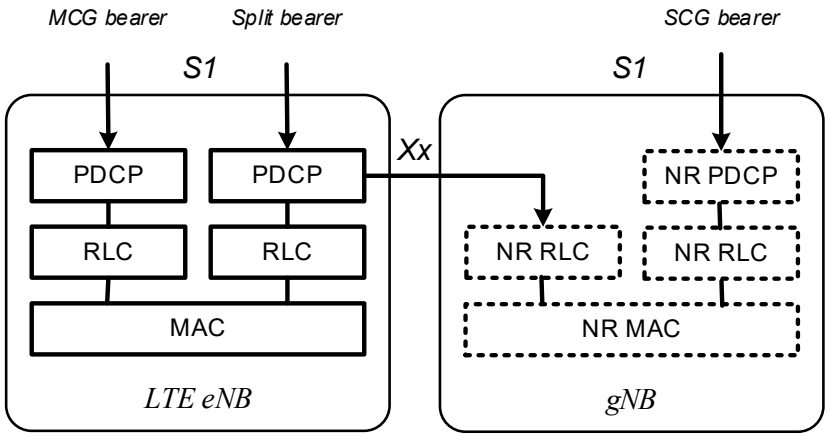


Figure 5.4.4.12.2-1: Architecture for Option 3 and 3a

Lenovo Ex. 1007
Page 312

The protocol architecture for SCG split bearer in Option 3x (SCG split bearer) is shown in the below figure.

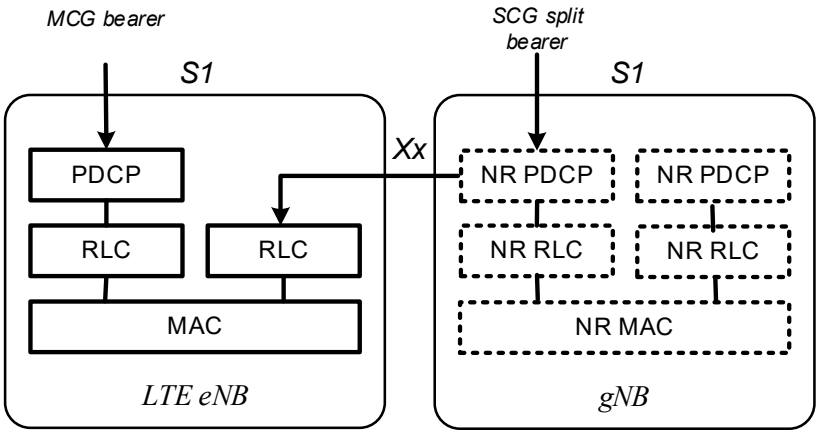


Figure 5.4.4.12.2-2: Architecture for Option 3x

In option 3 (MCG split bearer), the PDCP for the split bearer terminates at the eNB and therefore the standard LTE PDCP encryption applies and no security impacts are foreseen for the NR/gNB (Secondary gNB). Therefore, it can be concluded that Option 3 does not have any security impact on NR/gNB.

In option 3a (SCG bearer), the PDCP for the SCG bearer terminates at the gNB. This means the PDCP encryption for these bearers terminates at the gNB.

There are two possible solutions for supporting PDCP encryption.

NOTE: If the integrity protection over NR needs to be supported, then the below solutions can be easily extended to support integrity protection. However, the integrity protection can be provided only for bearers that terminate at the gNB.

Solution 1: NR supports the same security algorithms as LTE.

In this solution, the Dual Connectivity security procedures defined in Annex E of TS 33.401 can be reused as is with the gNB. This is because, LTE eNB (MeNB) can send the received UE EPS security capability to the gNB and the gNB can use it to select one of the supported encryption algorithm.

The benefit of this solution is that there is no security impacts on the LTE eNB due to NR. The disadvantage is that gNB can only use the same algorithms as the LTE algorithms.

Solution 2: NR may support different security algorithms than LTE

Variant 1:

In this solution, LTE eNB needs to be aware that it is working with NR/gNB and the Dual Connectivity security procedures defined in Annex E of TS 33.401 can be reused with relatively minor security enhancements to the eNB. If the eNB does not have the NR security capabilities of the UE, then the eNB requests those using the UECapabilityEnquiry message (see 5.6.3 of TS 36.331). It then passes NR security capabilities of the UE to the gNB. The response for the chosen algorithms is included in a transparent container that is protected in the RRC message when sent from the MeNB to the UE.

The benefit of this solution is that it allows the option for NR to select a different security algorithms than in LTE. The disadvantage is that it impacts eNB. However, if the eNB is anyhow impacted for supporting integration of NR for non-security reasons, then this solution is preferable to solution 1, as it allows for security algorithms of LTE and NR to evolve independently.

The following can be concluded for Option 3a:

- Option 3a can be supported without any security impacts to DC security procedures defined for LTE or with relatively minor enhancements to it.
- Option 3a, solution 2 is preferred if the impacts to eNB are acceptable.

Lenovo Ex. 1007
Page 313

In option 3x (SCG split bearer), for both the SCG split bearer and the SCG bearer, the PDCP encryption terminates at the gNB. From security point of view, the security procedures defined for option 3a can be reused for 3x. Therefore, it can be concluded that Option 3x can reuse the security procedures defined for Option 3a.

Variant 2:

Similar as in Variant 1, this variant implies that the LTE eNB must be aware that it is working with a NR/gNB, and the Dual Connectivity security procedures defined in Annex E of TS 33.401 can be reused with relatively minor security enhancements to the eNB.

Instead of letting the LTE eNB to request the NR security capabilities of the UE by using the UECapabilityEnquiry message (see 5.6.3 of TS 36.331) as proposed in Variant 1, this variant (Variant 2) proposes that the UE indicates support for new security algorithms in NR in NAS layer to the MME. The MME then indicates to the LTE eNB over S1 interface the UE support for the new security algorithms in NR.

Editor's Note: Impact and feasibility of Variant 2 w.r.t. MME is to be confirmed by CT1.

Figure 5.4.4.12.2-3, the call flow for Variant 2 based on Rel-12 DC.

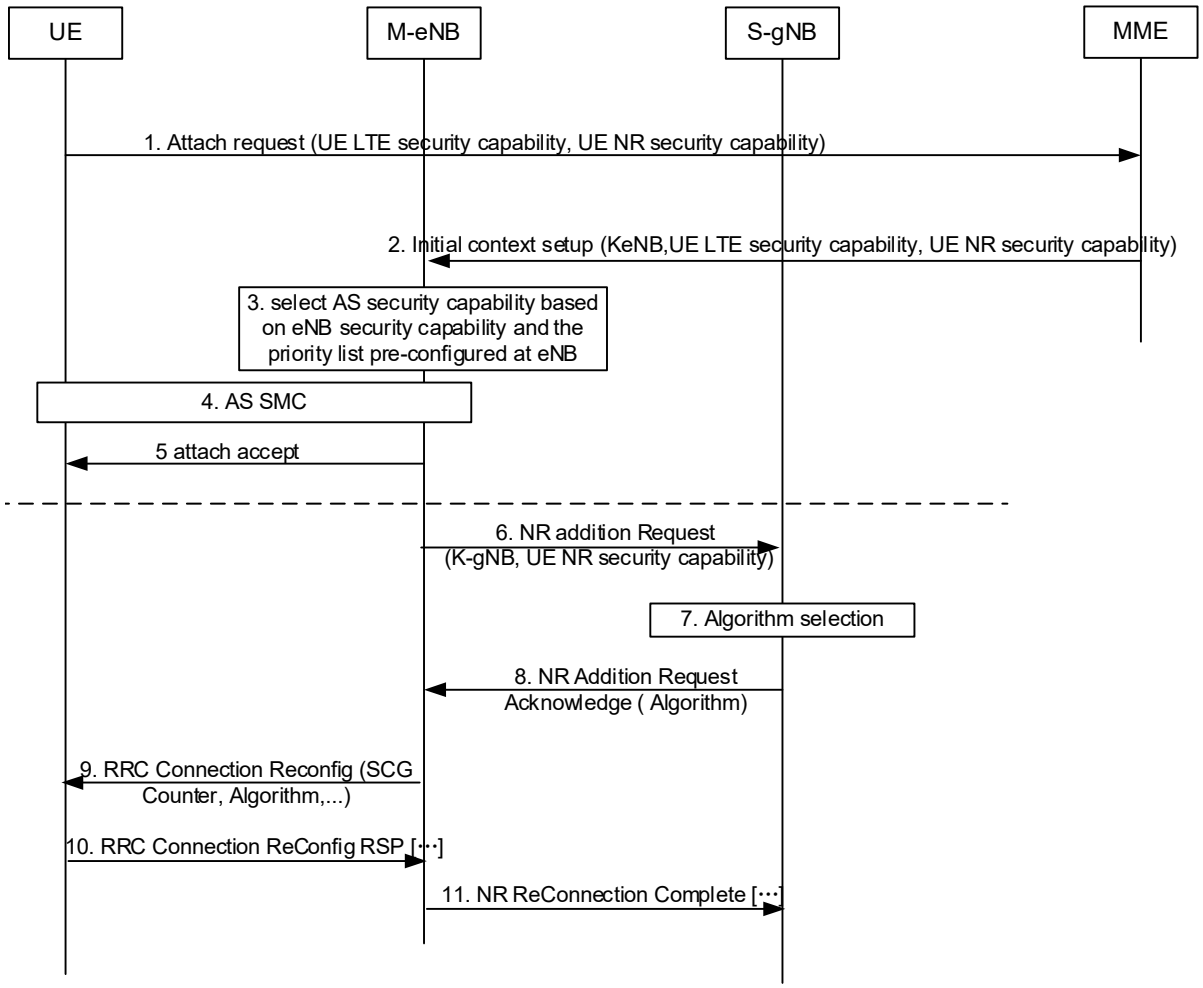


Figure 5.4.4.12.2-3 eNB obtains NR security capability through Initial context setup message

NOTE: This call flow shows MeNB always sending the NR capability to the SgNB. It may be possible that after repeated handover between un prepared MeNBs, this NR capability information may be lost at the MeNB

Editor's Note: The above call flow needs to be revised to separate the initial Attach request procedures from the eNB handover procedures.

In step 1, UE shall put the UE LTE security capability and the NR security capability into attach request message that terminates at MME.

Lenovo Ex. 1007
Page 314

Step2, all the security capability will be forwarded to M-eNB with KeNB in Initial context setup message.

Editor's Note: How does the NR security capabilities get passed to the MeNB if the UE either connects or hands over to a legacy eNB (i.e. one that does not understand the NR security capabilities) between becoming active and the bearer being established on the SgNB.

Step3, the eNB will send AS SMC to the UE after selecting eNB security capability, while the NR security capability shall be stored at eNB for future use.

Step6, when M-eNB decides to perform EN-DC, the UE NR security capability will be transferred to S-gNB through NR addition Request message.

Step7, S-gNB selects UP security capability based on received UE NR security capability and the priority list, then sends the select security capability in NR addition Request Acknowledge message in step 9.

Options for Signalling Radio Bearer or SRB termination:

The SRB termination for EN-DC is shown in the figure 5.4.4.12.2-4.

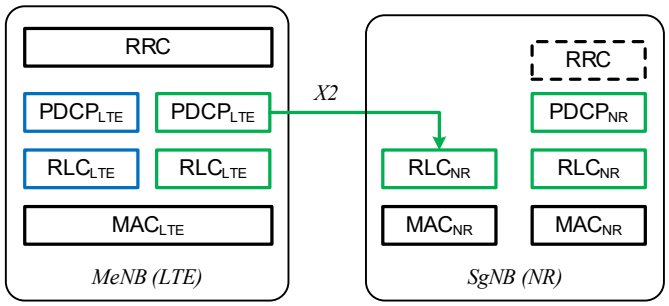


Figure 5.4.4.12.2-4: SRB termination: MCG SRB, MCG split SRB and SCG SRB

For the MCG SRB and the MCG split SRB, the PDCP layer terminates in the MeNB. Therefore, LTE PDCP ciphering and integrity protection for RRC messages can be used as is with EN-DC.

For the SCG SRB, the PDCP layer terminates in the NR/SgNB. Therefore, SCG SRBs need to use NR PDCP for ciphering and integrity protection of RRC message. The MeNB provides the S-KeNB to the SgNB as in LTE only dual connectivity. S-KeNB is used by the SgNB to derive further keys for ciphering and integrity protection of RRC messages. These key derivation needs to be specified separately for NR.

5.4.4.12.3 Evaluation

The proposed solutions for Option 3/3a/3x have either no impact or relatively minor impacts to the eNB.

5.4.4.13 Solution #4.13: Inputs to security algorithms at PDCP layer

5.4.4.13.1 Introduction

This solution addresses the inputs to the security algorithm at the PDCP layer to ensure keystream freshness and ensure that integrity protection is unique to each bearer for Option 3 architectures (see Key Issue #4.3). It is preferable to be able to use the same solution for Options 3 and standalone cases. The solution is about how to use ciphering and integrity keys in the security algorithms at the PDCP layer and not how to generate those keys

5.4.4.13.2 Solution details

The input parameters to the integrity algorithms are an integrity key, the message, a bearer identity BEARER, the 1-bit direction of transmission DIRECTION and a bearer and direction dependent input COUNT which corresponds to the PDCP COUNT (see Annex B of TS 33.401 [31] for details).

NOTE: If bearer dependent keys are used, then the use of bearer identity may be redundant

Lenovo Ex. 1007
Page 315

The inputs to the ciphering algorithm are the same, except that the key is a ciphering key and the length of data to be protected is included so the correct amount of keystream can be generated.

5.4.4.13.3 Evaluation

This solution is a straight forward method of providing the inputs to the security algorithms at the PDCP layer that enable no keystream re-use and the ability to integrity protect the transferred data uniquely on each bearer.

5.4.4.14 Solution #4.14: Flexibile mechanism for AS key-change

5.4.4.14.1 Introduction

The proposed solution completely addresses the key issue #4.11 on flexibility to retain or to change AS security keys and is related to key issue #3.2 on key refreshing.

5.4.4.14.2 Solution details

The proposed solution is illustrated in Figure 5.4.4.14.2-1. The UE communicates with the source cell over-the-air using radio interface (called Uu interface in LTE). The source cell and the target cell communicate via an interface known as Xn. If both the source and target cells are handled by same RAN node or in centralized RAN deployments, all the aspects of Xn are handled internally by the RAN node. Only few steps are shown in the figure for the sake of simplicity. The corresponding descriptions of the shown steps follow the figure.

Lenovo Ex. 1007
Page 316

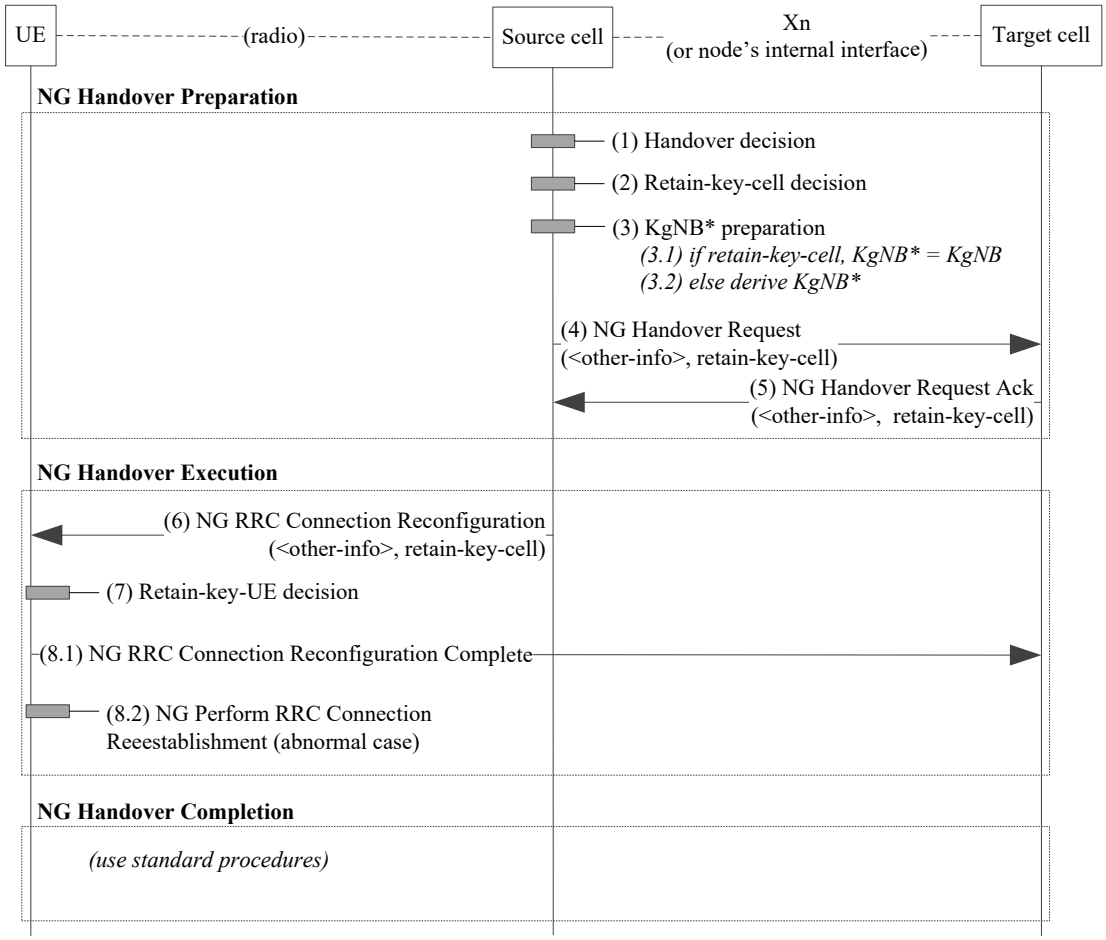


Figure 5.4.4.14.2-1: Flexibile mechanism for AS key-change

NG Handover Preparation

(1) The source cell decides to perform handover.

(2) The source cell decides whether to retain the key or not (denoted retain-key-cell).

(2.1) If the key (denoted KgNB) is to be retained, then retain-key-cell = true. The decision may depend upon one or more criterias, for example, the target cell belonging to the same PDCP anchor as the source cell, subscription specific or general policy sent by the core network, negotitation with the UE, etc. Details should be worked out in normative phase.

(2.2) Else, retain-key-cell = false.

(3) The source cell prepares the KgNB* taking Step (2) into account.

(3.1) If retain-key-cell is true, the source cell reuses the old key, i.e., KgNB* = KgNB.

(3.2) Else, the source cell derives a KgNB*, for example, horizontal or vertical derivation using KgNB.

(4) The source cell sends NG Handover Request, containing the retain-key-cell value, to the target cell. Doing so is aligned with the existing mechanism in LTE for sending KeNB* and NCC values (see Clause 9.1.1.1 and 9.2.30 in 3GPP TS 36.423).

(5) The target cell sends NG Handover Request Ack, containing the retain-key-cell value in transparent container, to the source cell. Doing so is aligned with the existing mechanism in LTE for sending HandoverCommand message (see Clause 9.1.1.2 in 3GPP TS 36.423, and clause 10.2.2 in 3GPP TS 36.331).

NG Handover Execution

Lenovo Ex. 1007
Page 317

(6) The source cell sends NG RRC Connection Reconfiguration message, containing the retain-key-cell value, to the UE.

(7) The UE decides whether the retain-key-cell is acceptable or not (denoted retain-key-UE). It is important to have a check at the UE side in order to prevent the networks from never refreshing the keys. The decision may depend upon one or more criterias, for example, policy set by or negotiated with the network, requiring key change when tracking area or RAN group changes, requiring key change when RAT changes, when key change counter exceed the some maximum value, etc.

Editor's Note: The details of the negotiation for this step (7) are ffs.

(8) Depending upon the decision in Step (7), the UE does following:

(8.1) If retain-key-UE is true, the UE sends NG RRC Connection Reconfiguration Complete to the target cell. The old AS keys are retained.

(8.2) Else, the UE performs NG RRC Connection Re-establishment (compare with clause 5.3.5.1 in 3GPP TS 36.331), which retuls in new AS keys (compare with clause 5.3.7.5 in 3GPP TS 36.331).

NG Handover Completion

Standard handover completion procecures are continued.

NOTE: Roaming UEs could also log the key change characteristics of the visited network and report the log to the home network. Doing so could be helpful in adjusting the UE's setting/policy, roaming agreement negotiation, etc.

5.4.4.14.3 Evaluation

The solution completely addresses the key issue #4.11.

It enables the NextGen network to optimize the RAN efficiency by allowing to retain or change the AS keys at HO.

It also prevents the poor policy/implementation at the network side by putting a control or check at the UE side.

There might be concerns that the decision of the network to retain or change the keys reveals the cell topology, which could be a problem. But, it is not a problem or a new issue. Note that already in LTE, information like TA list, MME code, etc., reveal some sort of network topology and are not considered problem.

5.4.4.15 Solution #4.15: Deriving ciphering and integrity keys in 5G

5.4.4.15.1 Introduction

This solution addresses the inputs to the KDF to derive the ciphering and integrity keys for 5G.

5.4.4.15.2 Solution details

The solution follows that used in LTE (see Annex A. of TS 33.401[31]) and proposed to use the KDF described in TS 33.220 [27].

NOTE: The master key varies depending on which ciphering and integrity key are being derived in the key hierarchy, e.g. in LTE the master key for NAS ciphering and integrity keys is K_{ASME} and the master key for deriving the RRC and UP ciphering and integrity keys is the K_{eNB}.

When deriving keys for the integrity and encryption algorithms from a master key for a particular case, the following parameters shall be used to form the string S.

- FC = 0x??

NOTE: An FC value will need to be assigned, but should be different to LTE.

- P0 = algorithm type distinguisher

- L0 = length of algorithm type distinguisher (i.e. 0x00 0x01)

Lenovo Ex. 1007
Page 318

- P1 = algorithm identity
- L1 = length of algorithm identity (i.e. 0x00 0x01)

Editor's note: 5G may require more inputs to the key derivation algorithms, e.g. if bearer dependent keys are used.

The algorithm type distinguisher is used to identify the use case that the key is being derived for, e.g. encryption of NAS message, integrity protection of RRC signalling (see Annex A.7 of TS 33.401 [31] for how it is done in LTE

The algorithm identity shall identify the particular 5G security algorithm that is being used (see clause 5 of TS 33.401 [31] for the assignment of values for LTE with a similar method to be used in 5G).

For an algorithm key of length n bits, where n is less or equal to 256, the n least significant bits of the 256 bits of the KDF output shall be used as the algorithm key.

5.4.4.15.3 Evaluation

This solution is a straight forward method of providing the inputs to the key derivation of ciphering and integrity keys to ensure that different keys are generated for different usages of the security algorithms (e.g. NAS ciphering and RRC integrity – see P0 part of the input) and for a given usage the keys are different when a different algorithm is used (see the P1 part of the input).

5.4.4.z Solution #4.z: <solution name>

5.4.4.z.1 Introduction

Editor's note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the security area.

5.4.4.z.2 Solution details

5.4.4.z.3 Evaluation

5.4.5 Conclusions

5.4.5.1 AS security during RRC idle mode (Key issue #4.1)

For key issue #4.1 "AS security during RRC idle mode", the available solutions can be grouped into two types. First one is a prevention type (solutions #4.2, #4.4, and #4.8) and another is a detection type (solution #4.10). Both types have advantages and can co-exist together.

- Prevention type solution is, in principle, preferred because UEs could be protected from camping to false base station. The proposed Solution #4.4 (#2 UE verifies gNB with 'System Query' message) requires the UE to communicate with the network despite of being in RRC_IDLE mode, Solution #4.4 (#1 Fake gNB detection using UL traffic monitoring) does not prevent UEs from camping onto false base station, Solution #4.8 is not addressing IDLE mode cell-reselection (but UE power-on scenario), and Solution #4.2, despite of the complexity introduced by its key management, it still does not protect the UEs in all scenarios (it is yet to be confirmed whether "other SIs" are always mandatory for cell reselection or not). Therefore, in their current state, no particular prevention type solution can be singled out or chosen as basis for normatic work in Phase I. However, 5G system will support a prevention type solution in Phase I, if the solution can be proven to be effective (in prevention) and efficient (in complexity). The Solution will also have to consider the work done in other working groups.
- Detection type solution seems to compliment, not compete with, mitigation type solution. From the network's point of view, it is always advantageous to be able to detect if there was any false base station attack, regardless of whether the UEs mitigated the attack or not. When the attacker is able to keep moving the false base station (i.e., not stationary for long time), it is challenging to actually catch the attacker, because by the time the false base station is detected and authorities reach the attack location, the attacker might have moved from there. However, detection is still valuable because first, it puts more work on attacker, and second, the attack itself will be less effective or mitigated if the attacker has to move away while the victim is in same location (i.e. not

Lenovo Ex. 1007
Page 319

moving). There is a proposed solution of detection type, i.e., #4.10. It does not have any major impact on the system and enables the network to collect measurements relevant to false base station. Since the actual detection is left for implementations, there is room for network implementations to adapt to the evolution of the attack. However as like MDT, regulator issues in collecting data from the UE by the network and usefulness of data in determination of fake eNBs need to be addressed.

5.4.5.2 Dual Connectivity architecture options 3/3a/3x (Non-Standalone NR with LTE anchor, EPC connected)

For the Dual Connectivity architecture options 3/3a/3x (Non-Standalone NR with LTE anchor, EPC connected) or EN-DC, the following is concluded for DRB termination:

- Option 3 does not have any security impact on NR/gNB.
- Option 3a can be supported without any security impacts to DC security procedures defined for LTE or with relatively minor enhancements to it.
- For Option 3a, Variant 1 of solution 2 in Solution #4.12 is preferred.

Editor's Note: Whether the impacts to eNB and MME of Variant 2 for option 3a are acceptable needs to be checked with RAN2 and CT1. If it is acceptable, then the above conclusion of preference for Variant 1 can be revisted.

- Option 3x can reuse the security procedures defined for Option 3a.

For the Dual Connectivity architecture options 3/3a/3x (Non-Standalone NR with LTE anchor, EPC connected) or EN-DC, the following is concluded for SRB termination:

- MCG SRB and MCG split SRB options do not have any security impact on NR/gNB and the LTE PDCP ciphering and integrity protection for RRC messages can be used as is with EN-DC.
- For SCG SRB (at SgNB) option, NR RRC ciphering and integrity protection keys are derived by the SgNB using S-KeNB that is provided by the MeNB. The SgNB uses its own key derivation function to derive the ciphering and integrity protection keys.

Editor's Note: It should be further studied whether adding an RRC control function to the SeNB and deriving its protection keys from the S-KeNB introduces new threats. If so, these threats need to be dealt with.

5.5 Security area #5: Security within NG-UE

5.5.1 Introduction

This clause deals with the security of sensitive data handled within the User Equipment.

5.5.2 Security assumptions

Editor's Note: This clause will document security assumptions related to each security area.

5.5.3 Key issues

5.5.3.1 Key issue #5.1: Secure storage and processing of credentials and identities

5.5.3.1.1 Key issue details

The Next Generation System requires the storage of credentials and identities (human and machine) in the User Equipment.

Lenovo Ex. 1007
Page 320

Subscription (human and machine) credentials and identities allow the network operator to authenticate its subscribers. Subscription authentication is needed to identify the origin and destination of the communication, to guarantee the Quality of Service and fulfill contractual, legal and regulatory obligations.

5.5.3.1.2 Security threats

An attacker may perform software and/or hardware attacks on the UE in order to extract the subscription credentials and identities that the attacker could then (re)use to clone the subscription.

The extraction of subscription credentials and identities would have the following threats for the subscriber, e.g.:

- The attacker could intercept the communications of the subscriber.
- The attacker could use the cloned subscription credentials and identities with his/her Mobile Equipment to impersonate the subscription. For example, the subscription would be billed for communications he/it is not the originator of.

The extraction of subscription credentials and identities would have the following threats for the network operator, e.g.:

- The operator could lose income because:
  - The attacker could use the cloned subscription credentials and identities with Mobile Equipment and impersonate the subscription and thereby using another subscribers subscription for his/her own good.
  - The attacker could use the cloned subscription credentials and identities with both his/her original Mobile Equipment and in other Mobile Equipment for which the attacker does not pay, e.g. in cases, (where a subscription is intended for use in one single Mobile Equipment at any given time).
  - The attacker could distribute the cloned subscription credentials and identities to other users such that an unlimited data plan could be shared between several users across many User Equipment.

Editor's Note: Subscriber versus user is for further study.

- The operator could no longer guarantee the origin and destinations of communications. This could have impacts on the billing, on the quality of service of the network, on the subscriber confidence in the network operator (brand reputation).
- The attacker could retrieve a secret allowing the remote administration of the subscription parameters which could eventually, in turn, lead to a denial of service attack.
- The network operator could no longer fulfill contractual, legal and regulatory obligations.

5.5.3.1.3 Potential security requirements

Within the 3GPP Next Generation System:

- The subscription credential(s) shall be integrity protected within the NG-UE using a tamper resistant secure hardware component.
- The long-term key(s) of the subscription credential(s) (e.g., K in EPS AKA) shall be confidentiality protected within the NG-UE using a tamper resistant secure hardware component.
- The long-term key(s) of the subscription credential(s) shall never be available in the clear outside of the tamper resistant secure hardware component.
- The authentication algorithm(s) that make use of the subscription credentials shall always be executed within the tamper resistant secure hardware component.
-
- It shall be possible to perform a security evaluation / assessment according to the respective security requirements of the tamper resistant secure hardware component.

Editor's Note: It is FFS whether such a security assurance scheme to be used for evaluation of the credentials and identifier storage and processing is within the scope of 3GPP and if so, the requirements related to it.

Lenovo Ex. 1007
Page 321

5.5.3.2 Key issue #5.2: Secure storage and processing of equipment identifier and credentials

5.5.3.2.1 Key issue details

The Next Generation System requires the secure storage of equipment identifier and credentials within the NG- UE. The equipment identifiers and credentials allow the network operator to authenticate the reported equipment identifier. This equipment identifier authentication is needed in order to verify that the equipment identifier reported by the device to the network is authentic.

5.5.3.2.2 Security threats

If an attacker is able to modify the equipment identifier, then the attacker may use the device to report a false equipment identifier to the network, thus leading to unnecessary signalling with the network (e.g., report a false equipment identifier that leads to failure of the equipment identifier authentication) or report a false equipment identifier to the network when the authentication of the reported equipment identifier is not performed.

5.5.3.2.3 Potential security requirements

Within 3GPP Next Generation System:

- the equipment identifier and credentials shall be integrity protected within the NG-UE.

5.5.3.3 Key issue #5.3: NG UE supporting different use cases

5.5.3.3.1 Key issue details

The Next Generation System requires NG UEs to support different/variety of vertical use cases.

5.5.3.3.2 Security threats

A NG UE not supporting full set of user plane encryption algorithms that is allowed to access NG service the NG UE is not designed to support could pose as a security risk to user plane traffic by potentially forcing the network to use less security (e.g. lighter and therefore potentially weaker algorithm, lighter and potentially weaker protocols, etc.).

5.5.3.3.3 Potential security requirements

Editor's Note: Security requirements need to align with SA1 requirements.

5.5.3.y Key issue #5.y: <key issue name>

5.5.3.y.1 Key issue details

5.5.3.y.2 Security threats

5.5.3.y.3 Potential security requirements

5.5.4 Solutions

5.5.4.1 Solution #5.1: Solution for Key Issue 5.1

5.5.4.1.1 Introduction

This solution addresses Key Issue 5.1

Lenovo Ex. 1007
Page 322

5.5.4.1.2 Solution details

The subscription credentials together with the USIM application (or its equivalent(s) in 5G) and the network access algorithm used to access the 5G network through a 3GPP or non-3GPP accesses shall always be stored and processed in a tamper resistant secure hardware solution defined by ETSI SCP.

5.5.4.1.3 Evaluation

This solution covers the threats and the requirements in Key Issue 5.1

Editor's note: The above statement needs more detailed explanation.

5.5.4.z Solution #5.z: <solution name>

5.5.4.z.1 Introduction

Editor's note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the security area.

5.5.4.z.2 Solution details

5.5.4.z.3 Evaluation

5.5.5 Conclusions

Editor's note: This clause will contain the evaluation between the solutions, and the conclusions made by SA3.

5.6 Security area #6: Authorization

5.6.1 Introduction

This security area covers both, authorization of the UE to access the network and authorization of the network to serve the UE.

5.6.2 Security assumptions

Editor's Note: This clause will document security assumptions related to each security area.

5.6.3 Key issues

5.6.3.1 Key issue #6.1: UE authorization

Editor's note: This key issue may have to be significantly revised depending on the reply to S3-160821 from SA1.

5.6.3.1.1 Key issue details

Traditionally, UE authorization has been achieved through the use of subscriber profiles. This concept is expected to continue for operator-controlled authentication and authorization procedures.

However, TR 22.862 contains the following requirements (cf. also key issue AA.3):

"The 3GPP system shall support industrial factory deployment where network access security is provided and managed by the factory owner with its ID management, authentication, confidentiality and integrity." and

"The 3GPP system shall support an authentication process that can handle alternative authentication methods with different types of credentials to allow for different deployment scenarios such as industrial factory automation".

Lenovo Ex. 1007
Page 323

Although authorization is not explicitly mentioned in these requirements, it may need further study whether subscriber profiles are still feasible for providing UE authorization to the NextGen serving network.

When 3rd party AAA servers are used to authenticate the user, there may be a need to propagate authorization information through a secure connection between the 3rd party AAA server and NextGen core network. This mechanism needs further study.

5.6.3.1.2 Security threats

- Unauthorized access by UEs to NextGen networks and services.

5.6.3.1.3 Potential security requirements

5.6.3.2 Key issue #6.2: Network authorization

5.6.3.2.1 Key issue details

Background on the situation in LTE:

EPS AKA, which is used in LTE access to the EPC, provides serving network authentication, i.e. the UE can securely identify the PLMN ID of the network that serves the UE. The UE can then compare the received PLMN ID with lists of preferred PLMNs and forbidden PLMNs stored in the UE. This can be used as a means to authorize the network. Furthermore, the UE can display the network name to the user, and the user can decide whether they want to connect to the network. In this way, the user could e.g. detect an unfamiliar operator name in a familiar area. This sort of network authorization by preference lists or user decision may become more important in NextGen than today if the number of serving networks a UE can connect to will multiply.

EAP-AKA', which is used in non-3GPP access to the EPC, provides access network authentication, i.e. the UE can securely identify the Access Network Identity (ANID) of the network that serves the UE. The ANID has a rich structure and is composed of a prefix and none, one, or more additional character strings up to a maximum length of 253 octets. However, this rich structure of the ANID is currently hardly used at all: The ANID is used only to identify the type of the access network, i.e. its value is one of the four constants 'HRPD', 'WIMAX', 'WLAN', 'ETHERNET'. Furthermore, no lists of preferred and forbidden access networks are defined for the UE in non-3GPP access to the EPC.

The present key issue is about further studying the possibility to allow more fine-grained network authorization decisions by the UE or by the user than available in LTE. Informing the UE or user that the home network authorized an access network of a particular type to serve the user may just not be good enough in the future if the number of serving networks a UE can connect to will multiply.

5.6.3.2.2 Security threats

- Unauthorized networks serving the UE that may eavesdrop on the UE or impersonate the UE or overcharge the UE.

5.6.3.2.3 Potential security requirements

Both the HPLMN and the NG UE should be able to authenticate a SN so that authorisation information can be validated by the NG UE.

The NG UE and/or the user should be able to decide if an available SN should be used or not. This is a measure where the NG UE and/or the user authorize the SN to serve the NG UE.

There should be the possibility for the HPLMN to predefine allowed and disallowed SNs in the NG UE.

Editor's Note: It is FFS to what extent the user and/or the NG UE should be involved in more fine-grained network authorization decisions.

Editor's Note: It is FFS how non-3GPP access technologies should be tackled in terms of authentication and authorisation of these networks by the NG UE/user.

Lenovo Ex. 1007
Page 324

5.6.3.3 Key issue #6.3: Authorization decoupled from authentication

5.6.3.3.1 Key issue details

Present 3GPP systems including EPS do not have high service granularity expected from NextGen networks.

The diversity of services in NextGen networks, provisioned by various stakeholders, warrants separate authorization for a particular service, group of services, or a Network Slice based on service requirements, i.e., dynamic authorization. Given the diversity of services in NextGen networks, it is not feasible to provide static authorization for all services upon initial authentication.

Services in NextGen networks may be dynamically provisioned and may be provided by more than one stakeholder/service provider. Such services will require dynamic authorizations and may need to avoid redundant authentications (i.e., in cases when the identity is authenticated, trustworthy, and sufficient for authorization). Authorization may directly follow an authentication or may be invoked later when a new service is requested, with or without a preceding authentication.

TR 23.799 describes solution warranting authorization based on 3rd party application service provider (and, therefore requiring such authorization to be de-coupled from authentication) in Sections 6.1.2 and 6.1.2.2.3.4. In addition, Section 6.4 of TR 23.799 describes authentication (e.g., NAS authentication) happening prior to and independent from the authorization for UE request for connectivity to a specific Data Network.

5.6.3.3.2 Security threats

Authorization tightly coupled with authentication may cause unnecessary (re-)authentications and thus lead to waste of security resources and potentially result in decreased availability of the system.

Editor's Note: It is for further study to identify and/or verify SA2 use cases for such decoupling in TR 23.799.

Editor's Note: It is for further study whether such authorization decoupled from authentication transpires on Service or Network Layer.

5.6.3.3.3 Potential security requirements

- It shall be possible to provide dynamic authorization, decoupled from authentication and triggered by service logic and/or operator policies.
- It shall be possible for a network to verify the dynamic authorization.
- It shall be possible for a network to establish audit trails of authorized accesses granted to authenticated identities.

5.6.3.y Key issue #6.y: <key issue name>

5.6.3.y.1 Key issue details

5.6.3.y.2 Security threats

5.6.3.y.3 Potential security requirements

5.6.4 Solutions

5.6.4.1 Solution #6.1: Network authorization by UE

5.6.4.1.1 Introduction

This is a solution for key issue #6.2: Network Authorization. It also includes cross-references to Security Areas #10 "Network domain security" and #11 "Security visibility and configurability".

5.6.4.1.2 Solution details

A UE may proceed as follows to authorize a network:

The UE extracts the identity of the network serving the UE, e.g. SN-id = Serving Network Identity (in case EPS AKA is used) or ANID = access network identity (in case EAP-AKA' is used) from a received authentication message. If a list of authorized serving/access network identities is available in the UE then the UE checks whether the received serving/access network identity is contained in this list. If so the UE proceeds. If a list of forbidden serving/access network identities is available in the UE then the UE checks whether the received serving/access network identity is contained in this list. If so the UE aborts the procedure by sending a reject message. If an identity was broadcast in a user-friendly (human-readable) form over the radio then the UE compares this broadcast identity with the received serving/access network identity. If they do not match then the UE aborts the procedure by sending a reject message. In all other cases, the UE displays the received serving/access network identity to the user. The user can then identify serving network identities that do not belong in the geographical area he is located in. In addition, the UE may block certain services, depending on risk model.

NOTE: The authentication of the serving/access network identity in EPS AKA or EAP-AKA' by the UE is no end in itself, but is used as a basis for a decision either by the UE (based on lists) or by the human user whether to proceed with connecting to this network. Merely comparing the serving/access network identity received with a broadcast identity (cf. next paragraph) is not enough as both may match, but may point to a network name not acceptable to the user. Therefore, unless there are lists of trusted or forbidden access networks in the UE, the serving/access network name needs to be displayed to the user for making a decision.

There are variants of this: Security area#10 on Network Domain Security contains a solution that proposes the use of Circles of Trust. The list of authorized serving network identities available in the UE could reflect membership of the network in one of these Circles of Trust. Due to the guarantees provided by the Circles of Trust, the UE can be assured that the received serving network identity has not been spoofed by means of impersonation in the Interconnection network. For the steps above, where something is displayed to the user, or where lists can be configured in the UE, there is an obvious dependency on Security area#11 on" Security visibility and configurability".

5.6.4.1.3 Evaluation

5.6.4.2 Solution #6.2: Dynamic Authorization by Operator/MNO

5.6.4.2.1 Introduction

Services in NextGen networks may be provided dynamically and possibly by more than one stakeholder/service provider. Such services will require dynamic authorizations. Authorization may directly follow an authentication or may be invoked later when a new service is requested, with or without a preceding authentication.

This solution addresses Key Issues 6.1: UE authorization and #6.3: Authorization decoupled from Authentication in cases where the Authorization is being handled by the Operator/MNO.

5.6.4.2.2 Solution details

The proposed architecture is illustrated in Figure 5.6.4.2.2-1.

Lenovo Ex. 1007
Page 326

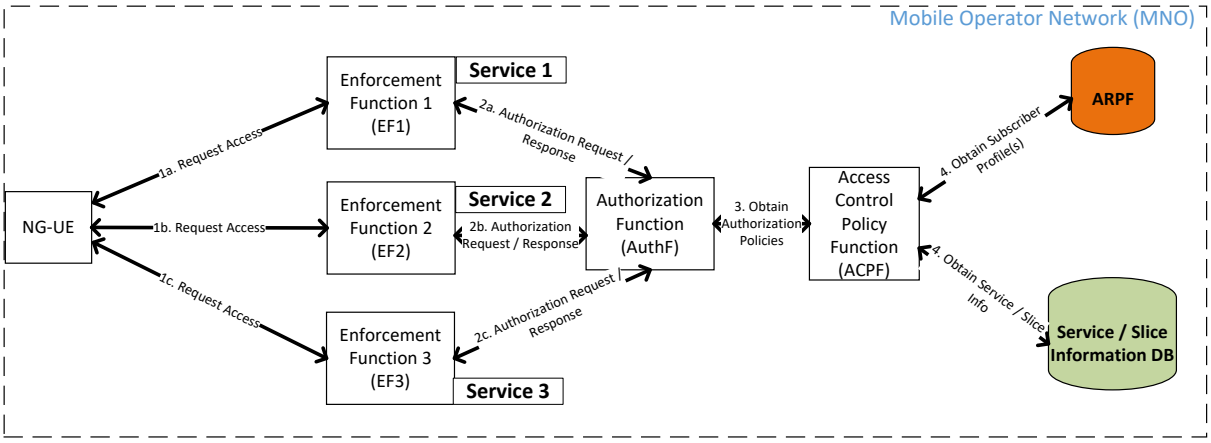


Figure 5.6.4.2.2-1. Dynamic Authorization by Operator/MNO

The architectural components are described as follows:

- Access Control Policy Function (ACPF): The ACPF is responsible for generating the policies required for performing subscriber / user authorizations to slices / services. The policies are updated on a regular basis based on operator policies and uploaded to Authorization Function(s).
- Authorization Function (AuthF): This function performs the authorization based upon a request from a subscriber and then makes a decision using the access control policies provisioned by the ACPF. The AuthF is located within an Operator / MNO domain.
- Service / Slice Information DB (SIDB): The SIDB contains details about the services / slices such as (e.g. slice-id, expected security level of a slice)
- Authentication Repository and Processing Function (ARPF): This is a store for subscriber / NG-UE profile and security related information.
- Enforcement Function (EF): These functions perform enforcements for policies relating to access control to services / slices based upon "Proof-of-Authorization".

Editor's Note: It is FFS how the architecture components described above can be mapped into approved SA2 components.

Details of the flow of messages for Figure 5.6.4.2.2-1 are provided below:

1. The NG-UE requests access to a service. The EF checks to see if the NG-UE has been authorized to access the service.
2. If the EF does not have authorization information about a NG-UE's, the EF then requests the AuthF to perform an authorization so that the NG-UE would be able to access a service. A corresponding response is generated by the AuthF after completion of steps 3 and 4. The response is generated based upon one or more authorization checks.
3. The AuthF obtains authorization policies from an ACPF, based upon which the AuthF performs authorization.
4. The ACPF obtains subscriber profile information from an ARPF / HSS and also obtains slice / service specific information from a SIDB and then generates detailed authorization rules. An example authorization rule would indicate that an equipment authentication may have to be carried out in order to be granted access to a service / slice. The ACPF is provided with general operator policies, relevant subscriber information, information on services / slices offered to subscribers. The general operator policies would determine the type of slices that would be accessible, type of authorization mechanisms (e.g. PoA). Relevant subscriber information such as IMSI, subscription information, preferences, default services may be either pre-provisioned or on a request basis. In addition, detailed slice / services information is provided to the ACPF.

   Editor's Note: Alignment of the Authorization message flow in Figure 5.6.4.x.2-1 and message flows for Attach Request and Service Request is FFS.

5.6.4.2.3 Evaluation

FFS

Lenovo Ex. 1007
Page 327

5.6.4.3 Solution #6.3: Dynamic Authorization by Trusted 3-rd Party

5.6.4.3.1 Introduction

Services in NextGen networks may be provided dynamically and possibly by more than one stakeholder/service provider. SA2 TR 23.799 describes requirements for authorization to be performed by a trusted third party in Sections 6.1.2 and 6.1.2.2.3.4.

Such services will require dynamic authorizations. Authorization may directly follow an authentication or may be invoked later when a new service is requested, with or without a preceding authentication.

This solution addresses Key Issues 6.1: UE authorization and #6.y: Authorization decoupled from Authentication in cases with industrial factory deployment and where the Authorization is being handled by a Trusted 3rd-party, e.g., the industrial factory.

5.6.4.3.2 Solution details

The proposed architecture is illustrated in Figure 5.6.4.3.2-1.

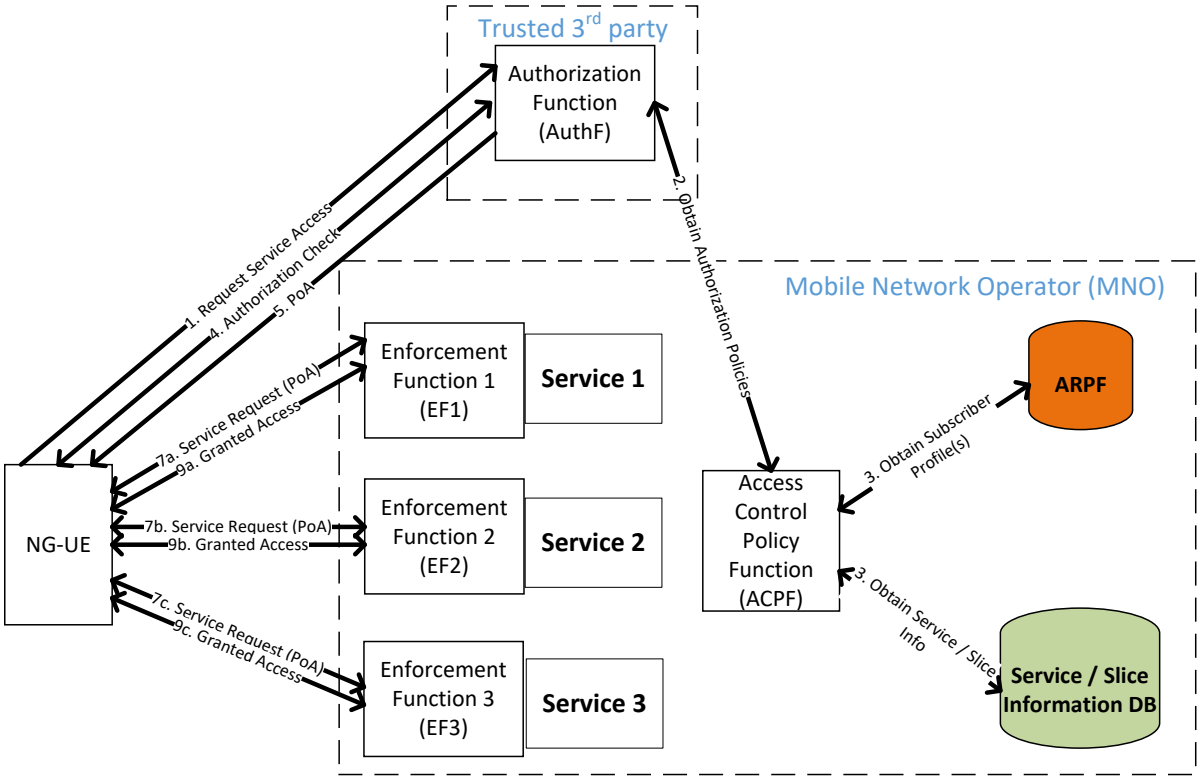


Figure 5.6.4.3.2-1. Dynamic Authorization by Trusted Third-party

The architectural components are described as follows:

- Access Control Policy Function (ACPF): The ACPF is responsible for generating the policies required for performing subscriber / user authorizations to slices / services. The policies are updated on a regular basis based on operator policies and uploaded to Authorization Function(s).
- Authorization Function (AuthF): This function performs the authorization based upon a request from a subscriber and then makes a decision using the access control policies provisioned by the ACPF. The AuthF issues a "Proof-of-Authorization" to a subscriber based upon possible additional authorization checks (e.g., equipment authentication). The AuthF is located within a trusted third party domain.
- Service / Slice Information DB (SIDB): The SIDB contains details about the services / slices such as (e.g. slice-id, expected security level of a slice)
- Authentication Repository and Processing Function (ARPF): This is a store for subscriber / NG-UE profile and security related information.

Lenovo Ex. 1007
Page 328

- Enforcement Function (EF): These functions perform enforcements for policies relating to access control to services / slices based upon "Proof-of-Authorization".
- Proof-of-Authorization (PoA): This is a proof by which an NG-UE can gain access to a service / slice. A PoA may be issued by an AuthF. The PoA may be in the form of signed messages or by means of tokens (e.g. OAuth token).

Editor's Note: It is FFS how the architecture components described above can be mapped into approved SA2 components.

Description of the functional components:

- Policy Information Point (PIP): The PIP contains information about the various attributes that may be used for determining authorization. Examples of the attributes may include: subscriber profile information, slice / service information, device information etc. Examples of PIP, may include: ARPF, HSS
- Policy Retrieval Point (PRP): The PRP is used as an entity that hosts general operator policies, slice / service policies, subscriber and device policies, general security policies (e.g. authorization / authentication) etc. An example of a PRP is a Policy and Charging Rules Function (e.g. NG-PCRF). In addition to a traditional PRP, the PRF can aggregate the various policies for slice / service access in order to create a policy rule which may then be used by a PDP.
- Policy Decision Point (PDP): The PDP makes a decision based upon a NG-UE's request and taking into considerations the different policy rules that may have been generated by the PRP. In the above scenario, the PDP function is performed by an AuthF. An example of an AuthF is a Prose Function. The PDP / AF generates a PoA based upon the authorization checks. The PDP is located within the domain of a Trusted Third party network.
- Policy Enforcement Point (PEP): This is a function that enforces policies. The PEP is the function that provides access to a service based upon verification of a PoA. This functional entity may reside at e.g., the eNB or the MME.

A high-level message flow diagram is illustrated in Figure 5.6.4.3.2-2.

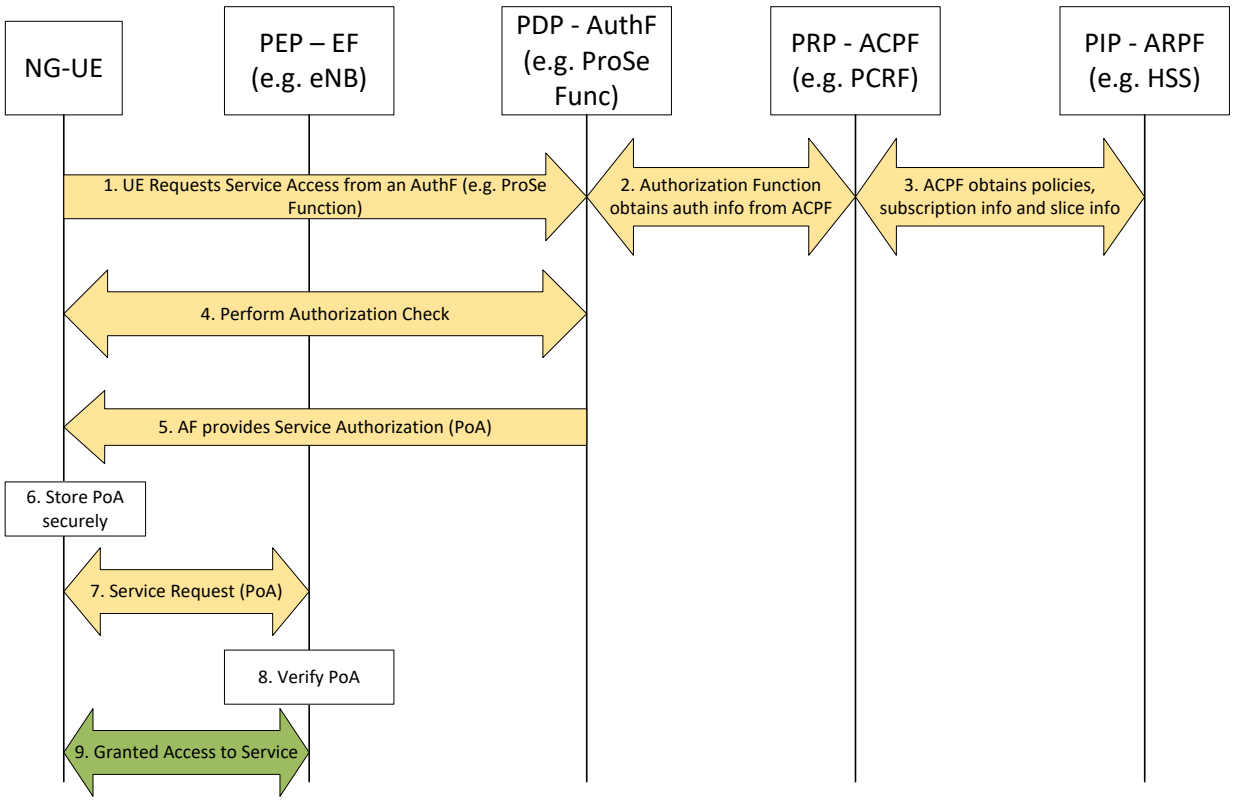


Figure 5.6.4.3.2-2. Message flow diagram

Description of the steps for Figure 5.6.4.3.2-2:

Lenovo Ex. 1007
Page 329

1. The NG-UE requests authorization for access to a service (e.g. Prose Direct Discovery or Direct Communication or both) from AuthF.
2. The PDP creates a specific request to the PRP (PCRF) based upon the request from NG-UE.
3. The PRP obtains policies, subscriber information, equipment information, slice / service information, etc. from PIP which may involve various data sources (e.g. ARPF / HSS). The PRP aggregates the various policies and generates authorization rules.
4. Based upon the rules that have been obtained by the AuthF, the AuthF may perform one or more additional authorization checks. Examples of such authorization checks may involve, an equipment authentication
5. Based on the results of the authorization checks, the AuthF provides a PoA to the UE. The PoA may be in the form of one or more Access Token(s). It is assumed that the PoA is provided to the UE using a secure communications channel.
6. The NG-UE securely stores the PoA, depending upon the type and validity of the PoA. In the case, of the access token, its scope and usage may be described in similar terms as the OAuth token.
7. The NG-UE presents the PoA to the PEP / EF (e.g. eNB, MME). It is assumed that the UE presents the PoA to the EF using a secure communications channel.
8. The EF verifies the PoA and determines the type of service access that has to be provided to the NG-UE. It is assumed that EF and AuthF share a trust relationship.
9. After the EF verifies the PoA the NG-UE is granted access to the service.

Editor's Note: Alignment of the Authorization message flow in Figure 5.6.4.3.2-2 and message flows for Attach Request and Service Request is FFS

5.6.4.3.3 Evaluation

FFS

5.6.4.4 Solution #6.4: EAP-based solution for secondary authentication and authorization

5.6.4.4.1 Introduction

This solution addresses KI #2.10 and KI #6.1.

5.6.4.4.2 Solution details

It is assumed that there will be a User Plane Function (UPF) in the Next Generation Systems playing a similar role as the PDN-GW in LTE. It is proposed to delay the secondary (PCO-based) authentication until IP connectivity established between the UE and the UPF. It is then proposed to use EAP for authentication between the UE and the potentially external AAA server where the UPF endorses the role of the EAP authenticator. This AAA and related credentials have nothing to do with the NextGen SDM/SEAF/AUSF/ARPF functions and credentials used for access/primary authentication. EAP is widely used and provide support for many authentication methods such as EAP-TLS, EAP-AKA, EAP-TTLS and EAP-PEAP. EAP payloads would be carried by the PANA protocol (rfc5191) which is IP-based.

Figure 5.6.4.4.2.3-1 shows a possible flow where this UP-based secondary authentication is run with an external AAA server. The requirements on this UPF entity include the support of PANA and EAP possibly in addition to the support of all the relevant features of PDN-GW such as the support of the SGi interface. In general, we will prefix LTE concepts with NG- whenever, it is meant the corresponding concept in Next Generation Systems.

The description of the different steps is given below.

Lenovo Ex. 1007
Page 330

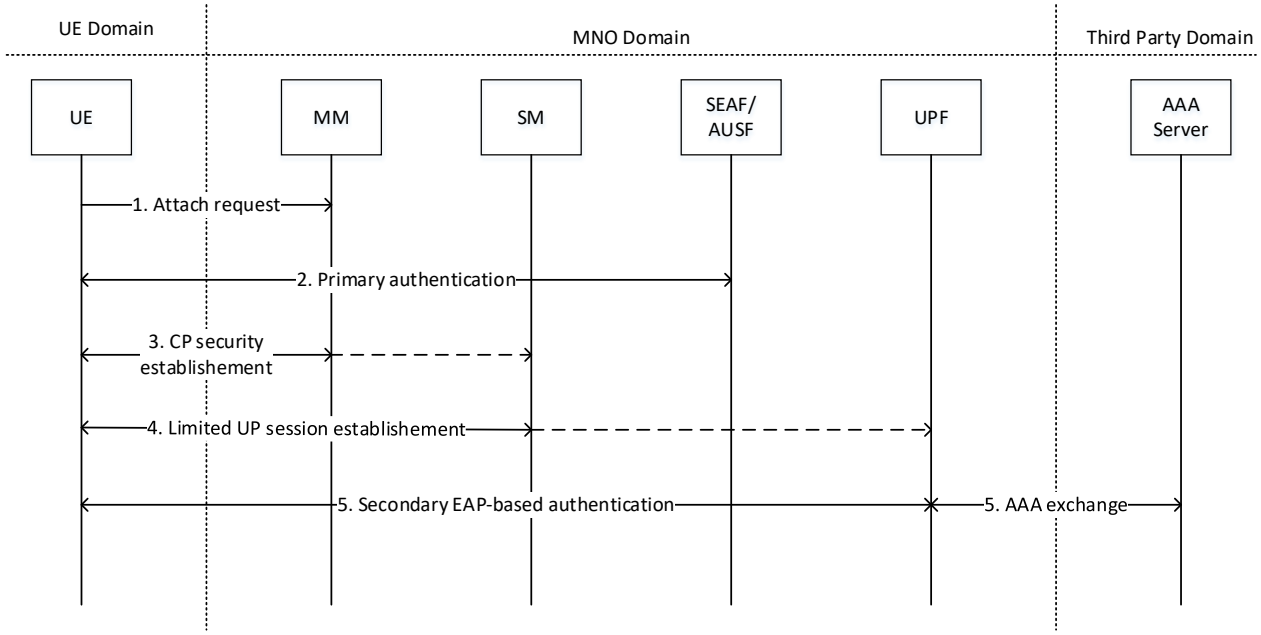


Figure 5.6.4.z.2.3-1: EAP-based secondary authentication

1. The NG-UE sends an attach request initiating the attach procedure.

2. The NG-UE runs the primary authentication with the AUSF through the SEAF The secondary authentication does not depend neither on how the SEAF and MM are deployed (collocated or split) nor on the location of the SEAF (home or visited PLMN).

3. Control plane security is established between the NG-UE and the end point of the NG NAS

4. A limited UP session is then established for the transport of user plane data between the NG-UE and the UPF. This is the only decisive step on which the secondary authentication depends assuming that this when IP connectivity is established between the NG-UE and the UPF.

5. The secondary EAP-based authentication is run between the NG-UE and an AAA server, within the Data Network being accesses, acting as an EAP server via the UPF acting as an EAP authenticator. The NG-UE is then granted access based on the outcome of this authentication procedure. It is possible that the UPF endorses also the role of the EAP server.

Conceptually, steps 1 to 3 are not necessarily needed. The only requirement for step 5 is that an IP connectivity is established between the NG-UE and the NG-PDN-GW which is hypothetically achieved in step 4. The secondary authentication is optional and the decision of whether execute it or not could be based on subscription information retrieved during the previous steps or on an operator policy. In case RAN security is established before step 5, then the EAP exchange would be protected on the air interface.

Figure 5.6.4.4.2.3-2 shows the protocol architecture for the EAP-based secondary authentication between the NG-PDN-GW and the NG-UE. The architecture draws similarity with how it is in LTE for the transport of the UP traffic between the UE and the PDN-GW. The greyed boxes highlight the new protocols.

Editor's note: The solution might need to be revised depending on the progress of SA2.

Editor's note: The use of non-IP to carry EAP is ffs.

Lenovo Ex. 1007
Page 331

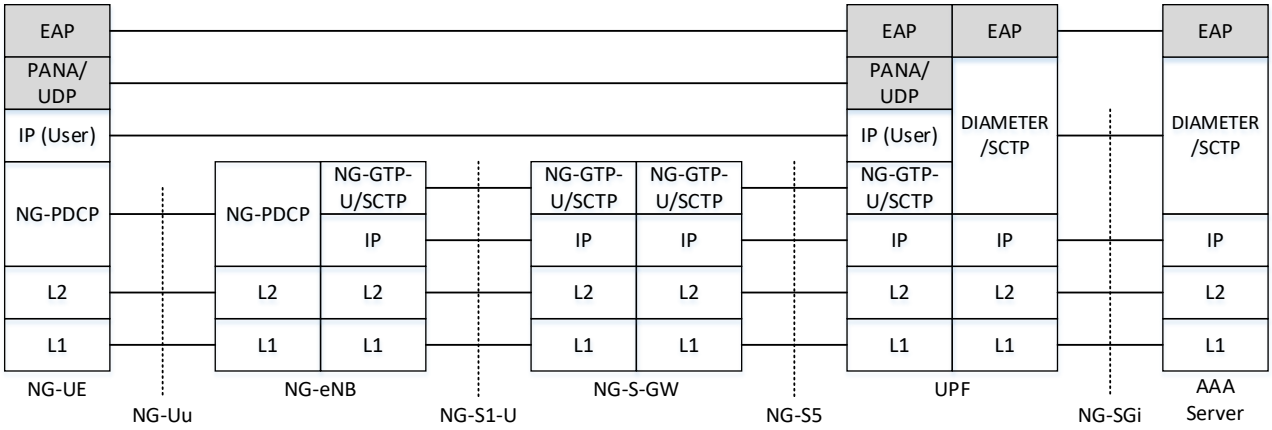


Figure 5.6.4.4.2.3-2: Protocol architecture for EAP-based secondary authentication

5.6.4.4.3 Evaluation

- TBD

5.6.4.z Solution #6.z: <solution name>

5.6.4.z.1 Introduction

Editor's note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the security area.

5.6.4.z.2 Solution details

5.6.4.z.3 Evaluation

5.6.5 Conclusions

Editor's note: This clause will contain the evaluation between the solutions, and the conclusions made by SA3.

5.7 Security area #7: Subscription privacy

5.7.1 Introduction

The subscription privacy is very important area for Next Generation system as can be seen by the growing attention towards it, both inside and outside the 3GPP world.

Outside the 3GPP, an alliance of mobile network operators, vendors, and universities called NGMN [9] has identified security and privacy as an enabler and essential value proposition of NextGen system and has presented that built-in privacy should be included as a design principle [10]. Similarly, a 5G PPP project called 5G-Ensure [11] has also identified privacy as one of the topmost priorities for the NextGen system stating that the privacy has an important social impact [12].

In the 3GPP, privacy is a topic that is addressed in several specifications. For example, the TR 33.849 [5] is a study on subscription privacy impacts in 3GPP that presents privacy key issues and risk mitigation approaches. The study identifies that the privacy needs to be addressed as a separate topic in its own. The TR 22.864 [6] also identifies subscription privacy as very important. It is mentioned that the privacy of personally identifiable information needs to be protected, for example from a less trusted access or a rouge network element. The study contains several potential security requirements related to subscription privacy, e.g. protecting the user identifying information from active and passive attacks, protecting user location information from active and passive attacks, and not allowing UE location or application usage information to be related to an individual user identity. Similarly, the TR 22.891 [7] contains privacy requirements such as possibility for the UE to hide its long-term identifier by using temporary identifier even for initial

Lenovo Ex. 1007
Page 332

attach and protecting the subscription privacy during system information collection. The TS 22.185 [8] has also identified privacy requirements in V2X context that need to be further elaborated in the Next Generation system context as well, e.g. ensuring that a UE cannot be tracked or identified beyond a short time-period.

Subscription privacy itself is a wide area that spans many key issues e.g. identifiers, mobility pattern, location or presence information, data usage pattern, etc. Relevant key issues and solutions are discussed in clause 5.7.3.

5.7.2 Security assumptions

The subscription privacy can potentially be compromised in various ways such as attack on 3GPP protocol interfaces, malware infection on 3GPP nodes, and illegitimate use of resources by an insider (i.e. inside attack). Figure 5.7.2-1 (TR 33.849 [5]) shows various sub-processes (e.g. collect, transmit, use, share, etc.) during a communication process that may impact subscription privacy. All these sub-processes need to be considered while defining privacy related key-issues and potential solutions.

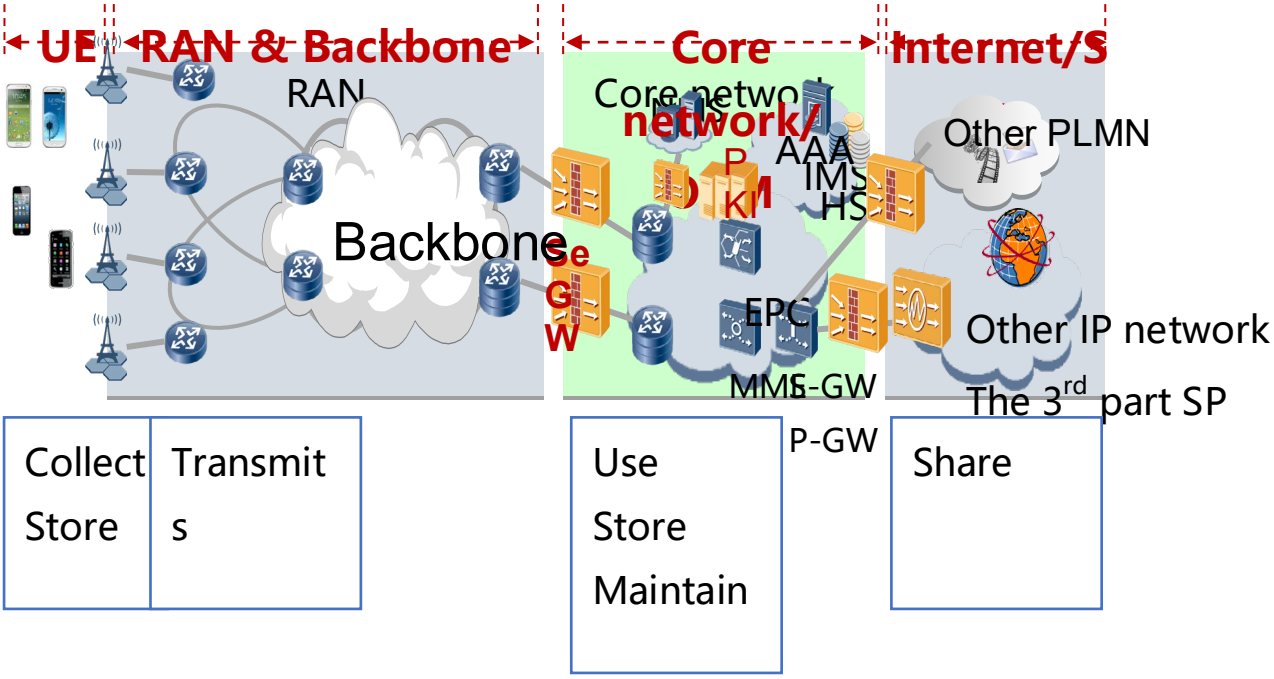


Figure 5.7.2-1: Conceptual view of privacy in 3GPP system

For the Next Generation system, along with the requirements on privacy, there are also requirements on minimizing signaling overhead (e.g. in the TR 22.864 [6]). Therefore, it is important for the solutions, which will be designed to fulfill the subscription privacy requirements, to be simple and to minimize signaling overhead.

5.7.3 Key issues

5.7.3.1 Key Issue #7.1: Refreshing of temporary subscription identifier

5.7.3.1.1 Key issue details

The GSM/GPRS, UMTS and LTE systems already use temporary subscription identifiers. For example, in a current LTE system, a Mobility Management Entity (MME) assigns an M-Temporary Mobile Subscriber Identity (M-TMSI) to a subscriber. The M-TMSI, which is local to a MME, and a MME Code (MMEC) form another identifier called an S-TMSI. The S-TMSI, which identifies a particular subscriber in a particular MME, is itself a part of an identifier called Globally Unique Temporary Identifier (GUTI). A GUTI uniquely and globally identifies a particular subscriber. The MME can allocate or reallocate a GUTI to a UE in the following messages:

- ATTACH ACCEPT: The MME either allocates the GUTI for the first time or optionally reallocates the GUTI depending upon if the UE sent an ATTACH REQUEST using an IMSI or an existing GUTI respectively.

Lenovo Ex. 1007
Page 333

- TRACKING AREA UPDATE ACCEPT: The MME optionally reallocates the GUTI.
- GUTI REALLOCATION COMMAND: The MME explicitly reallocates the GUTI.

Temporary subscriber identifiers are used as a privacy measure to mitigate subscription identification and tracking by eavesdroppers on the radio link, making it harder to track the location or activity of a particular subscriber. For example, in a current LTE system, a GUTI or an S-TMSI is visible in plain-text over the air in the following messages.

- RRC CONNECTION REQUEST: The S-TMSI may be used as an "InitialUE-Identity";
- RRC CONNECTION SETUP COMPLETE: The GUTI may be used as an "EPS mobile identity" in the tunnelled ATTACH ACCEPT message.
- Paging: The S-TMSI may be used as a "PagingUE-Identity".

In the past, acquiring or tracking the temporary subscription identifiers has been one of the most important attack strategies in compromising the subscription privacy. However, if the M-TMSI part of the GUTI or S-TMSI is randomly generated and is updated frequently, it is not feasible, or at least much more complex, for an eavesdropper to correlate the GUTI to any particular subscriber. The longer time a temporary identifier remains unchanged, the easier it is for an attacker to identify or track the corresponding subscriber, thereby compromising the privacy of the subscription.

Researchers in [64] presented the location leakage of a UE (in three PLMNs) because the observed PLMNs did not change the GUTI for the UE up to three days even when the UE was moving within a city, even though the LTE standards makes it possible to change the S-TMSI more frequently than that.

The major problem with a mechanism of GUTI allocation in a current LTE system is that it is up to the MME implementation and/or policy configuration when and if at all to reallocate the GUTI. It is also possible for the MME to keep (re)allocating the same old GUTI to the UE. The UE neither takes part in the generation of the GUTI nor verifies that new allocated GUTI is not the same as the old one. This opens up possibilities for either poor implementations or poor configuration that keeps the GUTI same for a long time.

Therefore, developing mechanisms to regularly refresh temporary subscription identifiers, that are used in a Next Generation system and that could compromise privacy, is one of the most important key issues towards achieving the subscription privacy.

5.7.3.1.2 Security threats

If the subscription identifiers are not appropriately protected, an inside or outside attack might lead to privacy incidents (and possibly privacy breaches) such as:

- unlawful exposure of subscription identifier;
- unauthorised detection of subscriber’s presence in certain location;
- unintentional tracking of subscriber’s movement; or
- unauthorised knowledge of subscriber’s activity patterns, etc.

Such incidents might ultimately have more serious consequences such as:

- damage to the victim’s reputation;
- compromise of the victim’s safety;
- damage to the operator’s reputation, or
- financial loss to both the victim and the operator.

Therefore, potential threats are

- The subscription identifier might be disclosed or made inferable to an unauthorized party.
- The subscriber’s location might be linked to its identifier by an unauthorized party.
- The subscriber’s communication or activity data might be linked to its identifier by an unauthorized party.

Lenovo Ex. 1007
Page 334

- The subscription identifiers across different services might be correlated by an unauthorized party.
- The subscription identifiers might be spoofed by an attacker.

5.7.3.1.3 Potential security requirements

- Temporary subscription identifiers shall be refreshed regularly with a frequency that avoids their persistent use.
- Common parameters should be specified that can be used to define the required refresh period.

Editor's Note: It is FFS to determine if it is feasible to regularly refresh RAN level temporary subscription identifiers.

5.7.3.2 Key issue #7.2: Concealing permanent or long-term subscription identifier

5.7.3.2.1 Key issue details

In a 3GPP system, permanent or long-term subscription identifiers are used during a communication process (e.g. in case of current LTE system: IMSI and MSISDN).

In the past, actively or passively acquiring such permanent subscription identifiers (especially the IMSI) has been one of the most important attack strategies in compromising the subscription privacy (especially the subscription location). Therefore, concealing permanent identifiers used in a Next Generation system, that are relevant to privacy, is one of the most important key issues towards achieving the subscription privacy.

In order to determine the scope of this key issue, it is important to first identify the network functions and interfaces where it is important and allowed to conceal the permanent identifier. Whether it is technically possible to conceal the permanent identifier is in the scope of solutions clause.

The following analysis is in reference to a current LTE system, based on a likely assumption that the Next Generation system will also have similar functions and interfaces, i.e. UE (device), eNB (serving RAN), MME (serving CN), and HSS (home CN). The Figure X illustrates various points where permanent identifiers (IMSI and MSISDN) are available in the current LTE system. The Figure X also shows a passive and an active IMSI catcher. The UE, the MME, and the HSS, all have the IMSI of a subscription. The eNB may have the IMSI, if the UE attaches using the IMSI. The passive IMSI catcher can eavesdrop on the Uu interface and collect the IMSI when the UE attaches using the IMSI. The active IMSI catcher, however, can ask the UE to provide its IMSI. The MME and the HSS have the MSISDN of the subscription. Note that the MSISDN might be available to the UE as well, e.g. optionally stored in USIM or requested via MSISDN notification procedure. However, the UE does not use the MSISDN for operational purposes.

Editor's Note: This analysis may be moved to the annex as LTE reference and replaced by Next Generation architecture analysis, once SA2 has settled on architecture.

Lenovo Ex. 1007
Page 335

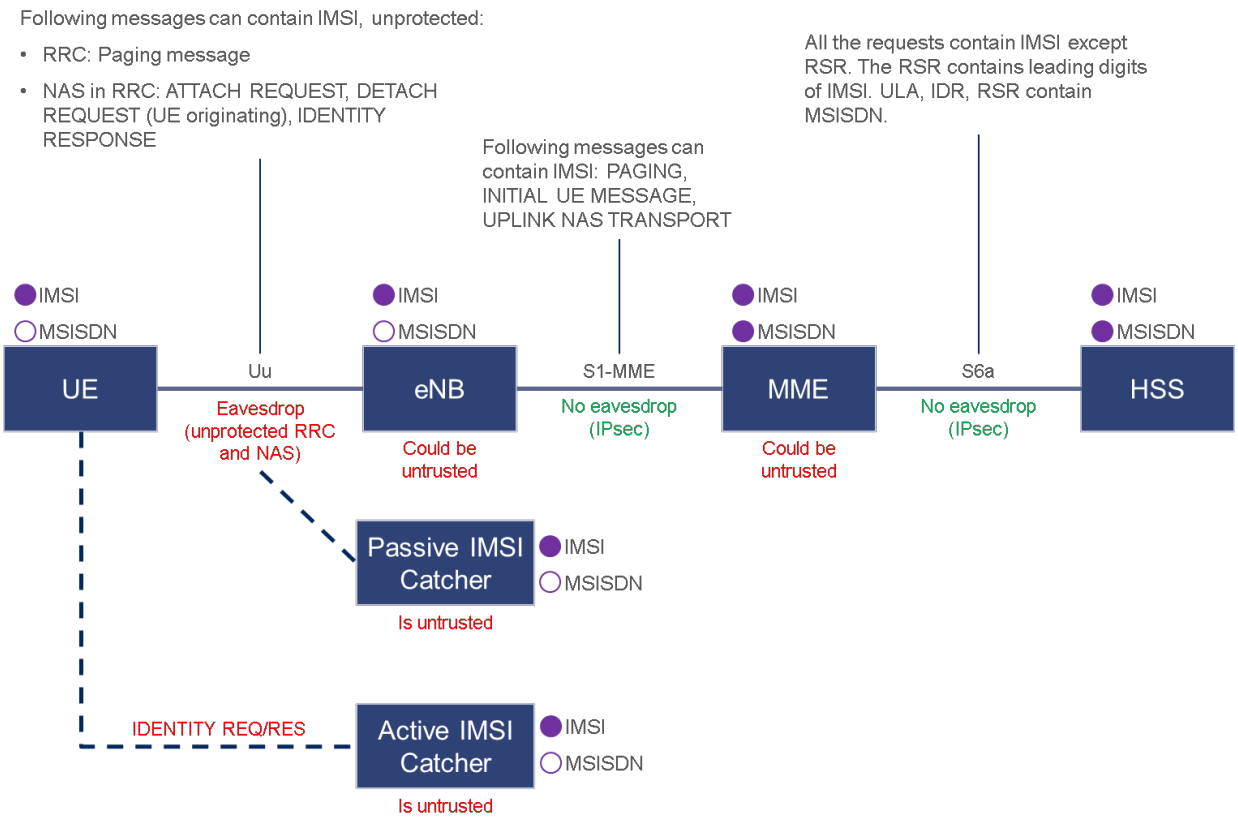


Figure 5.7.3.2.1-1: Various points where IMSI and MSISDN are exposed in a current LTE system

Interfaces and functions that do not need to be considered further in this key issue

The UE has the IMSI. Protecting the leakage of IMSI due to hardware or software vulnerability in the UE is out of scope of this key issue. Similarly, the HSS has both the IMSI and the MSISDN. Protecting the information leakage in the HSS is out of scope this key issue. The use of IPsec in S1-MME and S6a is not mandatory. However, when IPsec is adopted, the interfaces S1-MME and S6a are protected and are safe from eavesdrop. These interfaces can therefore be left out from further discussion.

NOTE: Storage of long-term identifier in the UE is covered in security area #5.

Interfaces and functions that are susceptible to IMSI exposure

The Uu interface is clearly susceptible to IMSI exposure due to passive and active attacks. If sending unprotected IMSI in the Uu interface can be avoided, then the existing IMSI catcher attacks will not be effective anymore.

The IMSI concealment can either terminate in the eNB or in the core (MME or HSS). In the latter case, the consequence is that the eNB will not know the IMSI either, which is fine because not knowing the IMSI does not hinder the functionality of the eNB. This is different than the use of S-TMSI. The eNB uses S-TMSI to choose which MME it should route the message to, but IMSI is not used for any such purpose. If the eNB does not get the IMSI, then internal attacks on the eNB also become ineffective in leaking the IMSI. There is also no LI requirement on the eNB for using IMSI to intercept the communication. Therefore, concealing IMSI at Uu and eNB is important and allowed.

For knowing the correct home network, the MME needs to know at least the MCC and MNC part of the IMSI. So, if MCC and MNC are indicated in some way, it is fine if MME does not know the full IMSI. This means the IMSI concealment terminates at HSS. Doing so would help relax the trust between the home network and the serving network. However, there are two concerns in doing so:

a) The first concern is that in the current LTE system, the MME knows or can know the MSISDN of the subscription from the HSS. So just concealing the IMSI does not solve the privacy issue. A solution for this could be to not give the MSISDN to the MME.

b) The second concern is about the LI requirements. Referring to the 3GPP TS 33.106 and 3GPP TS 33.107, following LI requirements do not allow IMSI concealment from the MME:

Lenovo Ex. 1007
Page 336

- a target shall be identifiable through its IMSI;
- a lawful intercept target can be a roaming user with a subscription belonging to another 3GPP network; and
- a visited network shall be able to support the interception of all services without home network assistance or visibility.

It means that concealing IMSI at MME, although important, is not allowed. Therefore, the scope of concealing the permanent identifier can be summarized as follows:

- left out of scope : at UE, S1-MME, S6a, and HSS (home CN);
- important and allowed : at Uu and eNB (serving RAN); and
- important but not allowed : at MME (serving CN).

The IMSI is used here just as a representation of an identifier that can be used for LI. For example, even if one permanent or long-term identifier (e.g. IMSI) is concealed from serving CN in the Next Generation system, it is likely that LI will require some other permanent or long-term identifier (e.g. MSISDN). The consequence is that concealing one identifier (e.g. IMSI) does not solve the privacy issue. If all the permanent or long-term identifiers are concealed from the serving CN and a mechanism is developed so that the home CN needs to be involved for identifying the LI targets, then the third LI requirement listed above will be violated.

Therefore, concealing the permanent or long-term identifiers from the serving CN, though important, would not be legal unless the LI requirements are revised or relaxed.

Fallback to earlier generations of 3GPP networks is another aspect that affects considerations about enhancements to concealing permanent or long-term subscriber identities. If a solution is introduced that makes the protection better in NextGen network than what we currently have for earlier generations of 3GPP networks, then it would be highly desirable that a circumvention of this solution by fallback to legacy 3GPP networks could be mitigated. As an example, let us consider an active attack with an "IMSI catcher". If NextGen UE is protected against IMSI catchers that pretend to be parts of genuine NextGen networks then the attacker could instead try whether the NextGen UE would reveal its IMSI to an IMSI catcher that pretends to be a genuine LTE eNodeB. This alternative attack would work against such NextGen UEs that also support LTE *unless* a suitable mitigation can be found.

5.7.3.2.2 Security and privacy threats

NOTE: Similar threats as in clause 5.7.3.2.2.

5.7.3.2.3 Potential security requirements

- The subscription identifier protection shall be at least as strong as provided by existing LTE system.
- Permanent subscription identifiers shall be concealed in communication, whenever feasible.

Editor's Note: It is FFS to determine if the permanent subscription identifiers could be concealed even during the first communication, e.g. initial ATTACH REQUEST.

- Temporary subscription identifiers shall be used instead of permanent subscription identifiers in communication, whenever feasible.

Editor's Note: It is FFS to determine if only the temporary subscription identifiers could be used in all communications.

5.7.3.3 Key issue #7.3: Concealing permanent or long-term equipment identifier

5.7.3.3.1 Key issue details

In a 3GPP system, permanent or long-term equipment identifiers are used during a communication process (e.g. in case of current LTE system: IMEI and MAC address).

Editor's Note: MAC address usage within this security area is FFS.

Lenovo Ex. 1007
Page 337

In a current LTE system, IMEI of the device is included in two types of NAS messages, i.e. IDENTITY REQUEST and SECURITY MODE COMPLETE. Both of these messages are protected when IMEI is transferred. However, during emergency bearer service request, when there is no valid subscription, a device includes its IMEI in an unprotected ATTACH REQUEST message.

The Next Generation system should also maintain the protection of permanent equipment identifier. It could also be studied if transferring permanent equipment identifier unprotected can be avoided completely, even for emergency services.

5.7.3.3.2 Security and privacy threats

NOTE: Similar threats as in clause 5.7.3.2.2.

5.7.3.3.3 Potential security requirements

- Permanent equipment identifiers shall be concealed in communication, whenever feasible.

Editor's Note: It is FFS to determine if permanent equipment identifiers could be concealed in all communication, e.g. also during an emergency bearer service request.

5.7.3.4 Key issue #7.4: Using effective temporary or short-term subscription identifiers

5.7.3.4.1 Key issue details

In a 3GPP system, many types of temporary or short-term subscription identifiers are used during a communication process (e.g. in case of current LTE system: GUTI, TMSI, C-RNTI, and IP address). The use of temporary identifiers, instead of permanent identifiers, makes it more difficult for an attacker to identify or track the subscriber, thereby enhancing subscription privacy.

However, if the temporary identifiers are poorly generated, it becomes easier for an attacker to identify the subscription. Let's take some unrealistically naive example, just for making the point clear. If a TMSI is generated by appending a counter to an IMSI, then an attacker can easily figure out the IMSI. If a TMSI or a CRNTI is generated using a sequential counter, an attacker can know how many subscribers are attached to a network or if any new subscriber entered an area.

Therefore, in order to preserve the subscription privacy, it is important in the Next Generation system to mitigate the chance of poor implementations for generating temporary subscription identifiers.

5.7.3.4.2 Security and privacy threats

NOTE: Similar threats as in clause 5.7.3.2.2.

5.7.3.4.3 Potential security requirements

- From one or more temporary identifiers, it shall not be feasible for an unauthorized party to identify the corresponding permanent identifier.
- From one or more temporary identifiers, it shall not be feasible for an unauthorized party to predict the next corresponding temporary identifier (i.e. the next temporary identifier of the same subscription).

5.7.3.5 Key issue #7.5: Transmitting permanent identifiers in secure interface

5.7.3.5.1 Key issue details

It is important to mitigate the risk of accidental or intentional exposure (e.g. due to sniffing of some interface by an insider) of permanent identifiers (subscription and equipment identifiers) in the radio access network (RAN) or the core network (CN, including interconnects). In a current LTE system, the RAN interface (Uu) is protected except for some initial RRC and NAS messages. The Next Generation system should at least maintain or improve the RAN interface security. In a current LTE system, the CN interfaces (e.g. S1-MME and S6a) are protected when IPsec is deployed, but

Lenovo Ex. 1007
Page 338

the adoption of IPsec is not mandatory, only recommended. The Next Generation system should at least maintain or improve the CN interface security.

5.7.3.5.2 Security threats

NOTE: Similar threats as in clause 5.7.3.2.2.

5.7.3.5.3 Potential security requirements

- Core Network traffic, which carries permanent subscription and equipment identifiers, shall be protected from eavesdropping.
- Radio Access Network traffic, which carries permanent subscription and equipment identifiers, shall be protected from eavesdropping.

Editor's Note: It is FFS if it is feasible to prevent eavesdrop of permanent subscriber and equipment identifiers in the radio interface in all scenarios, e.g. in a current LTE system - initial ATTACH REQUEST and emergency bearer service request.

5.7.3.6 Key issue #7.6: Transmitting permanent subscription identifiers only when needed

5.7.3.6.1 Key issue details

In a current LTE system, permanent or long-term subscription identifiers are available to multiple network functions (e.g. eNB, MME, and S-GW). In the Next Generation system, it can be fairly assumed that there will be not only different network functions, but also different network slices, services, and deployment scenarios. Therefore, the risk of exposing subscription's permanent identifier will increase. Hence it is important to design the protocols or interfaces so that permanent subscription identifiers are not transmitted to the entities where the permanent subscription identifier is not necessary for services and network operations. Moreover, when identification of a subscription is not necessary or when required by regulations, it should be possible to anonymize the permanent subscription identifiers before transmitting them.

5.7.3.6.2 Security threats

NOTE: Similar threats as in clause 5.7.3.2.2.

5.7.3.6.3 Potential security requirements

- It shall be possible to anonymize or conceal permanent subscription identifiers when appropriate. For example anonymization might be required by regulations, or the receiving node might not need to identify the subscription.

Editor's Note: It is FFS if the following two requirements should be handled as guidelines rather than requirements.

- Permanent subscription identifier should not be available to the network entities where the permanent subscription identifier is not necessary for services and network operations.
- Permanent subscriber identifiers shall not be transmitted in clear-text, whenever feasible.

5.7.3.7 Key issue #7.7: Using effective temporary or short-term equipment identifiers

5.7.3.1.7 Key issue details

Not only the subscription, but also the equipment could benefit from the usage of short-term identifiers when fulfilling privacy requirements. This key issue studies possibilities of using short-term identifiers for equipment and its effectiveness for equipment in a way that do not compromise the subscription privacy.

The usage of effective short-term equipment identifiers during a communication process may help to avoid the correlation between equipment identifier and subscription identifier for unauthorized entities.

Lenovo Ex. 1007
Page 339

5.7.3.7.2 Security and privacy threats

If equipment identifiers and subscription identifiers can be easily correlated, it may allow an attacker to compromise the subscriber's privacy. Further, correlation of equipment or subscription actions and data may allow an attacker to create interest or location profiles.

NOTE: Similar threats as in clause 5.7.3.2.2

5.7.3.7.3 Potential privacy requirements

- Temporary equipment identifiers should be used instead of permanent equipment identifiers in communication, whenever feasible.
- From one or more temporary equipment identifiers, it shall not be feasible for an unauthorized party to predict the next temporary identifier.

5.7.3.8 Key issue #7.8: Privacy protection of network slice identifier

5.7.3.8.1 Key issue details

NextGen architecture introduces the concept of network slices.

In order for the user to choose and to attach to a slice, an identification will be needed. The UE or the provider of the slice may use such slice identifier to select the relevant functions within a certain network slice.

Based on such network slice identification and on other information (e.g. subscription) available in the network, the UE can use different network slices depending on the type of application and service it requires.

5.7.3.8.2 Security and privacy threats

If an attacker can correlate the slice identifier with the subscription identifier, it is possible to identify a group of users that use the same slice, i.e. they belong to the same interest group, e.g. a group of police men or firefighters in MCPTT. If an attacker wants to deny service for a particular user group, the connection between subscription identifier and network slice identification may lead to such attack.

NOTE: Similar threats as in clause 5.7.3.2.2 also apply.

5.7.3.8.3 Potential security requirements

Ed.note: It is ffs whether for privacy purposes the identifier of a network slice may be temporary.

The identifier of a network slice may be confidentially protected.

It shall be not feasible by an unauthorized party to correlate a network slice identifier with long-term subscription identifiers.

5.7.3.9 Key issue #7.9: Need to protect entire Permanent Identifier.

5.7.3.9.1 Key issue details

Structured permanent identifiers, when not confidentiality protected in their entirety are capable of leaking Personally Identifiable Information (PII). For example, per TS 23.003, IMSI is composed as shown in figure 5.7.3.9.1-1.

Lenovo Ex. 1007
Page 340

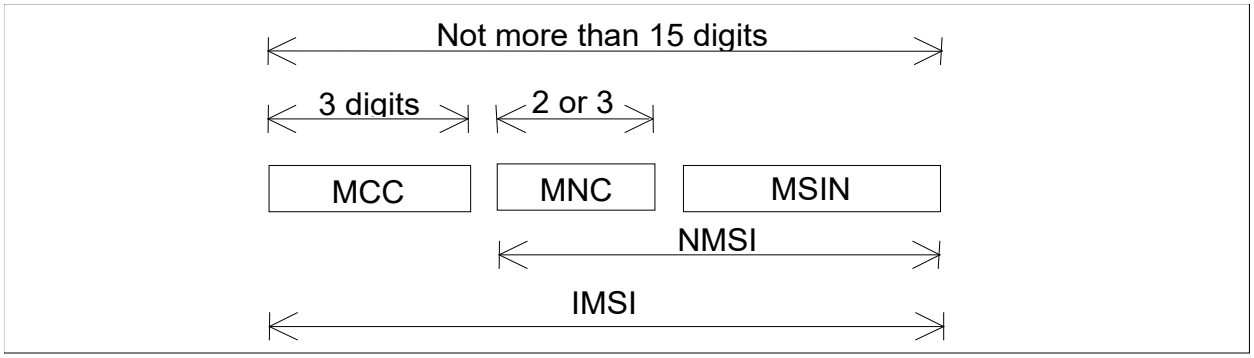


Figure 5.7.3.9.1-1: Structure of IMSI

IMSI is composed of three parts:

Mobile Country Code (MCC) consisting of three digits. The MCC identifies uniquely the country of domicile of the mobile subscriber;

Mobile Network Code (MNC) consisting of two or three digits for GSM/UMTS applications. The MNC identifies the home PLMN of the mobile subscriber. The length of the MNC (two or three digits) depends on the value of the MCC. A mixture of two and three digit MNC codes within a single MCC area is not recommended and is outside the scope of this specification.

Mobile Subscriber Identification Number (MSIN) identifying the mobile subscriber within a PLMN.

The National Mobile Subscriber Identity (NMSI) consists of the Mobile Network Code and the Mobile Subscriber Identification Number.

If only MSIN component of IMSI is being protected, the other components of IMSI (i.e., MCC and MNC) when captured by either passive or active attacker, are capable of conveying PII of the subscriber.

5.7.3.9.2 Security threats

Leaving a part of a Permanent Identifier unprotected can provide a passive attacker with enough foothold to weaken the entire Permanent Identifier protection.

In the case of a Sructured Permanent Identifier (e.g., an identifier holding multiple information components such as an IMSI), a passive or active attacker may glean PII of the subscriber based on the exposed components.

5.7.3.9.3 Potential security requirements

FFS

Editors Note: The tradeoff between having a requirement addressing threats above and complexity of associated solutions is FFS.

Lenovo Ex. 1007
Page 341

5.7.3.y Key issue #7.y: <key issue name>

5.7.3.y.1 Key issue details

5.7.3.y.2 Security threats

5.7.3.y.3 Potential security requirements

5.7.4 Solutions

5.7.4.1 Solution #7.1: UE can request an update of temporary identifier

5.7.4.1.1 Introduction

This solution addresses key issue #7.1.

5.7.4.1.2 Solution details

Editors' note: more details are needed here

Signalling messages should be defined to allow a UE to request the visited network to update its temporary identifier (or identities). It is too early to say exactly whether a new message type will need to be defined, or an existing message type adapted; and it is too early to say which node in the visited network will be the recipient of this message.

Note that this is a request that the visited network may (and normally will) fulfil – not a demand that it must fulfil. This means that the visited network retains ultimate control.

A possible, optional extension is that the UE drops the connection if the request is not fulfilled.

Note that this in no way reduces the network's ability to refresh temporary identities whenever its policy requires.

5.7.4.1.3 Evaluation

This solution partially addresses Key Issue #7.1. The network should, in any case, update temporary identifiers "often enough". But if that frequency is left to the individual network operator, as it has been in the past, then some operators may configure temporary identifiers to be updated very rarely. This solution allows the UE to take at least some action to improve matters in such circumstances.

If, in fact, a NextGen solution is adopted that **ensures** a suitably high frequency of refresh, then Solution #7.1 will add little value.

The solution is, necessarily, described only at a rather high level, because the detail depends on other choices about what sort of temporary identifiers are used and which network nodes are involved in assigning them. Nevertheless, it seems very likely that this solution will be achievable and applicable, no matter what choices are made.

5.7.4.2 Solution #7.2: UE encrypts permanent identifier sent to network

5.7.4.2.1 Introduction

This solution addresses key issue #7.1.

5.7.4.2.2 Solution details

5.7.4.2.2.1 Background

In this solution, NextGen networks need to have private keys, and UEs can obtain the corresponding public keys and verify their authenticity. The UE never sends its permanent identifiers (e.g. IMSI, IMEI) in clear, but only ever encrypted using the (verified) public key of the network.

Lenovo Ex. 1007
Page 342

Editor's note: It is ffs which messages should include encrypted identifiers. It is also ffs how exactly message formats should be adapted to accommodate the encrypted identifiers.

The mechanism is mandatory to implement and mandatory to use in networks. It is optional to support and optional to use in UEs, but support and use is recommended. Legacy UEs, or UEs for which signature verification would be in some sense too demanding, can send identifiers unencrypted, and networks should still accept these.

5.7.4.2.2.2 Provisioning and management of keys

The provisioning and management of public keys and certificates is the same as in solution #4.1. The UE uses the Network Node Public to encrypt permanent identifiers.

Editor's note: It is ffs whether to use the same Network Node key pair for both signature (in solution #4.1) and encryption (in solution #7.2), or to use a different key pair for each.

5.7.4.2.2.3 Revocation

Revocation is the same as in solution #4.1.

5.7.4.2.2.4 Signature algorithms and algorithm selection

UEs supporting this solution must support the ECIES signature algorithm.

Editor's note: It is ffs what reference to use for ECIES.

NOTE1: An alternative signature algorithm would be RSAES-OAEP (specified in PKCS #1 v2.2 and RFC 3447).

Editor's note: It is ffs how best to support new algorithms in future, such as quantum computing resistant algorithms. See the corresponding editor's note in clause 5.4.4.1.2.4.

NOTE2: It is important that any encryption algorithm used for this solution is probabilistic, so that the same identifier encrypted twice gives two different, unlinkable results.

5.7.4.2.3 Evaluation

TBD

5.7.4.3 Solution #7.3: Concealing permanent or long-term subscriber identifier by using pseudonyms and public key encryption

5.7.4.3.1 Introduction

This solution discusses one potential way to address the key issue #7.3 "Concealing permanent or long-term subscription identifier" by using the combination of pseudonyms and public key encryption of the permanent or long-term subscription identifier for rare cases.

NOTE: The "permanent or long-term subscription identifier" is referred as IMSI throughout the following text for conciseness.

In a current LTE system, there is already a mechanism of using short-term identifier in protocol procedures that involve a UE and a serving PLMN (e.g. C-RNTI by a radio access network and S-TMSI by a core network). However, when a short-term identifier for the UE does not exist or is lost in the core network, the UE is forced to identify itself using a long-term identifier (i.e. IMSI). The IMSI is used in an authentication procedure in which the serving PLMN uses the IMSI given by the UE to ask for relevant authentication information from a home PLMN.

.

Lenovo Ex. 1007
Page 343

5.7.4.3.2 Solution details

5.7.4.3.2.1 General

The UE and the home PLMN share a long-term identifier (IMSI) and a long-term key (K). The public key (PK_H) of the home PLMN is also available in the UE.

There is no need for a global PKI. Instead, the home PLMN may pre-provision the PK_H in the UE or use OTA to distribute the PK_H.

NOTE 1: It is in the scope of the security area #2 'Authentication' to decide which function (e.g. ARPF) stores the public (PK_H) and private (SK_H) key pair of the home PLMN.

NOTE 2: It is in the scope of the security areas #5 'Security within NG-UE' and the security area #12 'Credential provisioning' to decide which function (e.g. ME or USIM) stores the PK_H at the UE.

5.7.4.3.2.2 Attach using encrypted IMSI ($IMSI_{Enc}$)

During an initial attach, the UE encrypts its long-term identifier (IMSI) with the public key (PK_H) of the home PLMN and sends the encrypted IMSI ($IMSI_{Enc}$) to a serving PLMN.

Editor's Note: It is FFS to determine if it is feasible to provision a first pseudonym even before an initial attach in order to avoid the use of public-key encrypted identifiers.

NOTE 1: It is in the scope of the security areas #5 'Security within NG-UE' to decide which function (e.g. ME or USIM) encrypts the IMSI at the UE.

When the UE initiates an attach, it is necessary that the serving PLMN is able to identify the home PLMN of the UE. Therefore, the UE encrypts only the MSIN part of the IMSI while leaving in plain-text the MCC and the MNC part. The encryption needs to have randomization property, since otherwise every encryption would look the same and an attacker could tell that two encrypted identifiers conceal the same long-term identifier.

NOTE 2: The size of the $IMSI_{Enc}$ depends upon which public key encryption scheme is used. For example, using the Elliptic Curve Integrated Encryption Scheme (ECIES) based on a 256-bit elliptic curve with point compression, without a tag, and a format preserving encryption, the size of the $IMSI_{Enc}$ is in the order of 320 bits. It is in the scope of the security area #17 'Cryptographic algorithms' to decide if and which public key encryption schemes to standardize.

The home PLMN decrypts the $MSIN_{Enc}$ part of the $IMSI_{Enc}$ using the SK_H, and identifies the IMSI. The home PLMN is therefore able to fetch the corresponding security credentials to be used in the authentication procedure. Either the home PLMN or the serving PLMN may authenticate the UE.

NOTE 3: It is in the scope of the security area #2 'Authentication' to decide which function (e.g. ARPF) decrypts the $IMSI_{Enc}$ at the home PLMN.

The message size for transferring the $IMSI_{Enc}$ is larger than for the plain-text IMSI because of public key encryption. Therefore, after the UE is authenticated, the home PLMN assigns a pseudo IMSI ($IMSI_{Pseudo}$) to the UE, the $IMSI_{Pseudo}$ having the same length and format as the IMSI. In order to save the radio resources in attach procedures, the UE uses the $IMSI_{Enc}$ only when the valid $IMSI_{Pseudo}$ is not available. The $IMSI_{Pseudo}$ may be transferred encrypted (e.g. using a shared key resulting from public-key encryption, or using a key derived from K) between the home PLMN and the UE. However, if solution #7.X is used to reveal the IMSI to the serving PLMN, then $IMSI_{Pseudo}$ could be revealed as well in the similar fashion so that the serving PLMN sends the $IMSI_{Pseudo}$ in a protected message to the UE. There is no privacy breach in doing so because the serving PLMN already knows the IMSI.

The serving PLMN sends the $IMSI_{Pseudo}$ to the UE in in a separate protected message or piggy-backed to an existing protected message (e.g. in an NAS Attach Accept message in the current LTE system sent by a MME to a UE). During the $IMSI_{Pseudo}$ assignment, the $IMSI_{Pseudo}$ need not contain the MCC and the MNC, because they are already known from the IMSI.

It is possible that a poor implementation and/or policy configuration of the home PLMN could assign the same $IMSI_{Pseudo}$ repeatedly to the UE or the home PLMN could toggle between two fixed $IMSI_{Pseudo}$ for the UE. Therefore, the UE verifies that the newly assigned $IMSI_{Pseudo}$ is a fresh one, for example by at least comparing to the last one or the last two. The effect of such verification is that toggling a fixed set of $IMSI_{Pseudo}$ (which is not good) will require even more considerations (e.g. more memory and processing to maintain the set and its state for each UE) and therefore will

Lenovo Ex. 1007
Page 344

be discouraged. If the verification fails, the UE may take some soft-actions such as trying to reconnect to the network or perform other self-crippling features such as disconnecting from the network or refusing to establish a user plane connection.

NOTE 4: It is in the scope of the security area #2 'Authentication' to decide which function (e.g. ARPF) generates and stores the $IMSI_{Pseudo}$ at the home PLMN.

NOTE 5: It is in the scope of the security areas #5 'Security within NG-UE' and the security area #12 'Credential provisioning' to decide which function (e.g. ME or USIM) verifies and stores the $IMSI_{Pseudo}$ at the UE.

Figure 5.7.4.3.2.2-1 shows a simplified $IMSI_{Enc}$ attach procedure with respect to the variant of the solution #7.7 in 5.7.4.7.2.2, i.e. when the serving PLMN authenticates the UE and when the home PLMN reveals the IMSI to the serving PLMN to comply with LI requirements.

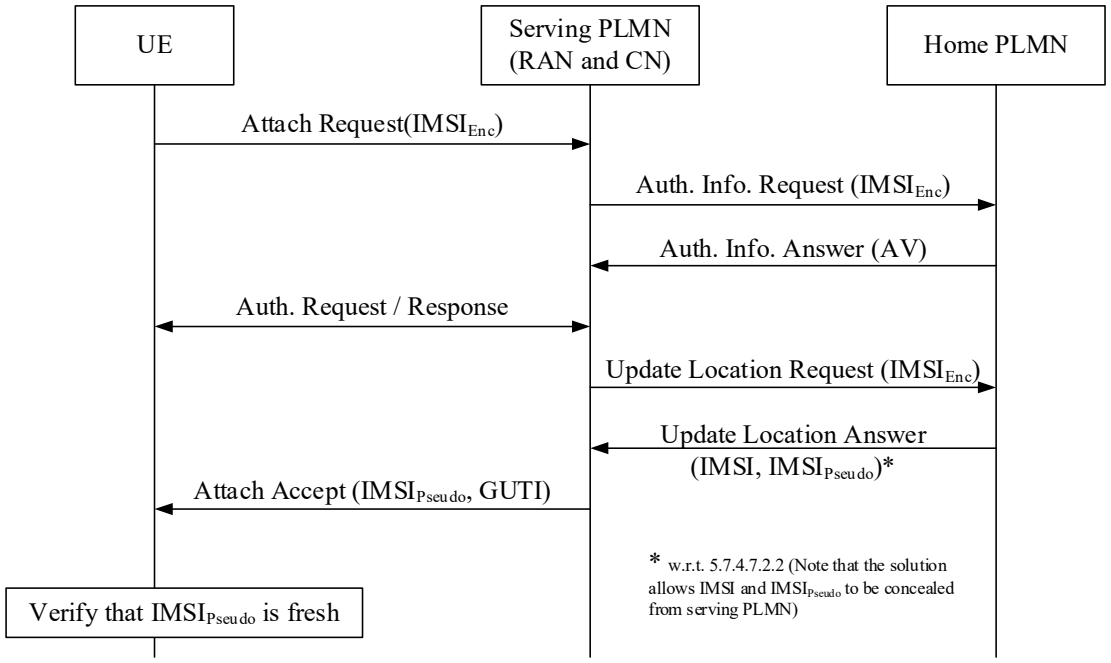


Figure 5.7.4.3.2.2-1: Simplified $IMSI_{Enc}$ attach procedure (w.r.t variant 5.7.4.7.2.2)

.

5.7.4.3.2.3 Attach using pseudo IMSI ($IMSI_{Pseudo}$)

Re-authenticating the UE is not required during all communications and therefore, for optimization, the serving PLMN assigns its own short-term identifiers to the UE. For example, the use of such short-term identifiers (i.e. GUTI or S-TMSI) already exists in a current LTE system.

However, when a short-term identifier used in the serving PLMN is lost or becomes invalid, the UE is required to reveal its identifier again. If the UE loses the short-term identifier, the UE sends the $IMSI_{Pseudo}$ in an Attach Request. If the serving PLMN loses the short-term identifier, the serving PLMN requests the UE to identify itself using the $IMSI_{Pseudo}$. The UE sends its $IMSI_{Pseudo}$ including the MCC and the MNC of the home PLMN. The rest of the process continues similarly as described in clause 5.7.4.3.2.2 except that UE uses $IMSI_{Pseudo}$ instead of $IMSI_{Enc}$. The home PLMN assigns a new $IMSI_{Pseudo}$ to the UE. As such, the UE does not use the same $IMSI_{Pseudo}$ multiple times

Figure 5.7.4.3.2-2 shows a simplified $IMSI_{Pseudo}$ attach procedure with respect to the variant of the solution #7.7 in 5.7.4.7.2.2, i.e. when the serving PLMN authenticates the UE and when the home PLMN reveals the IMSI to the serving PLMN to comply with LI requirements.

Lenovo Ex. 1007
Page 345

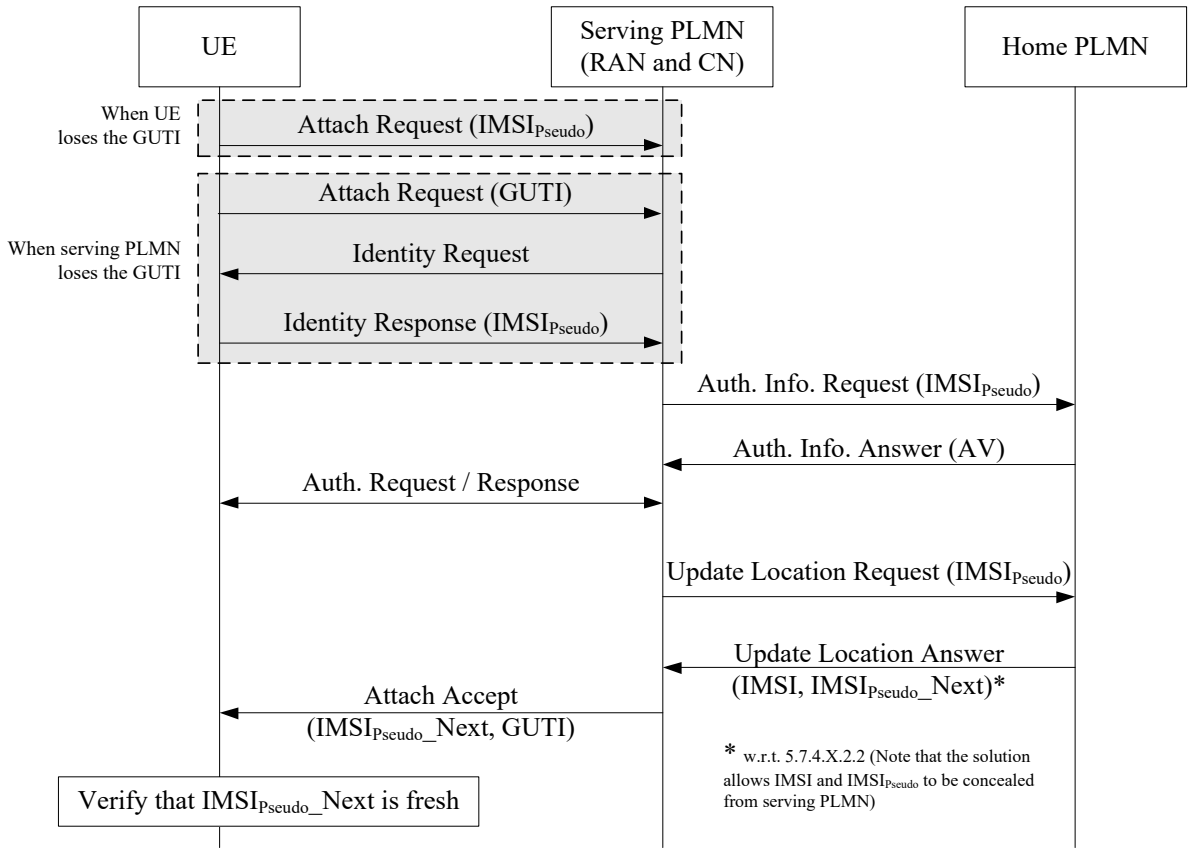


Figure 5.7.4.3.2-2: Simplified $IMSI_{Pseudo}$ attach procedure (w.r.t variant 5.7.4.7.2.2)

Editor's Note: It is FFS to determine how a potential DoS attack on the HSS, caused by computational overload due to public key decryption, can be minimized.

NOTE: Details on how to deal with LI with VPLMN is given in clause 5.7.4.7.

5.7.4.3.2.4 Handling abnormal cases

A recovery mechanism is necessary to handle an unlikely, but possible, event of the $IMSI_{Pseudo}$ getting out-of-sync between the UE and the home PLMN. Following abnormal cases are identified for the sake of completeness and to show that the UE is not locked out of the system:

5.7.4.3.2.4.1 Invalid $IMSI_{Pseudo}$

This is a case when the UE sends an $IMSI_{Pseudo}$, but the home PLMN does not recognize the $IMSI_{Pseudo}$. This case may occur, for example, when the UE had incorrectly stored the $IMSI_{Pseudo}$ due to hardware or software glitch or the home PLMN had lost the $IMSI_{Pseudo}$ due to hardware or software failure. The recovery mechanism for this case is similar to what exists today for the LTE system and is shown in the Figure 5.7.4.3.4.1-1 followed by the description of the steps:

Lenovo Ex. 1007
Page 346

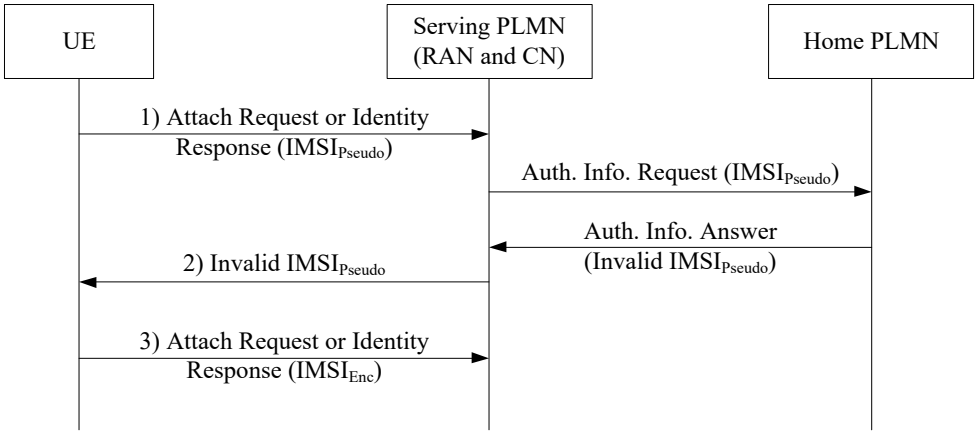


Figure 5.7.4.3.4.1-1: Handling $IMSI_{Pseudo}$ that is invalid

1) The UE sends an $IMSI_{Pseudo}$ to the network.

2) The network sends an indication of "invalid $IMSI_{Pseudo}$" to the UE.

3) The UE sends an $IMSI_{Enc}$ to the network. The rest of the procedure proceeds as described in earlier subclauses.

NOTE: Since the public key encryption used is probablisitc, i.e. having a randomization property, the same IMSI when encrypted multiple times produces different $IMSI_{Enc}$ values. Therefore, it is not feasible for an OTA sniffer to link multiple $IMSI_{Enc}$ values to the same IMSI.

5.7.4.3.2.4.2 Already assigned $IMSI_{Pseudo}$

This is a case when the UE_1 sends an $IMSI_{Pseudo}$, but the $IMSI_{Pseudo}$ is currently assigned to the UE_2 in the home PLMN. This case may occur, for example, when the UE_1 had incorrectly stored the $IMSI_{Pseudo}$ due to hardware or software glitch and the stored $IMSI_{Pseudo}$ happened to be the one currently assigned to the UE_2. The recovery mechanism for this case is similar to what exists today for the LTE system and is shown in the Figure 5.7.4.3.2.4.1-1, followed by the description of the steps.

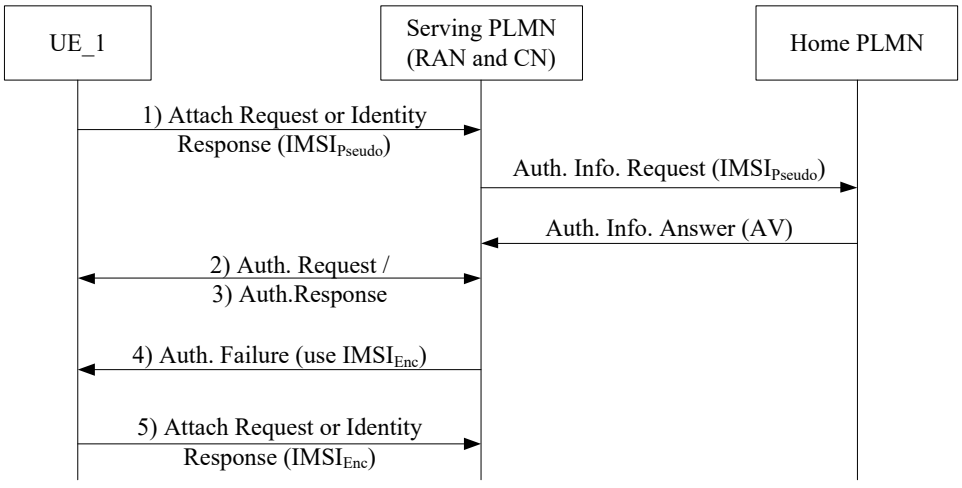


Figure 5.7.4.3.2.4.1-1: Handling $IMSI_{Pseudo}$ that is assigned to another UE

1) The UE_1 sends an $IMSI_{Pseudo}$ to the network.

2) The network identifies that the $IMSI_{Pseudo}$ belongs to the UE_2 and therefore sends authentication challenge (corresponding to the UE_2) to the UE_1.

3) The UE_1 sends authentication response to the network.

Lenovo Ex. 1007
Page 347

4) The network detects the authentication failure and sends failure message to the UE_1, optionally indicating the UE_1 to use $IMSI_{Enc}$.

5) The UE_1 sends the $IMSI_{Enc}$ to the network. The rest of the procedure for the UE_1 proceeds as described in earlier subclauses. The network knows that the $IMSI_{Pseudo}$ was sent by the UE_1 and not by the UE_2. Therefore, the network keeps the $IMSI_{Pseudo}$ still assigned to the UE_2. The UE_1 is assigned a new $IMSI_{Pseudo}$.

5.7.4.3.3 Evaluation

The solution has the following properties:

- The UE only needs to store one public key associated with the home PLMN. This is significantly different than requiring the UE to store the public key of all potential serving PLMNs it may roam into, or having to distribute those keys when needed. There is no need for a global PKI. Instead the home PLMN operator can configure or revoke its public key in the UE, e.g., using OTA.
- The encryption needs to be randomized, but that does not constitute a serious problem, since most or all existing public key encryption schemes are randomized.
- Because of public key encryption, the $IMSI_{Enc}$increases the size of the attach message. However, the solution rarely uses the $IMSI_{Enc}$, i.e. only when $IMSI_{Pseudo}$ does not exist or is out-of-sync.
- The UE verifies that the same $IMSI_{Pseudo}$ is not assigned to it all the time.
- The solution is compatible both when the authentication of the UE is done at the home PLMN or at the serving PLMN.

The solution addresses all the three requirements of the key issue #7.3 and is effective in concealing the long-term identifier from any passive or active attacker anywhere on the path between the UE and the serving PLMN's core network, including IMSI-catchers, untrusted or compromised network entities.

5.7.4.4 Solution #7.4: Privacy enhanced Mobile Subscription identifier (PMSI)

5.7.4.4.1 Introduction

Editor's note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the security area.

This solution presents a way to provide identifier privacy during the attach procedure in the NextGen system. For the attach to the network, a UE presents a short-lived identifier to the network instead of IMSI used in LTE or UMTS systems. The short-lived identifier, named "Privacy enhanced Mobile Subscription identifier", is used during an attach, and if the attach procedure includes an authentication and is successfully completed, the UE and network (i.e., HSS or equivalent function in the NextGen system) update the PMSI with a new one that would be used for the next attach in a secure way.

5.7.4.4.2 Solution details

A NextGen UE is provisioned with an IMSI and an initial PMSI associated with its subscription by the operator. The PMSI has the same format as IMSI so that a serving network is able to determine the home PLMN based on the first 5 or 6 digits of the PMSI.

The solution is described assuming that the CP-CN and SEAF are co-located to make the flows easier to understand as they look like LTE. It was also assumed that K_{ASME} is the name of the key provided in the authentication vector (AV).

When the UE attaches to the network, the UE provides its PMSI in the attach request. When a CP-CN/SEAF receives the attach request from the UE, it sends an authentication information request including PMSI to the AUSF. Upon receiving the authentication information request, the AUSF retrieves the PMSI from the request and identifies the corresponding IMSI associated with the PMSI. Based on the identified IMSI, the AUSF prepares an authentication vector as in LTE. In addition to the authentication vector, the AUSF selects (or derives) a next PMSI that would be used for the next attach by the UE. The next PMSI is encrypted using a shared key with the UE and included in the authentication information response message for the CP-CN/SEAF. The CP-CN/SEAF forwards the encrypted PMSI to the UE in the NAS authentication request message.

Lenovo Ex. 1007
Page 348

Editor's note: It is FFS to find out whether the PMSI update procedure could be piggy-backed into the AKA procedure. This would enable the possibility for PMSI update also when the UE is connected to a legacy serving network.

If the authentication with the CP-CN/SEAF is completed successfully, the UE acknowledges the receipt of the next PMSI to the AUSF. The CP-CN/SEAF in the serving network can request the IMSI associated with the PMSI when it is required.

Editor's note: LI aspects in VPLMN are FFS.

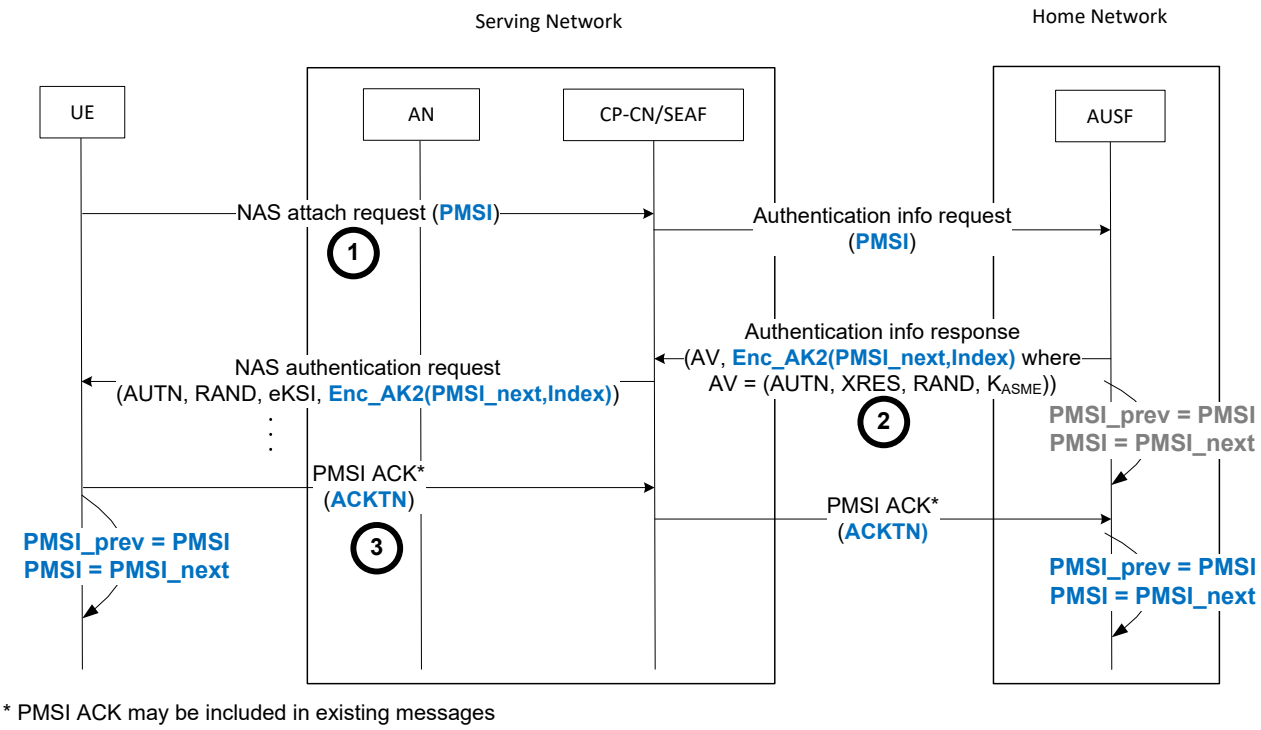


Figure 5.7.4.4.2-1. Attach procedure using PMSI

The initial PMSI and PMSI derivation key (i.e., K_{PMSI}) are installed at the UE and AUSF. The PMSI derivation key is used to confirm that the UE and AUSF have been synchronized with the next PMSI that would be used for the next attach.

Editor's Note: how to provision the initial PMSI and PMSI derivation key is FFS.

1. The UE sends an attach request using the PMSI to the network. When the CP-CN/SEAF receives the attach request message from the UE, it sends an authentication information request message to the AUSF where the authentication information request message includes PMSI and the serving network identifier. The AUSF identifies the IMSI that is associated with the PMSI and prepares an authentication vector, i.e., AV. Then, the AUSF selects the next PMSI that would be used by the UE for the next attach. The next PMSI (i.e., PMSI_next) is derived from the PMSI received from the CP-CN/SEAF as follows:

$$\text{PMSI\_next} = \text{MCC} \mid \text{MNC} \mid \text{Truncate-x}(\text{F1}(K_{PMSI}, \text{PMSI}))$$

where F1 is a PMSI derivation function, e.g., HMAC-SHA-256, K_{PMSI} is a PMSI generation key, MCC is the mobile country code and MNC is the mode network code, and Truncate-x is a function that truncates the input to x bits (e.g., by taking the first x bits of the input).

PMSI is associated with an index for at least two reasons. First, the PMSI_next derived for the UE may be currently used by another UE. In such case, the AUSF derives a new PMSI_next by running the PMSI derivation again using the PMSI_next as input to F1. This derivation continues until a new PMSI is not currently being used by other UEs. Whenever a PMSI next is derived, the associated index is increased by a certain number (e.g., 1). This index is provided to the UE so that the UE can derive the correct PMSI_next using the index. Second, the use of index to calculate PMSI ensure that PMSI is fresh for that user.

Lenovo Ex. 1007
Page 349

2. The AUSF sends an authentication information response to the CP-CN/SEAF including the authentication vector and the PMSI_next and index pair. The PMSI_next and index pair is encrypted using a key (AK2) that is only known to the UE and AUSF. This key is derived based on K_{PMSI} as:

AK2 = KDF(K_{PMSI}, RAND)

where KDF is a key derivation function and RAND is a random number. The same RAND used for deriving AUTN in AV may be used for the key derivation.

At this point, the AUSF sets (1) the PMSI_prev to the PMSI used for the current authentication and (2) the PMSI to the PMSI_next for the next attach; and sets the pending PMSI acknowledgement flag.

a. PMSI_prev = PMSI
b. PMSI = PMSI_next
c. Pending ack = 1.

NOTE 1: If the ongoing authentication procedure fails for some reason, there would be a case that the UE may not have received the PMSI_next after sending an attach request to the network. In such case, the UE needs to attach to the network again using the same PMSI that was used for the previous failed attach. If the AUSF was not acknowledged the receipt of the PMSI_next from the UE, the PMSI_prev may be used by the AUSF to identify the IMSI.

The CP-CN/SEAF sends an authentication request message to the UE based on the received AV. Also, the CP-CN/SEAF includes the encrypted PMSI_next and index pair in the authentication request message.

Editor's note: It is FFS whether PMSI encryption method could be such that encrypted PMSI_next and index pair could be embedded into parameters of the legacy authentication request message.

3. The UE performs authentication with the CP-CN/SEAF and if the authentication is successful, the UE derives the AK2 in the same way as in the AUSF. Using the AK2, the UE decrypts the PMSI_next and index pair and verifies the PMSI_next by deriving it in the same way as in the AUSF. If the PMSI_next and index pair is verified, the UE sets (1) the PMSI_prev to the PMSI used for the current authentication and (2) the PMSI to the PMSI_next for the next attach.

d. PMSI_prev = PMSI
e. PMSI = PMSI_next

Until the next attach occurs, the UE uses the PMSI_prev as its identifier and provides it to the network when requested.

The UE sends the PMSI acknowledgement (i.e., PMSI ACK) message that includes the acknowledgement token (ACKTN) to the AUSF, where the ACKTN is constructed as:

ACKTN = MAC-A

where MAC-A = F2(AK3, PMSI_next | index)

where F2 is a message authentication function and AK3 = KDF(K_{PMSI}, "ACK authentication key")

NOTE3: ACKTN is used to acknowledge the receipt of PMSI_next and index.

The CP-CN/SEAF forwards the PMSI acknowledgement received from the UE and the associated PMSI to the AUSF.

Editor's note: Including the associated PMSI (that was sent in message 1) in the PMSI acknowledgement message enables the AUSF to identify the PMSI_next that shall be acknowledged. Whether the CP-CN/SEAF or the UE includes the PMSI in the acknowledgement message is FFS.

Editor's note: whether the acknowledgements could be embedded into legacy signalling messages is FFS. This would enable PMSI update also when UE is connected to a legacy serving network.

When the AUSF receives the PMSI acknowledgement message, the AUSF verifies the ACKTN by deriving it in the same way as in the UE. If the verification is successful, the AUSF clears the pending PMSI acknowledgement flag (i.e., Pending ack) set in step 2.

Editor's note: It is FFS in which message, the serving network may obtain the IMSI associated with the PMSI.

Editor's note: Dealing with the failure cases, e.g the HSS losing PMSIs, without revealing IMSI is FFS.

Lenovo Ex. 1007
Page 350

If the PMSI acknowledgement is lost, the corresponding PMSI at the AUSF is in the pending acknowledgement state. When the UE uses the PMSI for the next attach, the AUSF shall locate the PMSI from the acknowledged PMSIs or unacknowledged PMSIs. The unacknowledged PMSIs shall not be allocated to other UEs.

Editor's Note: The exposure of HPLMN's routing information (e.g. MCC and MNC in case of IMSI) will be dealt with in a new KI.

5.7.4.4.3 PMSI initialization

When a UE attaches to a network, if it does not have a PMSI, the UE triggers the PMSI initialization procedure as follows.

1. The UE performs a PMSI initialization procedure by sending PMSI initialization indication to the network during the attach (using an IMSI).

NOTE 1: PMSI initialization is solely determined by the UE, which prevent a rogue base station from requesting an IMSI by triggering PMSI initialization.

NOTE 2: If a USIM supports the PMSI, PMSI initialization happens only once. Therefore, the IMSI is sent to the network only once.

NOTE 3: If a USIM does not support the PMSI, PMSI initialization shall be done by the ME. In such case, PMSI initialization happens when the USIM is installed in a new device.

Editor's note: It is FFS whether PMSI initialization by the ME causes a substantial privacy risk and needs to be mitigated by other means.

2. Upon receipt of authentication information request by the serving network with the PMSI initialization indication, the AUSF prepares authentication vector (AV) as normal, but derives two keys from the K_{ASME} in the AV.

   K_{PMSI}' = KDF(K_{ASME}, "PMSI generation key derivation")

   K_{ASME}' = KDF(K_{ASME}, "K_{ASME} derivation during PMSI initialization")

   where KDF is a key derivation functions, e.g., HMAC-SHA-256

   Then, K_{ASME} in the authentication vector is set to K_{ASME}'. K_{PMSI}' is used to encrypt the $K_{PMSI,}$ PMSI and PMSI index that are initialized to the UE.

NOTE 4: the original K_{ASME} derived by AUSF does not leave the AUSF. The original K_{ASME} is only used to generate K_{ASME}' and K_{PMSI}' by the AUSF.

3. The AUSF includes the encrypted K_{PMSI}, PMSI, and PMSI index in the PMSI initialization information element and sends the PMSI initialization information element to the UE as a part of the authentication information response.

NOTE 5: The PMSI initialization information element shall be defined.

4. Upon receipt of NAS authentication request from the network, the UE performs the following.

   The UE derives K_{PMSI}' and K_{ASME}' form K_{ASME} as done by the AUSF.

   The UE uses K_{ASME}' for K_{ASME}.

   The UE obtains $K_{PMSI,}$ PMSI and PMSI index by decrypting the received message from AUSF using K_{PMSI}'.

Editor's note: The UE behavior in case of authentication failure is FFS.

At the completion of step 4, the AUSF and the UE are synchronized with the K_{PMSI}, PMSI, and PMSI index.

5.7.4.4.4 Evaluation

If the authentication procedure fails for some reason, the solution proposes that the UE attachs to the network using the same PMSI that was used for the previous failed attach. However, by using the same PMSI, an attacker may be able to correlate pseudonyms and thus, compromise privacy.It is always a trade-off whether to have new signalling messages or

Lenovo Ex. 1007
Page 351

whether to add new functionality in UE and AU. This solution proposes that CP-CN/AU forwards the encrypted PMSI to the UE in the NAS authentication request message. Thus, there is a need to specify a new NAS messages.

5.7.4.5 Solution #7.5: Effective generation of temporary or short-term identifiers using channel estimation

5.7.4.5.1 Introduction

This solution addresses key issues #7.4 and #7.7.

It proposes a way to efficiently generate temporary or short-term identifiers in next generation system by using the randomness properties of channel estimation.

The channel estimation is an important part of Channel State Information (CSI) that indicates how a signal propagates from the transmitter to the receiver. The CSI makes it possible to adapt transmissions to current channel conditions and to achieve reliable communication. Besides, channel estimation is unpredictable and presents random properties due to propagation effects such as scattering, diffraction, fading, and power decay with distance.

The principle of this solution is to take advantage of this randomness to feed the generation of temporary or short-term identifier.

5.7.4.5.2 Solution details

The solution assumes that CSI reporting is available in next generation system. Moreover, the solution assumes that a secure link has been established between the UE and the CN.

In the following, the term depositary refers to the entity in the CN that manages the temporary/short-term ID that needs to be changed. From an LTE point of view, the depositary could be the MME (for GUTI), the eNB (for C-RNTI) or the PGW (for IP-address).

The general process is illustrated in figure x and is described below.

1. The UE and the gNB are communicating over the Uu interface. For the purpose of the communication, channel estimation can be performed in order to adapt the link to the propagation conditions.
2. A change request is emitted in order to change a temporary/short term ID. This change request can come from the depositary, the gNB or the UE.
3. If no channel estimation was performed during 1, this is done by the UE and/or the gNB. Depending on the temporary/short-term identifier that needs to be changed, the channel estimation measured by the UE (option A) or the gNB (option B) is sent through CSI reporting to the depositary. The CSI report can contain the complete response or a selected part depending on the application case.

In order to ensure the randomness of the CSI report, some processing can be applied on the channel estimation to improve its randomness quality. This operation can be done either by the UE or the gNB, either by the depositary in 4.

4. The depositary uses the CSI report as a random source for the generation of the new temporary/short-term identifier. Depending of the application case, the depositary can :
   - use only the channel estimation report as a source to generate a new identifier,
   - combine the channel estimation report with a own process that could exhibit deterministic properties (if based on counter for instance). The random channel estimation could efficiently hide these flaws.

   Editor's note: How collisions are handled in the core network is ffs

5. The depositary transmits the new temporary/short-term identifier to the appropriate entity, UE (option A), or gNB (option B), depending on the application case.

Lenovo Ex. 1007
Page 352

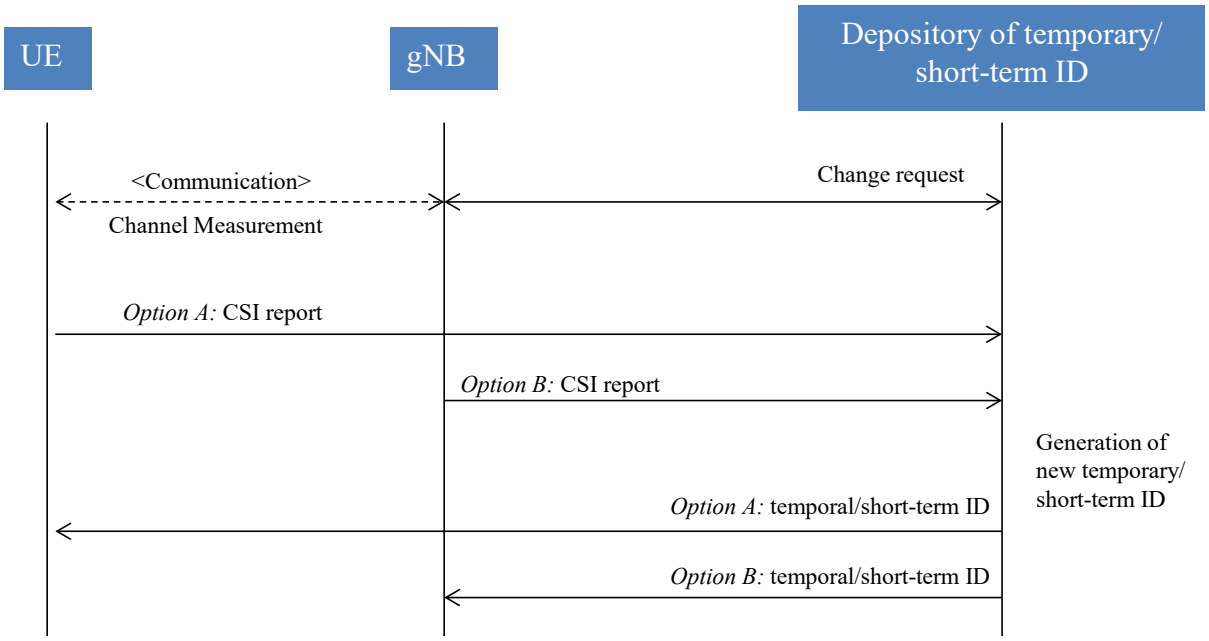


Figure 5.7.4.5.2-1: Generalized data-flow for generating temporary/short-term identifiers

5.7.4.5.3 Evaluation

The solution presented here has the following properties:

- The method reuses the computation of channel estimation that is done for other purposes (equalization, link adaptation, etc.) and thus does not require the implementation of new particular techniques.
- The channel estimation is unpredictable for an attacker. Indeed, with spatial decorrelation, an eavesdropper cannot observe the same channel and thus cannot compute the temporary identifier itself.

Editor's note: The unpredictability of the channel estimation is ffs

- From one or more temporary identifiers, it is not possible for an unauthorized party to identify the corresponding permanent identifier as specified in 5.7.3.4.3. Indeed, the process does not rely on the permanent identifier.
- From one or more temporary identifiers, it is not possible for an unauthorized party to predict the next temporary identifier as specified in 5.7.3.4.3 and 5.7.3.7.3. The computation of the next temporary identifier is based only on the channel estimation that is unpredictable and changes after only few seconds due to spatial and time decorrelation.
- The method can be combined with other techniques that need to be randomized. It enables to use a simple generation process by the depositary completed by a random source from the channel.
- The method can be used both for any kind of temporary or short-term identifier (for subscriber, device, etc).

Editor's note: This method shall be evaluated in comparison with current techniques.

Editor's note: It is ffs to show how this method improves the refreshment of the temporary identifiers.

Editor's note: How to deal with mobility issue at the NAS level is ffs

5.7.4.6 Solution #7.6: Parameters for Refreshing of temporary subscription identifier

5.7.4.6.1 Introduction

This solution defines a non-exhaustive list of parameters that could be used to define the maximum period for temporary identifiers. This solution addresses key issue# 7.1.

By defining these parameters, recommendations can be given for different subscription / service refresh parties in a consistent way and products can be developed in a consistent way from many suppliers.

Lenovo Ex. 1007
Page 353

5.7.4.6.2 Solution details

The refresh period should be defined as one or more of the following where the first to occur triggers a Temporary subscriber identifier refresh:

- a number of request for a specific service (e.g. the number of outgoing calls)
- a time period
- a number of radio resource changes

5.7.4.6.3 Evaluation

TBA

5.7.4.7 Solution #7.7: Revealing permanent or long-term subscriber identifier to a serving PLMN

Editor's Note: The requirements on LI in NextGen are FFS or at least need to be confirmed by SA1 or SA3-LI.

NOTE: FFS whether this solution meats VPLMN non-assistance requirements.

5.7.4.7.1 Introduction

The solution #7.3 proposes a mechanism that conceals the long-term subscriber identifier from all network entities on the path between the UE and the home PLMN (HPLMN), including the serving PLMN (SPLMN). However, doing so has implications on lawful interception (LI) as discussed in the clause 5.7.3.3.1. This solution addresses LI aspects for solutions addressing the key issue #7.3.

In order to address the LI requirements, the solution provides variants that reveal the long-term identifier to the SPLMN, which can be summarized as follows:

- the long-term identifier is always concealed from all the network entities in the path between the UE and the serving PLMN's core network, including the serving PLMN's radio access network; and
- the long-term identifier is known to the SPLMN's core network only after the UE has successfully completed the authentication.

5.7.4.7.2 Solution variants

5.7.4.7.2.1 Solution 7.7-A: Home PLMN authenticates UE

A UE is authenticated at a home PLMN and not at a serving PLMN. In other words, the serving PLMN proxies the authentication procedure between the UE and the home PLMN. The home PLMN itself authenticates the UE instead of sending authentication information (e.g. authentication vector in the current LTE system) to the serving PLMN. Since the UE identifier that is used in the authentication procedure is a pseudonym or an encrypted long-term identifier, the serving PLMN does not yet know the long-term identifier.

If the home PLMN determines that the UE is successfully authenticated, the home PLMN sends the long-term identifier and necessary keying material for the UE to the serving PLMN in a separate message or piggy-backed to an existing message. Now, the serving PLMN knows the long-term identifier of the UE and can perform lawful interception without the home PLMN's assistance or visibility.

NOTE: A successful UE authentication at the home PLMN, proxied by a serving PLMN, implicitly indicates that the UE is present at the serving PLMN.

5.7.4.7.2.2 Solution 7.7-B: Serving PLMN authenticates UE

A UE is authenticated at a serving PLMN and not at a home PLMN. This is similar to what is done in the current LTE system where the home PLMN sends authentication vector to the serving PLMN so that the serving PLMN can itself authenticate the UE. However, since the UE identifier that is used in the authentication procedure is a pseudonym or an encrypted long-term identifier, the serving PLMN does not yet know the long-term identifier.

Lenovo Ex. 1007
Page 354

When the home PLMN gets informed by the serving PLMN that the UE is successfully authenticated and is registered in the serving PLMN (e.g. via an Update-Location-Request message in the current LTE system sent by a MME to a HSS), the home PLMN sends the long-term identifier to the serving PLMN in a separate message or piggy-backed to an existing message (e.g. in an Update-Location-Answer message in the current LTE system sent by a HSS to a MME). Now, the serving PLMN knows the long-term identifier of the UE and can perform lawful interception without the home PLMN's assistance or visibility.

NOTE: A confirmation from a serving PLMN to a home PLMN about successful UE authentication makes the serving PLMN accountable for claiming that UE is actually present at the serving PLMN.

5.7.4.7.3 Evaluation

- The authentication of the UE can be done either at the home PLMN or at the serving PLMN.-
- When the authentication is done at the home PLMN, proxied by a serving PLMN, it is implicitly indicated that the UE is present at the serving PLMN.
- When the authentication is done at the serving PLMN, the home PLMN can hold the serving PLMN accountable in case of false claims on the presence of the UE at the serving PLMN.
- The long-term identifier is known to the serving PLMN's core network only after the UE has successfully completed the authentication.

5.7.4.8 Solution #7.8: Opportunistic encryption for IMSI exchange

5.7.4.8.1 Introduction

This solution addresses key issues #7.2.

Editor's note: This solution may also address the key issue planned in the EN of 5.7.4.3 "The exposure of HPLMN's routing information (e.g. MCC and MNC in case of IMSI) will be dealt with in a new KI".

5.7.4.8.2 Solution details

In this solution the UE and the gNB use opportunistic encryption in order to exchange the IMSI when it is strictly necessary. It is thus assumed that a previous attempt with a temporary identifier has failed as indicated in Figure x (step 1 and 2).

To avoid a clear text transmission of the IMSI, the UE can build a secure link over the radio air interface with the gNB. It is for further study which opportunistic algorithms can be used by the UE and the gNB. Examples of algorithms are:

- cryptographic algorithms based on elliptic curves such as Diffie-Hellman. This algorithm has the advantage to be well developed but requires high computing capabilities.
- secret key generation that takes advantage of channel randomness to design a key that is shared only by the gNB and the UE. This algorithm requires less computing capabilities (as it re-uses the channel estimation resource). However, this algorithm mainly applies in Time Division Duplex (TDD).

The information necessary for the setting of such scheme can be exchanged:

- during the prior exchanges of the identification procedure (during the attempt with temporary identifier step 1 of figure 5.7.4.8.2-1). This solution increases signalling but enables a faster computation of the algorithm in case of IMSI transfer.
- in a specific procedure after the failure of the temporary identifier corresponding to step 3 of figure x. In this case, the classical procedure with the temporary identifier is more efficient, but the later computation of the key between the UE and the gNB requires extra exchanges, what can cause latencies.

The computed key protects both the HPLMN's routing information part (MNC and MCC in LTE) and the subscriber's identifier part (such as the MSIN in LTE) what provides an enhanced protection against eavesdropping (step 4 of figure x).

Moreover, this key can be computed and held into memory once the authentication is performed, for a further usage to protect a new attach procedure, or to protect the exchange of other sensitive information regarding privacy. In addition, it can be used in another integrity control mechanism.

Lenovo Ex. 1007
Page 355

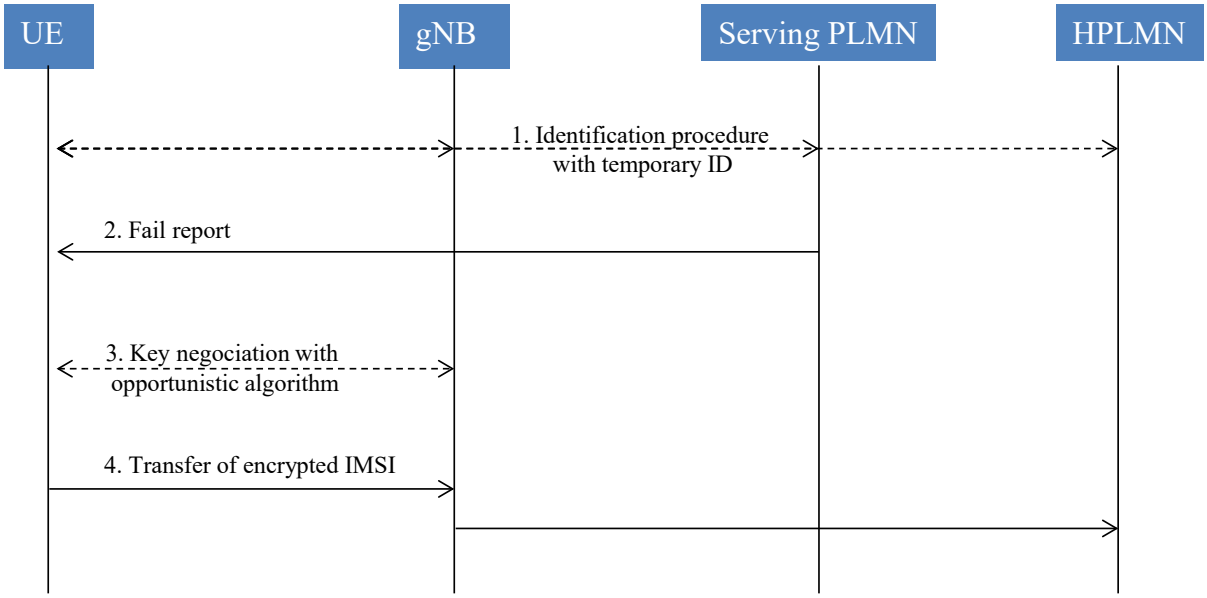


Figure 5.7.4.8.2-1: Generalized data-flow for opportunistic encryption

NOTE: Opportunistic encryption could also be extended and applied for the exchange of GUTI/TMSI to resist against tracking based on these identifiers.

Editor's note: It is FFS to show how opportunistic encryption can be resilient against active attack

5.7.4.8.3 Evaluation

This method provides a protection of the radio air interface and prevents passive eavesdropper from catching IMSI. Besides, it protects from advanced eavesdropping that has network access as it protects the HPLMN's routing information (eg. MCC and MNC part of the IMSI).

The method does not rely on a prior distribution of keys since they are computed on the fly by the UE and the gNB. Several variants can be implemented depending on UE capabilities.

Moreover, this computed key could be further used in other security mechanisms (new attach procedure or integrity control).

Besides, the proposed solution could also be extended to protect GUTI/TMSI exchanges in order to prevent tracking based on these identifiers.

Another advantage is that since this protection is being solely achieved in the serving network, it allows being fully compliant with serving/home network regulatory policies.

However, this method can be sensitive to some man-in-the-middle attack as soon as transmission is unauthenticated during the key negotiation procedure. Nevertheless, an integrity control of the messages for the computation of the key could contribute to detect and mitigate such attacks.

5.7.4.9 Solution #7.9 Adding the Diffie-Hellman key exchange process to the attach procedure

5.7.4.9.1 Introduction

NOTE: This solution addresses passive attacks only.

The proposed scheme is to address the key issue #7.2 Concealing permanent or long-term subscription identifier, and it also relates to the key issue 3.1 Interception of radio interface keys sent between operator entities

Lenovo Ex. 1007
Page 356

The Diffie-Hellman (DH) key exchange protocol is the mostly used key agreement scheme to establish the shared secret keys between two parties over public channel. We propose to add the Diffie-Hellman key exchange process to the attach procedure in order to eliminate three security threats if attacks are passive: privacy of subscriber identifies, long-term secret key leakage, insecurity of links between MNOs. The basic idea is that the DH key exchange protocol is integrated into the identity acquisition stage of the attach procedure. The agreed secret key K_{DH} between a UE and the network is used to generate the ciphering key K_E to encrypt the real identity of a UE such that a passive attacker is unable to catch it. At the end of the AKA protocol, UE and the network generate the same key K_{mid} on the basis of the shared root key. Then UE and the network compute the session key Ks using the key K_{mid} and the key K_{DH}. In the SMC stage, the MAC values of the message security mode command and the message security mode response are calculated with the session key Ks in order to confirm the correctness of the key Ks. The proposed scheme can also alleviate the possible DoS attacks in the attach procedure by embedding anti-DOS attacks measure in the protocol.

5.7.4.9.2 Solution details

Three authentication-related functions are involved in the attach procedure, which are:

- Authentication Credential Repository and Processing Function (ARPF)
- Authentication Server Function (AUSF)
- Security Anchor Function (SEAF)

The proposed attach procedure is depicted in Figure 5.7.4.9.2-1, where the term "UE" instead of "NG-UE" is still used for simplicity.

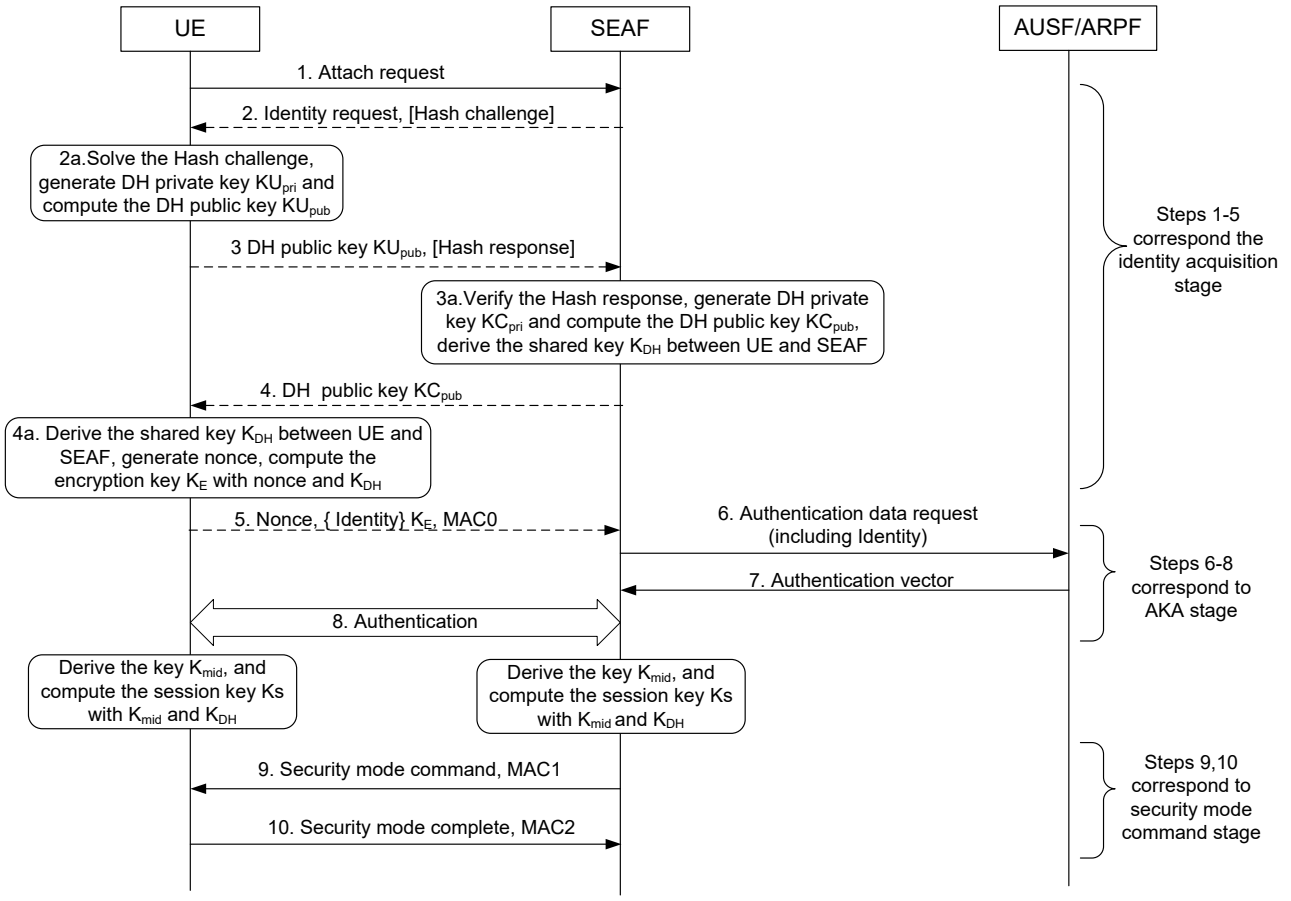


Figure 5.7.4.9.2-1. The proposed attach procedure

The proposed attach procedure is illustrated as follows:

1. UE initiates the attach procedure, and sends an *Attach request* to the SEAF, including the temporary identity like GUTI used in LTE if available.

Lenovo Ex. 1007
Page 357

2. After receiving the *Attach request*, if the temporary identity is in the *Attach request* message, SEAF checks whether there exists a real identity corresponding to the temporary identity and whether SEAF has established a shared DH key K_{DH} with the UE, SEAF will go into step 6 in the case that both conditions are met. Otherwise, SEAF sends *Identity request* message back to the UE, which optionally includes the hash challenge to thwart DoS attacks. The *Identity request* message is also dispatched by SEAF if no temporary identity GUTI is contained.

If the SEAF has justified that it is under DoS attacks, it will embed the *hash challenge* into the *Identity request* message. It is constructed as follows. The SEAF randomly generates a positive integer *x* with *n* bit length in binary, a 128-bit long random number *rand*, and computes the hash value of *x* , *rand*, and *attach request*, i.e. hash(*x*, *rand*, *attach request*), where *n* is determined by the resource usage degree in SEAF, the higher degree the resource is used, the larger the value of *n* is. Hash(*x, rand, attach request*), *rand*, and *n* are denoted as *hash challenge*.

2a.Upon receipt of *Identity request* message, if *hash challenge* is present, UE will first attempt to find the correct integer *x`* by using exhaustive search within the length of *n.* If hash (*x`,rand, attach request*) is equivalent to hash(*x, rand, attach request*) then the correct integer *x`* is obtained , and set *x`* as the *hash response*. UE generates the Diffie-Hellman (DH) private key KU_{pri}, and computes the corresponding DH public key KU_{pub}.

3. UE responds SEAF with its DH public key KU_{pub} and optionally with *hash response*.

3a. After receiving the response from the UE, if the *hash response* is included in the message, SEAF compares it with *x*. SEAF will abort the attach procedure if the *hash response* is not equal to *x*. Otherwise, SEAF generates the DH private key KC_{pri}, and calculates the associated DH public key KC_{pub}. Furthermore, SEAF derives the shared key K_{DH} between itself and UE by using its private key KC_{priv} and UE's public key KU_{pub}.

4. Like a usual DH key exchange, SEAF sends its public key KC_{pub} to UE.

4a. After receiving KC_{pub}, UE derives the shared key K_{DH} between itself and SEAF by using its private key KU_{priv} and SEAF`s public key KC_{pub}. To encrypt its identity, UE generates a nonce, and derives the encryption key K_E and integrity key K_M as follows:

K_E=KDF(nonce, K_{DH}, 1);

K_M=KDF(nonce, K_{DH}, 2);

where KDF is the key derivation function.

5. UE delivers the nonce, the identity encrypted with K_E , and message authentication code MAC0 which is computed over the message by using K_M, to SEAF.

In the same way as UE, SEAF derives the encryption key K_E and integrity key K_M. It first verifies MAC0, if the verification is successful, then it decrypts the encrypted part of the message with K_E to get the real identity of UE. Otherwise, it terminates the attach procedure.

6. SEAF forwards the UE`s identity to AUSF/ARPF in the *Authentication data request* message.

7. ARPF looks up the UE`s root key according to UE`s identity, and AUSF calculates the *Authentication vector* based on the root key K. Then AUSF sends the *Authentication vecto*r to SEAF.

8. Like in LTE, UE and SEAF perform mutual authentication, and acquire the intermediate key K_{mid} which is similar to the key K_{asme} in LTE. Both compute the session key Ks as follows:

Ks=KDF(K_{DH}, K_{mid})

9. SEAF sends the *Security mode command* message to UE, whose message authentication code MAC1 is computed by using the session key Ks.

10. UE verifies the received MAC1 by using the session key Ks. If the verification fails, UE terminates the attach procedure. Otherwise, UE responds to SEAF with the *Security mode complete* message, whose message authentication code MAC2 is computed by using the session key Ks. After receiving the *Security mode complete* message, SEAF checks the correctness of MAC2. If the check fails, SEAF aborts the attach procedure. Otherwise, UE and SEAF complete the attach procedure.

Lenovo Ex. 1007
Page 358

UE and SEAF can assure that they possess the same session key Ks after successfully verifying MAC1 and MAC2, respectively. This further implies that they have agreed upon the same key K_{DH}. Finally the key K_{DH} is stored in UE and SEAF, respectively, in order to be used for generating the new session key in the next attach procedure.

The session key Ks is viewed as the key anchor, which is used to derive other keys for confidentiality and integrity protection. For efficiency, the Diffie-Hellman (DH) key exchange protocol used in the procedure can be replaced with Elliptic Curve Diffie-Hellman key exchange protocol.

5.7.4.9.3 Evaluation

The proposed scheme is evaluated from the following perspectives:

5.7.4.9.3.1 Security

(1) DoS attacks

The proposed scheme mitigates DoS attacks by embedding the hash challenge/response mechanism in the identity acquisition stage. This mechanism forces attackers to spend more computation resource than SEAF if the network is under DoS attacks. As a result, SEAF will execute asymmetric cryptographic computation only in the case that it is free of DoS attacks. Other mechanisms, such as back-off timer, could be used for anti DoS attacks. However, effectiveness to mitigate DoS attacks is different compared to the proposed scheme. A malicious UE may comply with a back-off timer as long as it's baseband processor is unaffected. In case the baseband processor is infected, the UE will most likely not comply with the back-off timer rule, and overwhelms the SEAF using *attach request messages* without stop so that a lot of these messages will be treated as valid ones sooner or later by the SEAF. This will cause a high load on the SEAF which has to carry out the Diffie-Hellman computation and on the AUSF/ARPF which has to fetch AVs for valid IMSIs. This solution protects the AUSF/ARPF by requiring the UEs to provide a proof of work that is verified by the SEAF before forwarding the attach request to the AUSF/ARPF. This same mechanism also prevents that the SEAF has to carry out the high load computation unless the UE provides a correct proof of work.

The 'cost' of this solution is that genuine UEs have to carry out a number of hash operations when the network is under attack.

(2) Privacy of subscriber identifiers

The proposed scheme can prevent passive attackers from acquiring subscriber identifiers as they are encrypted with the encryption key K_E. However, it cannot defend against active attacker who acts as a base station to induce UE to disclose its identifier, because at the identity acquisition stage UE has not known whether the base station is authentic.

(3) Long-time secret leakage

The proposed scheme prevents passive attacker from getting the session key Ks even if the long-time secret is known to them. This is because the generation of session Ks depends on not only the intermediate key K_{mid} that is derived from the long-time secret, but also the shared key K_{DH}. The passive attacker cannot derive the session key without knowing K_{DH}.

(4) Insecurity of links between MNOs

A passive attacker cannot acquire the session Ks even if it has known the authentication vector by eavesdropping the communication at links between MNOs. Analog to the long-time leakage, the passive attacker is unable to get the session key Ks due to the lack of knowledge of K_{DH}.

In a nutshell, the proposed scheme can defend against passive attacks but not active ones.

5.7.4.9.3.2 Complexity

The proposed scheme is comparatively simple as its operation does not need a PKI. On the other hand, its simplicity makes it subject to active attacks.

5.7.4.9.3.3 Compatibility

The proposed scheme is highly backward compatible with the LTE EPS system because it does not touch the LTE AKA protocol. Moreover the mature identity management system in LTE (IMSI-GUTI mapping) can still be used in the 5G

Lenovo Ex. 1007
Page 359

system because the proposed scheme keeps the identity management unchanged , and enhances it by concealing the real identity of UE at the initial attach procedure.

5.7.4.9.3.4 Efficiency

The proposed scheme is efficient in the context of the reuse of shared key K_{DH} between UE and the SEAF. A UE can generate the session key Ks by reusing K_{DH} when attaching the network again as long as there is no synchronization problem between IMSI and GUTI. The can significantly reduce the computation cost rising from the DH computation.

5.7.4.10 Solution #7.10: Applying DHIES to the attach procedure

5.7.4.10.1 Introduction

The proposed scheme is to address the key issue #7.2 Concealing permanent or long-term subscription identifier, and it also relates to the key issue 3.1 Interception of radio interface keys sent between operator entities.
DHIES (Diffie-Hellman Integrated Encryption Scheme) is an enhanced ElGmal encryption scheme[4]. It integrates different functions into one scheme for message encryption, including public key operation, encryption algorithm, message authentication algorithm, and KDF (Key Derivation Function). It works as follows. To send an encrypted message to a recipient, the sender first generates its DH private key and computes its ephemeral DH public key. Then it fetches the authentic DH public key of the recipient, and derives the shared key between itself and the recipient using its private key and receipt's public key. Appling the shared key to KDF, the sender obtains the encryption key and integrity key used for assuring the confidentiality and integrity of the message, respectively. The resulting ciphertext comprises the ephemeral DH public key of the sender, the symmetrically encrypted message, and message authentication code (MAC). The ECC variant of DHIES is called ECIES(Elliptic Curve Integrated Encryption Scheme), which has been specified in several standards, such as ANSI X9.63 standard [5], IEEE 1363a [6], and ISO/IEC 18033-2 standard [7].

We propose to apply DHIES to the attach procedure in order to eliminate three security threats: privacy of subscriber identifies, long-term secret key leakage, insecurity of links between MNOs. The basic idea is that DHIES is integrated into the identity acquisition stage of the attach procedure. The authenticity of DH public key of the network is assured in a way that it is contained in a certificate. UE validates the certificate with the help of a PKI before computing the shared key K_{DH} using the DH public key of the network. The management of the PKI refers to 5.4.4.1 of TR 33.899. The real identity of a UE is encrypted by using DHIES so that an attacker (even active) is unable to catch it. At the end of the AKA protocol, UE and the network generate the same key K_{mid} on the basis of the shared root key. Then UE and the network compute the session key Ks using the key K_{mid} and the key K_{DH}. In the SMC stage, the MAC values of the message security mode command and the message security mode response are calculated with the session key Ks in order to confirm the correctness of the key Ks. The proposed scheme can also alleviate the possible DoS attacks in the attach procedure by embedding anti-DOS attacks measure in the protocol.

5.7.4.10.2 Solution details

Three authentication-related functions are involved in the attach procedure, which are:

- Authentication Credential Repository and Processing Function (ARPF)
- Authentication Server Function (AUSF)
- Security Anchor Function (SEAF)

The proposed attach procedure is depicted in Figure 5.7.4.10.2-1, where the term "UE" instead of "NG-UE" is still used for simplicity.

Lenovo Ex. 1007
Page 360

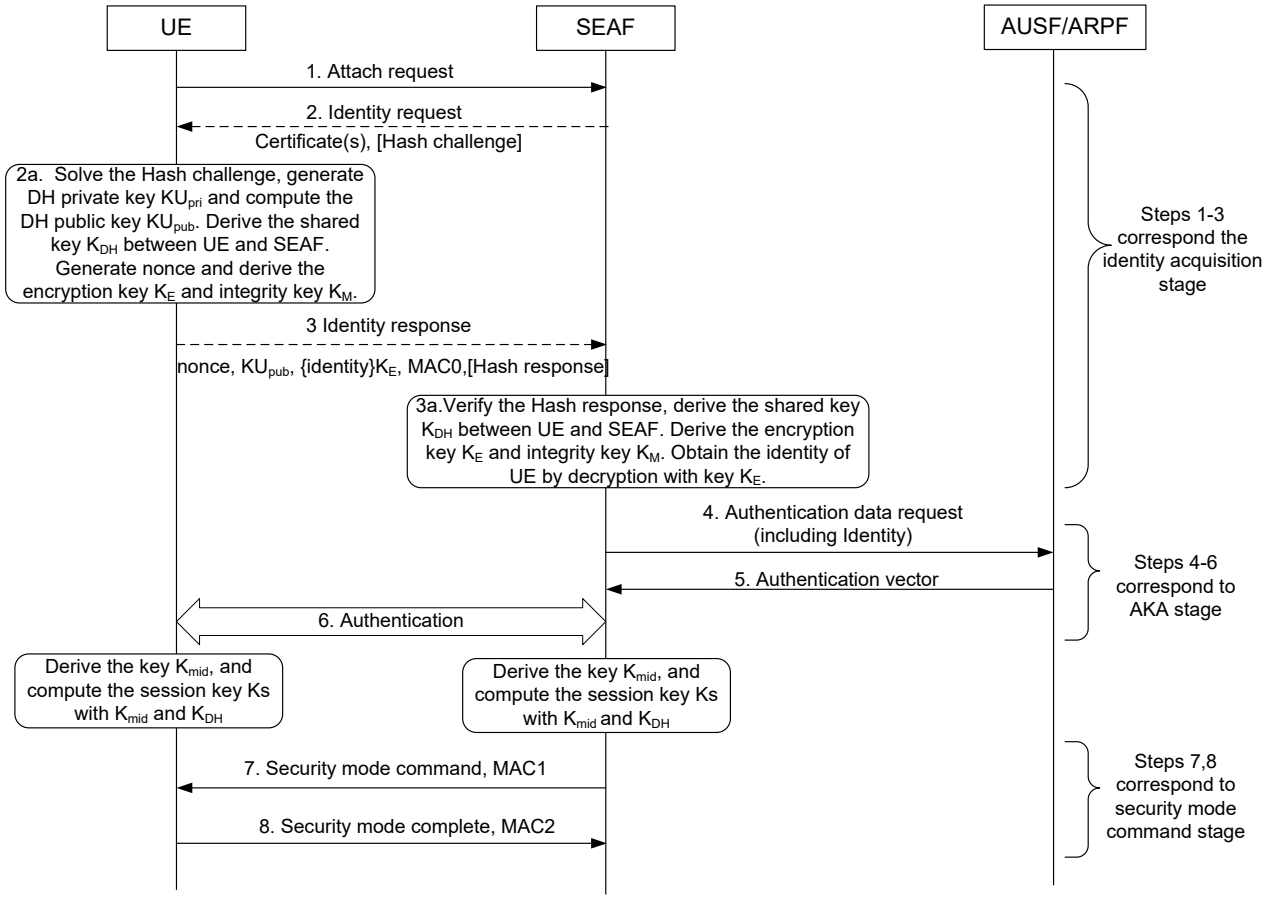


Figure 5.7.4.10.2-1: The proposed attach procedure

Editor's note: It is ffs whether the SEAF sends only its certificate or its certificate along with the network's certificate to UE.

The proposed attach procedure is illustrated as follows:

1. UE initiates the attach procedure, and sends an *Attach request* to the SEAF, including the temporary identity like GUTI used in LTE if available.

2. After receiving the *Attach request*, if the temporary identity is in the *Attach request* message, SEAF checks whether there exists a real identity corresponding to the temporary identity and whether SEAF has established a shared DH key K_{DH} with the UE, SEAF will go into step 4 in the case that both conditions are met. Otherwise, SEAF sends *Identity request* message back to the UE, which contains the certificate of SEAF, and optionally includes the hash challenge to thwart DoS attacks. The DH public key of SEAF is encapsulated in the certificate. The *Identity request* message is also returned to UE by SEAF if no temporary identity GUTI is contained in *Attach request* message.

If the SEAF has justified that it is under DoS attacks, it will embed the *hash challenge* into the *Identity request* message. It is constructed as follows. The SEAF randomly generates a positive integer *x* that is *n* bit length in binary, a 128-bit long random number *rand*, and computes the hash value of *x,rand,* and *attach request*, i.e. hash(*x*, *rand*, *attach request*), where *n* is determined by the resource usage degree in SEAF, the higher degree the resource is used, the larger the value of *n* is. Hash(*x, rand, attach request*), *rand,* and *n* are denoted as *hash challenge*.

2a. Upon receipt of *Identity request* message, if *hash challenge* is present, UE will first attempt to find the correct integer *x`* by using exhaustive search within the length of *n*. If hash (*x`,rand, attach request*) is equivalent to hash(*x, rand, attach request*) then the correct integer *x`* is obtained , and set *x`* as the *hash response*. UE validates the received certificate with the help of a PKI, and retrieves the DH public key KC_{pub} of SEAF from the certificate. UE generates the Diffie-Hellman (DH) private key KU_{pri}, and computes the corresponding DH public key KU_{pub}. UE derives the shared key K_{DH} between it and SEAF by using its private key KU_{priv} and the public key KC_{pub} of SEAF.

Lenovo Ex. 1007
Page 361

3. To encrypt its identity, UE generates a nonce, and derives the encryption key K_E and integrity key K_M. Then UE sends the *Identity response* message to SEAF, which consists of nonce, the DH public key KU_{pub} of UE, the identity encrypted with K_E, message authentication code MAC0 which is computed over the aforementioned message parts by using K_M, and optionally *hash response* to SEAF. K_E and K_M are calculated as follows:

K_E=KDF(nonce, K_{DH}, 1);

K_M=KDF(nonce, K_{DH}, 2);

where KDF is the key derivation function.

3a. After receiving the *Identity response* from the UE, if the *hash response* is included in the message, SEAF compares it with *x*. SEAF will abort the attach procedure if the *hash response* is not equal to *x*. Otherwise, SEAF derives the shared key K_{DH} between itself and UE by using its private key KC_{priv} and UE's public key KU_{pub}, and computes the encryption key K_E and integrity key K_M in the same way as UE . After that SEAF verifies MAC0, if the verification is successful, it decrypts the encrypted part of the message with K_E to get the real identity of UE. Otherwise, it terminates the attach procedure.

4. SEAF forwards the UE`s identity to AUSF/ ARPF in the *Authentication data request* message.

5. ARPF looks up the UE`s root key according to UE`s identity, and AUSF calculates the *Authentication vector* based on the root key K. Then AUSF sends the *Authentication vecto*r to SEAF.

6. Like in LTE, UE and SEAF perform mutual authentication, and acquire intermediate key K_{mid} which is similar to the key K_{asme} in LTE. Both compute the session key Ks as follows:

Ks=KDF(K_{DH}, K_{mid})

7. SEAF sends the *Security mode command* message to UE, whose message authentication code MAC1 is computed by using the session key Ks.

8. UE verifies the received MAC1 by using the session key Ks. If the verification fails, UE terminates the attach procedure. Otherwise, UE responds to SEAF with the *Security mode complete* message, whose message authentication code MAC2 is computed by using the session key Ks. After receiving the *Security mode complete* message, SEAF checks the correctness of MAC2. If the check fails, SEAF aborts the attach procedure. Otherwise, UE and SEAF complete the attach procedure.

UE and SEAF can assure that they possess the same session key Ks after successfully verifying MAC1 and MAC2, respectively. This further implies that they have agreed upon the same key K_{DH}. Finally the key K_{DH} is stored in UE and SEAF, respectively, in order to be used for generating the new session key in the next attach procedure.

The session key Ks is viewed as the key anchor, which is used to derive other keys for confidentiality and integrity protection. For efficiency, DHIES used in the procedure can be replaced with ECIES.

5.7.4.10.3 Evaluation

The proposed scheme is evaluated from the following perspectives:

Lenovo Ex. 1007
Page 362

5.7.4.10.3.1 Security

(1) Man-in-the-middle attacks

The proposed scheme prevents man-in-the-middle attacks by introducing the double authentication mechanism: one is DHIES in the identity manage stage, the other one is AKA process in the AKA stage. DHIES is actually one way authentication scheme in the sense that only the dedicated SEAF with the associated private key can decrypt the messages. This implies the SEAF authenticates itself to UE by using its private key. The authenticity of DH public key of SEAF is assured by a PKI. As a result, before performing man-in-the-middle attacks to acquire the session key Ks, an adversary has to carry out the following attacks: cracking SEAF to acquire the private key of SEAF, cracking PKI to forge the certificate of SEAF, and stealing the root key used in the AKA protocol. Even though the root key is leaked, it is still impossible for an attacker to get the session key Ks because of the high security level of PKI and SEAF.

(2) DoS attacks

The proposed scheme mitigates DoS attacks by embedding the hash challenge/response mechanism in the identity acquisition stage. This mechanism forces attackers to spend more computation resource than SEAF if the network is under DoS attacks. As a result, SEAF will execute asymmetric cryptographic computation only in the case that it is free of DoS attacks. Other mechanisms, such as back-off timer, could be used for anti DoS attacks. However, effectiveness to mitigate DoS attacks is different compared to the proposed scheme. A malicious UE may comply with a back-off timer as long as it's baseband processor is unaffected. In case the baseband processor is infected, the UE will most likely not comply with the back-off timer rule, and overwhelms SEAF using attach request messages without stop so that a lot of these messages will be treated as valid ones sooner or later by SEAF. This will cause a high load on the SEAF which has to carry out the Diffie-Hellman computation and on the AUSF/ARPF which has to fetch AVs for valid IMSIs. This solution protects the AUSF/ARPF by requiring the UEs to provide a proof of work that is verified by the SEAF before forwarding the attach request to the AUSF/ARPF. This same mechanism also prevents that the SEAF has to carry out the high load computation unless the UE provides a correct proof of work.

The 'cost' of this solution is that the genuine UEs have to carry out a number of hash operation when the network is under attack.

(3) Privacy of subscriber identifiers

The proposed scheme can prevent attackers from acquiring subscriber identifiers no matter the attack is active or passive, because subscriber identifiers are encrypted with the encryption key K_E. There is no way for an adversary to get the encryption key K_E because this requires it to break either PKI or SEAF.

(4) Long-time secret leakage

The proposed scheme prevents passive attacker and active attacker from getting the session key Ks even if the long-time secret is known to them. This is because the generation of session Ks depends on not only the intermediate key K_{mid} that is derived from the long-time secret, but also the shared key K_{DH}. The attacker cannot derive the session key Ks because it is unable to deduce the key K_{DH} unless it can crack the PKI or SEAF.

(5) Insecurity of links between MNOs

An attacker cannot acquire the session Ks even if it has known the authentication vector by eavesdropping the communication at links between MNOs or injected a forged authentication vector into the SEAF. Analog to the long-time leakage, the attacker is unable to get the session key Ks due to the lack of knowledge of K_{DH}.

5.7.4.10.3.2 Complexity

The proposed scheme itself is comparatively simple. Its complexity mainly comes from the operation because a PKI is required when it is deployed.

5.7.4.10.3.3 Compatibility

The proposed scheme is highly backward compatible with the LTE EPS system because it does not touch the LTE AKA protocol. Moreover the mature identity management system in LTE (IMSI-GUTI mapping) can still be used in the 5G system because the proposed scheme keeps the identity management unchanged , and enhances it by concealing the real identity of UE at the initial attach procedure.

Lenovo Ex. 1007
Page 363

5.7.4.10.3.4 Efficiency

The proposed scheme is efficient in the context of the reuse of shared key K_{DH} between UE and the SEAF. A UE can generate the session key Ks by reusing K_{DH} when attaching the network again as long as there is no synchronization problem between IMSI and GUTI. The can significantly reduce the computation cost rising from the DH computation.

Editor's note: Whether DH is needed for generate the session key in case PKI is already introduced is FFS.

5.7.4.11 Solution #7.11: Protect the Permanent or Long Term User Identity with Public Key Technologies

5.7.4.11.1 Introduction

This solution addresses key issue #7.2 and #7.3.

As described in the above key issues, both permanent subscriber ideneitifiers such as IMSI and the device identifiers such as IMEI shall be protected. In key issue #7.2, it mentioned that MME must know the IMSI as required by the LI. However, it also mentioned that the protection of permanent or long term subscriber shall at least be as strong as provided in the legacy system such as UMTS and LTE. Therefore, in this contribution, we provie two solutions with public key technologies as follows:

- Solution A: protect the permanent or long term identifiers with a termination point at AN
- Solution B: protect the permanent or long term identifiers with a termination point at core network function, e.g.AUSF/SEAF.

5.7.4.11.2 Solution details

As we know, in the UMTS or LTE system, the permanent or long term identity are transmitted in signalling such as attachment request or identity response. These signallings are transmitted without protection because no session keys are generated at this stage. Therefore, it is impractical to use symmetric key to proect these signallings. Public key is one of the most suitable chocies.

There are two types of public technologies, PKI based public key and Idenity based public key. In solution #7.2, PKI based public key is proposed for identifier protection. Therefore, in this solution, we focus on the solution with Identity-based public key. For the Identity-based encryption technology, we propose to use the method specified in RFC 6508 [1].

To use the Identity-based technology for data encryption according to RFC 6508 [63], the receiver need to be provisioned with a Receiver Secret Key(RSK), denoted as K_(ID, T), which is generated by the Key Management Service (KMS), where ID is the identity of receiver, and T is used to denote the KMS server KSM_T. The entity perfoming encryption need to be provisioned with a KMS public key for encryption, denoted as Z_T. A node can encrypt message with receiver's ID and Z_T. The receiver can decrypt the encrypted message with its RSK, K_(ID, T).

In the follow, we assume that the funcation of KMS is included in the credential repository.

5.7.4.11.2.1 Protect the Permanent or Long Term Identifiers with a termination point at AN

In this solution, we aussme that protection of the identifier is terminated at the Access Network. The procedures are separated into three stages. In the first stage, RAN is provisioned with Identity-based credentials and parameters. In the second stage, UE is provisioned with ID-based parameters. In the third stage, UE use the Identity-based encryption method to encrypt the NAS signalling and RAN uses follows:

1. Credential Repository provision credentials to RAN

   1.1 RAN receives Identity based public/private key pairs from credential repository, including BS_ID, which is the Identity-based public key for encryption, K_(BS_ID, T), which is private key for decryption, and also a global parameters, Z_T, for encryption.

   1.2 RAN stores the BS_ID, K_(BS_ID, T), and Z_T in its storage.

2. Credential repository provisioning KMS parameters to UE. Note, the KMS here belongs to an operator and different operators may have different KMS and thus may have different key generation parameters.

Lenovo Ex. 1007
Page 364

2.1 UE is provisioned with Z_T from KMS

2.2 UE stores the Z_T in its storage.

3. UE using the BS_ID to protect the NAS signalling

3.1 RAN broadcast BS-ID over the air interface

3.2 UE store the BS-ID in its storage

3.3 When UE receive NAS signalling from upper layer, it finds the Z_T and BS_ID first, and then encrypt the message with BS_ID and Z_T.

3.4 UE transmitted the encrypted message to the RAN.

3.5 RAN find the Z_T and Receiver Secret Key, K_(BS_ID, T), according to BS_ID, and then decrpt the NAS signalling with Z_T and, K_(BS_ID, T).

3.6 RAN forwards the NAS signalling to the core network.

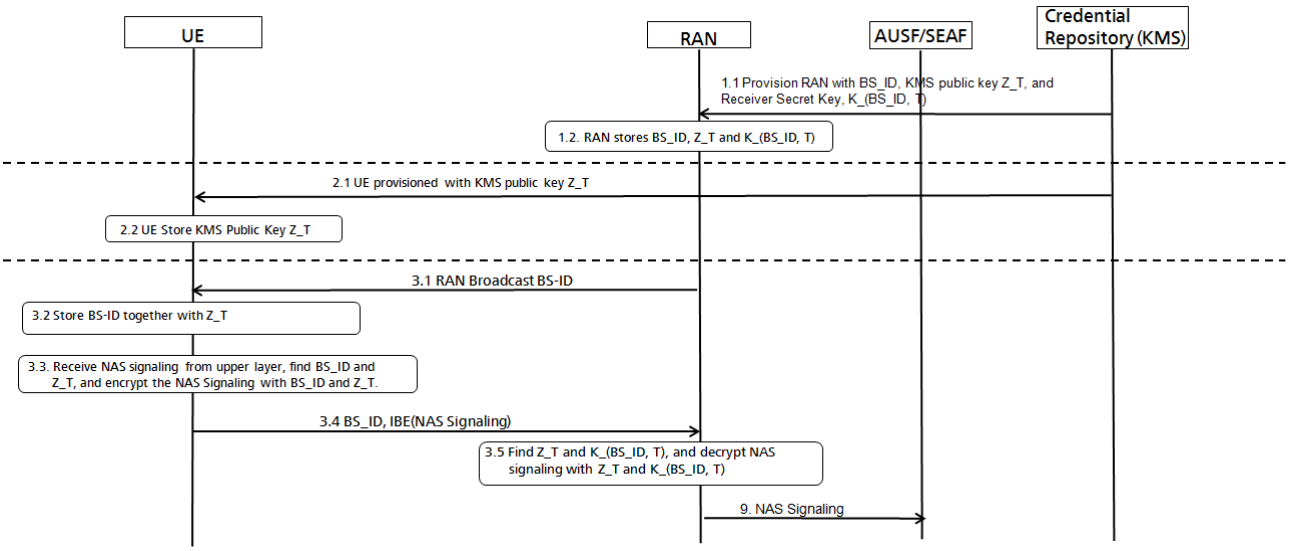


Figure 5.7.4.11.2.1-1: Protect the Permanent or Long Term Identifiers with a termination point at AN

For roaming cases, the credential repository of home operator may provision a UE with the roaming operator's KMS public key and other parameters before roaming to the visited networks.

Editor's note: The roaming case needs to be described more. E.g. how can a home operator know which network the user will roam to.

5.7.4.11.2.2 Protect the Permanent or Long Term Identifiers with a termination point at Core Network

In this solution, we aussme that protection of the identifier is terminated at the core network, e.g. AUSF/SEAF. The differences are that the Credential Repository provisions the Identity-based ID, eNAS_ID, KMS public key, Z_T, and Receiver Secret Key, K_(eNAS_ID, T). For different AUSF/SEAF, the eNAS_ID can be different, and one AUSF/SEAF can be provisioned with multiple eNAS_ID.

The procedures are as follows:

1. Credential Repository provision credentials to AUSF

1.1 AUSF/SEAF receives Identity based public/private key pairs from KMS, including eNAS_ID, which is the Identity-based public key for encryption, K_(eNAS_ID, T), which is private key for decryption, and also a KMS public key, Z_T.

1.2 AUSF/SEAF stores the eNAS_ID, Z_T, and K_(eNAS_ID, T), in its storage.

Lenovo Ex. 1007
Page 365

2. Credential repository provisioning KMS parameters to UE. Note, the KMS here belongs to an operator and different operators may have different KMS and thus may have different key generation parameters.

   The procedures are the same as step 2.1 – 2.2 in solution 1.

3. AUSF/SEAF sends eNAS_ID to RAN

   3.1 AUSF/SEAF selects an eNAS_ID and sends it to RAN.

   3.2 RAN stores eNAS_ID.

4. UE encrypt NAS signalling with eNAS_ID.

   4.1 RAN broadcast the eNAS_ID over the air interface.

   4.2 UE receives the eNAS_ID and stores in it in its storage.

   4.3 When UE receive NAS signalling from upper layer, it finds the Z_T and eNAS_ID first, and then encrypt the message with eNAS_ID and Z_T.

   4.4 UE transmitted the encrypted message to the RAN.

   4.5 RAN forwards the encrypted NAS signalling to the core network

   4.6 AUSF/SEAF decrpts the NAS signalling with Z_T and K_(eNAS_ID, T).

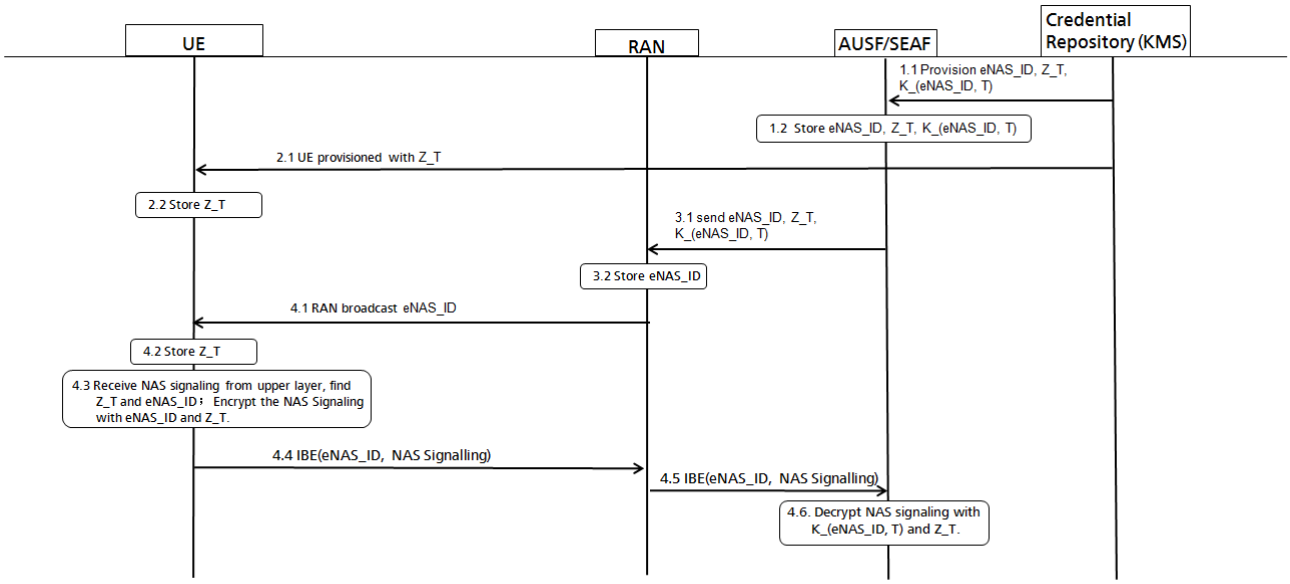


Figure 5.7.4.11.2.2-1: Protect the Permanent or Long Term Identifiers with a termination point at Core Network

5.7.4.11.3 Evaluation

Tba.

5.7.4.12 Solution #7.12: Mechanisms of Pseudo-IMSI for hiding long-term identifier

5.7.4.12.1 Introduction

Solutions 7.3 and 7.4 describe the usage of pseudonyms to conceal the subscriber's long-term identifier. Pseudonyms are calculated by UE and HSS. The solution described in this clause provides an alternative to parts of these solutions. Thus, this solution addresses also key issue #7.2 on concealing permanent subscriber identifiers.

Lenovo Ex. 1007
Page 366

5.7.4.12.2 Solution details

Editor's note: Solution terminology alignment with the common NextGen terminology is FFS.

5.7.4.12.2.1 Introduction of Pseudo-IMSI (P-IMSI) by replacing MSIN-part by Mobile Station PseudoNym (MSPN)

The home PLMN and UE generate a new pseudonym that follows a standard IMSI format, in which the MCC and MNC are defined as usual, and the MSIN is replaced by the value specially generated by using a common function.

This value, called the Mobile Station PseudoNym (MSPN), is used in place of MSIN outside the USIM and HSS domain. That is, both USIM and HSS derive the MSPN, and when the session is being established, the Pseudo-IMSI for the session is constructed using MCC, MNC, and MSPN.

NOTE: At manufacturer time, an initial P-IMSI is provisioned to the UE and stored at the HSS. It is used for first contact to the system and will not be used anymore after UE has received its first authentication challenge. Further an association constant $MSPN_{ASSOC}$ is provided to UE and HSS, such that HSS can link pseudonyms. See below for details.

The Pseudo-IMSI (P-IMSI) is informative enough for the MME to discover the HSS, as it contains real MCC and MNC of the IMSI. It is sufficient to locate the subscription record in the HSS as HSS knows how to map the MSPN to the MSIN, and therefore identify the real IMSI, assemble authentication vector, for authentication, and provide session specific policies to the EPC. It can also be mapped to the Chargeable User Identity at the trusted interface between the EPC and Billing Domain.

The MSPN in P-IMSI is not semantically different from the MSIN in IMSI. Once the MSPN is computed, it is retained by the USIM and the HSS, in association with the MCC and MNC, as the P-IMSI – the semi-permanent identity associated with the IMSI. In the USIM, it is overwritten with a new computed value with every authentication procedure. If the network queries the mobile for its permanent identifier (IMSI), the current cached P-IMSI is reported by the USIM instead of IMSI. Only HSS would be able to map the P-IMSI to the real IMSI of the subscription.

The following computation of MSPN is proposed:

$$MSPN = Truncate\{Convert_{Binary\text{-}to\text{-}Decimal}[f_p(MSPN_{ASSOC}, RAND, K)]\}$$

Where:

- K is the long-term secret key shared between the USIM and the AuC;
- $MSPN_{ASSOC}$ is the fixed MSPN value associated with the MSIN in the subscription database. In computation it is used as the association constant.
- RAND is the random challenge selected for the Authentication Vector,
- f_p is the KDF defined for this process,
- $Convert_{Binary\text{-}to\text{-}Decimal}$ is the process of converting the result of computation to the Decimal representation, and
- Truncate is a process that truncates the converted decimal result to the required 9 or 10 digits of expected MSPN number.

5.7.4.12.2.2 NextGen signalling support for P-IMSI

The HSS has to clearly recognize that the P-IMSI is sent to it by the Serving System, and not the IMSI reported by a legacy USIM. This has to be recognized before the subscription record is accessed, because the HSS cannot know in advance of the P-IMSI capabilities of the USIM in the mobile that accessed the serving system.

This can be, for example, achieved by allocating a specific combination of MCC and MNC to all subscriptions that are capable of, and are expected to operate using MSPN, e.g. specific MNCs per country. This is possible because allocation of a particular MNC for the Operational deployment purpose is a decision of the Operator. From the operational point of view, the combination of the MCC and MNC represents a specific HSS instance that is recognized by the Serving System.

Lenovo Ex. 1007
Page 367

Alternatively, a special signalling indication may be defined in NextGen that allows the HSS to recognize that MSPN has been reported by the USIM instead of the MSIN. This proposal does not recommend such solution, as it may require signalling support at multiple involved network entities instead of affecting only USIM and HSS.

5.7.4.12.2.3 Collision prevention

While computing the MSPN, the HSS has to ensure that the computed number does not collide with any other currently valid MSPN computed for another IMSI by the same HSS with the same MCC|MNC combination. Note that collision with any real IMSI is already avoided by default, if a specially allocated MCC|MNC combination is used for the HSS handling this MSPN. Otherwise care shall be taken to avoid collision with any other real IMSI. I.e. if collision is discovered, the HSS has to select another RAND and re-compute the authentication vector and the MSPN until the collision is avoided.

5.7.4.12.2.4 Retention of computed MSPN values

Even though in LTE the HSS is recommended to return only one AV to the MME at the time to reduce the possibility of AV mis-synchronizations, the HSS is never informed whether or not the AV is used by the MME, and therefore, the HSS does not know which RAND of the delivered AV was used by the USIM in computing the MSPN when the UE was requested to report its permanent identifier. Therefore, some computed MSPNs may never be used, while others could be used out of expected order by the MME to identify the request for authentication vector.

NOTE: One MSPN may also be used multiple times, because UE may access the network with GUTI which will be resolved by the MME to the same P-IMSI value without asking the USIM for its permanent identifier. I.e. Meanwhile, a newly received AKA Challenge will cause creation of a new MSPN in the USIM which will replace the previous value. Therefore, even though the USIM should retain only one MSPN value computed for the next request for P-IMSI, the HSS may need to retain several.

5.7.4.12.2.5 Description of the HSS process steps

Figure 5.7.4.12.2.5-1 shows process steps executed at the HSS when the authentication vector is requested by the serving system:

1. HSS received the Authentication Information Request from the MME containing the P-IMSI as the identity of the UE. HSS obtains the $MSPN_N$ from the received P-IMSI.

2. HSS checks the local MSPN cache for matching $MSPN_N$ value. If match is not found, proceed to step 8. Otherwise, proceed to step 3.

3. HSS locates the IMSI associated with the $MSPN_N$ and accesses the subscription record for this IMSI.

   a. Provided that subscription policy allows to return the Authentication Vector, the HSS selects the RAND and computes the next value of the $MSPN_{N+1}$.

4. The HSS checks if the computed value of $MSPN_{NEXT}$ collides with any currently stored values in MSPN cache. If collision is discovered, return to step 3.a to select another value of RAND. If there is no collision with any currently stored MSPN values in a cache, proceed to step 5, 6, and 7.

5. Use selected RAND to create and return the Authentication Vector.

6. HSS marks the received $MSPN_N$ as Current $MSPN_{CURR}$, and deletes from the cache the value of MSPN that was previously marked as Current for this subscription record (associated with IMSI). There can be one and only one $MSPN_{CURR}$ per associated IMSI. Note, that there could be multiple unrelated requests to the HSS using the same $MSPN_{CURR}$, until another $MSPN_N$ is received that is resolved to the same IMSI. At that point HSS gets the indication that the $MSPN_{CURR}$ is no longer used, and can be replaced with the received $MSPN_N$.

7. The newly computed $MSPN_{N+1}$ is added to the pending cache in association with related IMSI.

8. This step is executed when HSS cannot find in its cache the MSPN associated with any IMSI. Conventionally, the 3GPP 29.272 describes the Diameter Error #8 "DIAMETER_ERROR_USER_UNKNOWN". Handling of this Error by the UE and the USIM configured to support the P-IMSI is described in the section below.

Lenovo Ex. 1007
Page 368

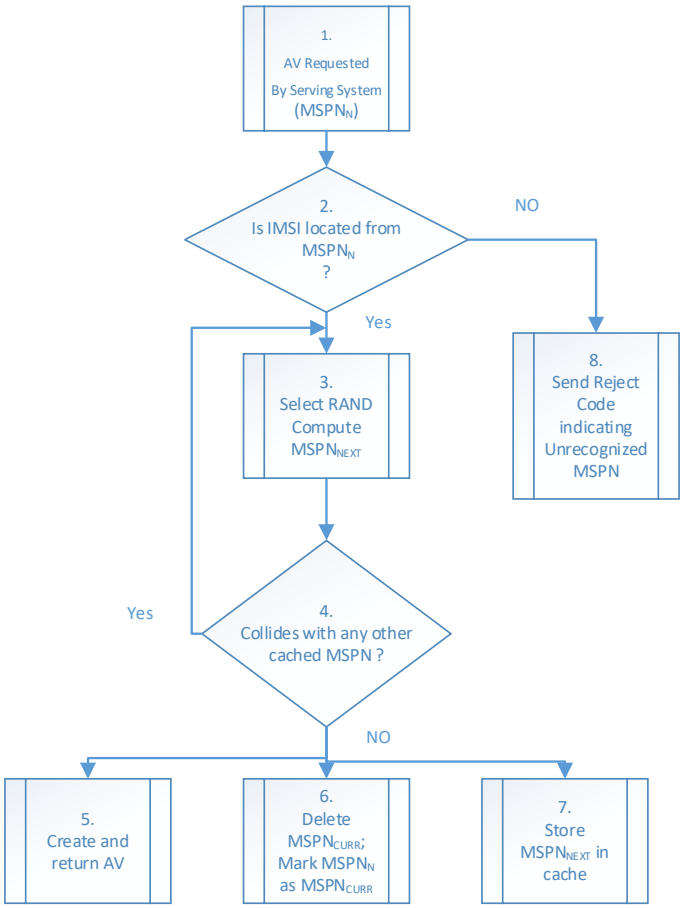


Figure 5.7.4.12.2.5-1 HSS process steps

5.7.4.12.2.6 Description of the USIM Process Steps

Figure 5.4.7.12.2.6-1 outlines the process at the USIM when authentication challenge is received.

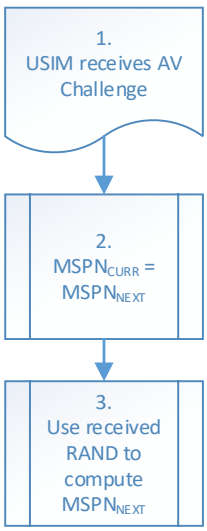


Figure 5.4.7.12.2.6-1: USIM process steps

1. USIM received the AKA Challenge to be authenticated.

2. This is an indication that that identity (P-IMSI with MSPN$_N$) reported by the USIM was recognized by the HSS, and it becomes the MSPN$_{CURR}$, in other words, known and used by the serving system for mapping GUTI and locating the HSS, and also known by the HSS to locate the permanent subscription record.

Lenovo Ex. 1007
Page 369

3. The RAND received in the AKA Challenge is used to compute and store the $MSPN_{NEXT}$ for the future access when ME requests the permanent identity from the USIM. In this step the previously stored $MSPN_{NEXT}$ gets overwritten with the newly computed value based on the received RAND. This value may be overwritten with yet another value when next RAND is received, and may never be reported to the UE, unless the request for permanent identity is received. At that time it is sent to the UE, and if, in response, the valid authentication challenge is received, the USIM will mark it as $MSPN_{CURR}$ as in step 2.

When request for permanent identity is received from the ME, the following USIM processing of request of permanent identity is needed, as shown on Figure 5.4.7.12.2.6-2.

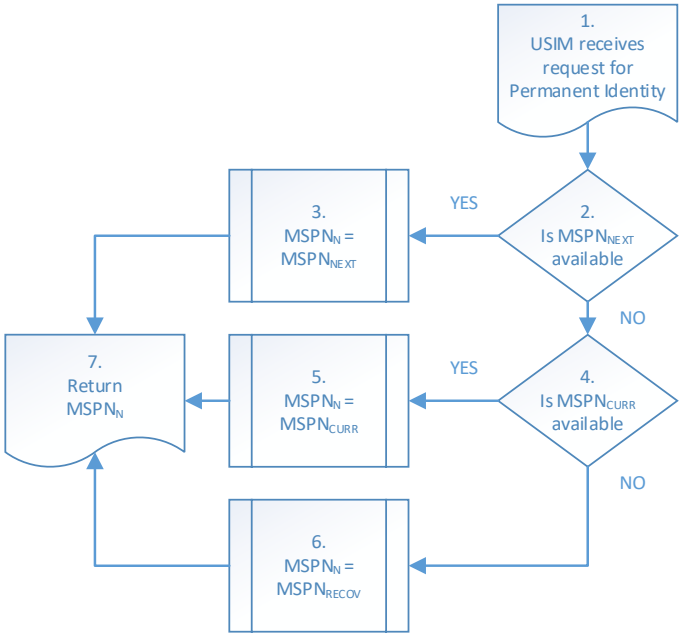


Figure 5.4.7.12.2.6-2: USIM process steps when Permanent Identity is requested

1. USIM receives the Request for permanent identity. This typically happens when Attach with GUTI cannot be resolved by the MME to an identity known to the HSS, or HSS does not recognize the reported identity.

2. If USIM has received an AKA Challenge in the past, which is an indication that HSS has successfully associated its $MSPN_{CURR}$ access with the subscription record (IMSI), then the $MSPN_{NEXT}$ was computed at that time and is available. Proceed to step 3. Otherwise, if there is no $MSPN_{NEXT}$ in the USIM, which means that the last identity ($MSPN_{CURR}$) used in accessing the network was not authenticated for any reason, and therefore was not changed, proceed to step 4.

3. USIM sets the returned identity $MSPN_N$ to the $MSPN_{NEXT}$. This value was computed during last access when HSS could successfully associate the reported identity with the IMSI, and therefore compute and return the AKA Authentication Vector.

4. USIM approaches this step only when the HSS cannot resolve the reported $MSPN_N = MSPN_{NEXT}$. In this case the HSS returns the Diameter Error which is propagated to the USIM and renders the $MSPN_{NEXT}$ invalid. This is a fall-back recovery procedure that uses the last known MSPN that was properly resolved by the HSS, because the AKA Challenge was received for it. Proceed to step 5.

5. USIM sets the returned identity $MSPN_N$ to the $MSPN_{CURR}$. This value was used during last access when HSS could successfully associate the reported identity with the IMSI. Proceed to step 7.

6. In case when neither access with $MSPN_{NEXT}$ not with $MSPN_{CURR}$ is successful and the HSS still returns an Error indicating that subscription cannot be found, a recovery may be initiated by UE. Proceed to step 7.

Editor's Note: Recovery procedure is ffs.

7. The $MSPN_N$ is returned to the ME as a part of the P-IMSI.

Lenovo Ex. 1007
Page 370

5.7.4.12.3 Evaluation

This solution does not rely on public key crypto, thus computational effort and message size can be kept low.

P-IMSI is computed from a root key (K), a randomizer RAND, and a constant $MSIN_{ASSOC}$. Semantically the procedure is different to solution #7.3 and #7.4, but the result has same math properties.

$MSPN_{NEXT}$ is computed from the K and $MSPN_{ASSOC}$ which are not known to the serving system. The RAND, of course, is known, but cannot allow the serving system to precompute the next MSPN. Therefore, concealment of next expected value from SN is given and correlation of pseudonym is not possible.

Implementation effort can be kept low. NAS message can be used without major changes. The solution uses a traditional size of the identity element, which is 15 decimal digits for the P-IMSI.

Confirmation of usage of the correct values in UE and HSS derived from RAND can be achieved implicitly, when next P-IMSI is received by HSS. UE and HSS do not need to synchronize explicitly.

5.7.4.13 Solution #7.13: Refreshing CN short-term subscriber identifiers

5.7.4.13.1 Introduction

This solution addresses the key issues #7.1 "Refreshing of temporary subscriber identifier" and #7.4 "Using effective temporary or short-term subscriber identifiers". The solution proposes potential ways to refresh the core network short-term subscriber identifiers (c.f. GUTI, S-TMSI in LTE) by building into the protocol design, the refreshment of core network short-term subscriber identifier. By doing so, the proposed solution aims at closing the doors for poor implementation or poor configuration, regarding the identifier refreshment, in the NextGen Core (NGC) and or the UE.

NOTE: The short-term subscriber identifiers used in the radio access network (c.f. C-RNTI in LTE) are not in the scope of this solution.

5.7.4.13.2 Solution details

5.7.4.13.2.1 General

It shall be mandatory to refresh the core network short-term subscriber identifier during or after certain NextGen NAS (NG-NAS) procedure(s) or NG-NAS message(s). In order not to introduce unnecessary signalling or computational overheads, only those NG-NAS procedure(s) or message(s) shall trigger the refreshment where the short-term identifier is actually used. Some examples of such procedure(s) or message(s) in terms of a current LTE system are attach procedure, tracking area updating procedure, service request procedure in response to the paging message, and paging procedure. An explicit procedure such as the one similar to a GUTI reallocation procedure, in a current LTE system, may also still be useful. The acknowledgement or confirmation of the identifier refreshment may be performed as a part of the triggering procedure, e.g. using message(s) such as ATTACH complete, TAU complete, or GUTI reallocation complete in terms of a current LTE system.

A UE, communicating with the network, might support both the legacy LTE and the NextGen system, i.e. both a LTE MME and a NGC function. Therefore, in order not to break the legacy mechanism, the UE performs the mandatory refreshment mechanism only with the NGC. Two variants of the solution are discussed as follows.

5.7.4.13.2.2 Solution Variant-A

The UE and the NGC each derive the next short-term identifier from common parameters known to the two parties, e.g., K_{ASME} in LTE and a parameter that changes for each derivation, such as the previous short-term identifier, or a random value chosen by the NGC. The derivation can be done using, e.g., the KDF. The generated short-term identifier will be used the next time the UE contacts NGC. In this way, neither implementations nor configurations can avoid the refreshment of short-term identifier, thereby enhancing the subscriber's privacy.

Figure 5.7.4.13.2-1 illustrates a high-level generalized data-flow of the variant-A.

Lenovo Ex. 1007
Page 371

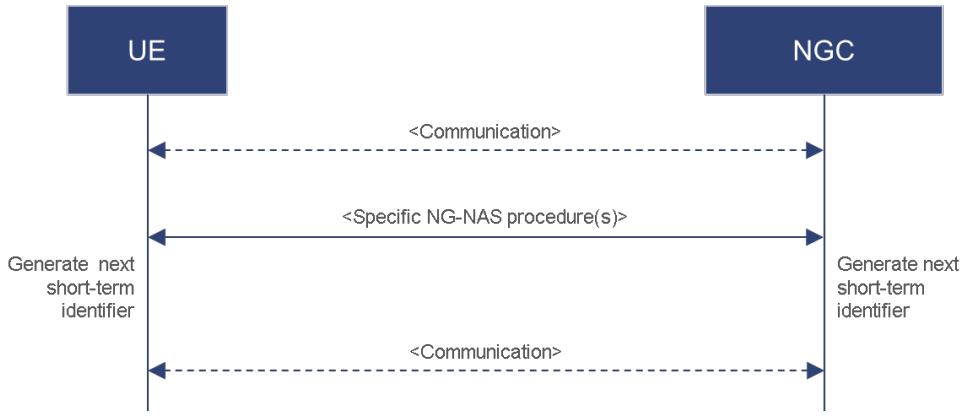


Figure 5.7.4.13.2-1: High-level data-flow of solution (variant-A)

The short-term subscriber identifier used in the NGC may have some defined structure, e.g. for routing purposes, and it may not be possible to generate or randomize all the bits of the identifier value. For example, in a current LTE system, a GUTI is constructed using the following fields (3GPP TS 23.003 [65]):

GUTI = MCC (12 bits) || MNC (12 bits) || MMEGI (16 bits) || MMEC (8 bits) || M-TMSI (32 bits)

The first 48 bits, i.e. MCC || MNC || MMEGI || MMEC, uniquely identify the MME that assigned the GUTI. Furthermore, it is also specified in [65] that the M-TMSI shall not have a value with all 32 bits equal to 1, and the 2 MSBs of the M-TMSI have special meaning. Hence, there are 30 bits available for any MME for assigning unique identifiers to the UEs that are served by the MME.

Therefore, only the part of the identifier that is not a part of a standard structure should be generated separately at the UE side and the NGC side, e.g. 30 bits of the M-TMSI in a current LTE system. The NGC may also need to transfer one of more parts of the identifier to the UE, e.g. MCC, MNC, MMEGI, MMEC and 2 bits of M-TMSI in a current LTE system.

The generation of the short-term identifier must be done with care to ensure that the probability of collisions between short-term identifiers allocated to different UEs is sufficiently small. Should there be collisions the NGC will not be able to tell the two UEs apart and would have to resort to a recovery mechanism, e.g., requesting the long-term identifier.

It should be noted that the reliability of this mechanism can be brought to the same level as the currently used mechanism in LTE, GSM/GPRS and UMTS. For example, lost messages can be re-transmitted as is done in the LTE NAS protocol.

5.7.4.13.2.3 Solution Variant-B

The NGC assigns a new short-term identifier to the UE in NGC-NAS messages like in LTE. Some examples of such message(s) in terms of a current LTE system are ATTACH ACCEPT, TRACKING AREA UPDATE ACCEPT, and GUTI REALLOCATION COMMAND. Apart from mandating the NGC to assign a new short-term identifier each time to the UE, it is crucial that the UE verifies the freshness of the newly assigned short-term identifier. Because, a poor implementation and/or policy configuration of the NGC could assign the same identifier repeatedly to the UE or the NGC could toggle between two fixed identifiers for the UE. Therefore, the UE verifies that the newly assigned short-term identifier is a fresh one, for example by at least comparing to the last one or the last two.

Editor's Note: It is FFS to determine how many of last assigned temporary identifiers are sufficient for the UE to check for enhancing the privacy.

If the verification fails, the UE disconnects from the network, refuses to establish a user plane connection or other self-crippling feature. Figure 5.7.4.13.2-2 illustrates a high-level generalized data-flow of the variant-B.

Lenovo Ex. 1007
Page 372

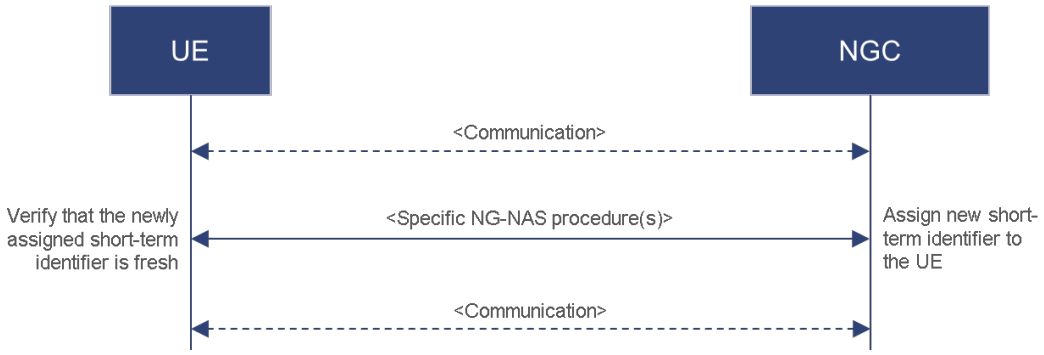


Figure 5.7.4.13.2-2: High-level data-flow of solution (variant-B)

5.7.4.13.3 Evaluation

Editor's Note: LTE standard allows changing GUTI, but this is an optional feature and up to the operator policy. One solution is to mandate in NextGen to change GUTI at each TAU accept, attach accept, etc. The advantage of using the proposed variants A and B is FFS.

Variant-A changes the short-term identifier per a variable calculation. Therefore, if the NGC does not perform the same calculation, it will not recognize the UE on the next communication between the two, degrading the performance of the NGC. This provides an incentive to adhere to stricter implementation and privacy configuration policy in the NGC.

In Variant-B, the NGC may chose not to renew the short-term identifier. Doing so would result in degraded service for the UEs, since the UEs check whether they are allocated a new short-term identifier or nor.

One could argue that there may be an incentive for UE manufactures not to implement the self-crippling functions. To provide also them with an incentive to implement the UEs in a privacy conscious fashion, it could be added as a feature that is configurable via the UE's user interface.

5.7.4.14 Solution #7.14: Privacy protection of permanent or long-term subscription identifier using ABE

5.7.4.14.1 Introduction

This solution presents an alternative mechanism to address the key issue #7.2 "Concealing permanent or long-term subscription identifier" only in the case where a temporary subscription identifier is not available (c.f. initial Attach Request in LTE). In the sequel, "subscription identifier" denotes a permanent or long-term subscription identifier, e.g. IMSI.

In the solution, the subscription identifier is encrypted on the UE by using a global public key and a public attribute bound to a private key according to the Attribute-Based Encryption (ABE) scheme [rif 1]. The scheme provides assurance that only the authorized entity owning the private key bound to the public attribute is able to decrypt the encrypted subscription identifier.

An authorized entity can be any serving network that is provisioned with a valid decryption key (i.e., the private key corresponding to the attribute used in encryption). The ABE scheme permits the serving network to satisfy LI requirements, i.e., the serving network is able to intercept all the mobile network services of the LI target without the home network's assistance or visibility.

Therefore, the solution conceals the entire subscription identifier from attackers on the air interface (c.f. Uu interface in LTE), as well as on the interface between the RAN and the core network (c.f. S1-MME interface in LTE) since the subscription identifier is not transmitted in clear-text.

Lenovo Ex. 1007
Page 373

5.7.4.14.2 Solution details

5.7.4.14.2.1 General

The solution is based on a single (global) public key used by all the UEs (worldwide) to encrypt the respective subscription identifier in any case where a temporary subscription identifier is not available (c.f. initial Attach Request in LTE).

Editor's Note: It is FFS to determine which entity is responsible for managing the single (global) public key and if it is feasible to do so.

Each UE is provisioned with the global public key and the UE uses the global public key independently from the network where the UE is attaching (e.g. initial Attach Request in a roaming scenario). Only the attribute used in encryption changes depending on the network that the UE is attaching to.

An entity is able to decrypt the subscription identifier only if it is an authorized entity, meaning that it has been provisioned with a valid private key having corresponding attribute. For this reason this solution requires only one global public key and "N" private keys, where "N" comprises all authorized entities. In an initial setup phase the global public key is bound to a Universe of authorized attributes which comprises the "N" authorized entities together with some redundancy. N should include at least the current mobile network operators and preferably it should be overestimated to include new operators.

Editor's Note: It is FFS to clarify parameters and the relation between them, in particular:

- the size of the global public key as a function of "N".
- the estimated value or size of "N" that is safe to use in the NextGen, i.e. shorter "N" might overflow if the number of authorized entities increase drastically
- how much redundancy is needed and what is the corresponding effect in the size of the global public key.

Editor's Note: It is FFS to clarify how new authorized entities are added and what is the corresponding effect in the global public key.

In this context, an authorized entity is every serving network, which the UE can be connected to (e.g., the home network and the visited network(s) in roaming). Each private key is bound to the global public key through an attribute (which can be related to the identity of the serving network), according to the Attribute-Based Encryption scheme. The attribute uniquely identifies the authorized entity that is allowed to decrypt the subscription identifier, i.e., the entity that owns the corresponding private key. Specifically, the attribute (which can be an identifier) identifies the serving network that is currently serving the UE and a specific valid private key of the serving network.

The serving network attribute can be broadcasted over the air together with the mobile network identifier (e.g., the PLMNID), and it is used by an UE, during the Attach procedure, together with the global public key to encrypt the subscription identifier before sending it over the air.

The entity receiving the encrypted subscription identifier can decrypt it only if its private key is bound to the attribute that the UE has used in encryption. This implies that if a fake attribute is broadcasted over the air, the UE is not able to properly encrypt, since the fake attribute was not included in the initial Universe of authorized attributes. If a valid attribute (spoofed) different from the attribute owned of the current serving network is broadcasted, the fake entity is not able to decrypt it, unless it has also compromised the corresponding private key. Therefore, a fake entity is not able to perform the permanent or long-term subscriber identifier decryption unless it has compromised one currently valid private key.

The solution further offers following two options.

5.7.4.14.2.2 Option 1

During an Initial Attach, according to the solution, the UE encrypts its subscription identifier by using the global public key and the attribute received in broadcast over the air (the attribute identifying the serving network to which the UE is currently connected to). The authorized entity receiving the encrypted subscription identifier decrypts it and then requests from the UE's home network the authentication data (AV) using the decrypted subscription identifier. During or after every authentication procedure a temporary subscription identifier will be assigned to the UE which will be used in future communication instead of the ABE-encrypted subscription identifier.

Lenovo Ex. 1007
Page 374

Editor's Note: it is intentionally not covered by this contribution how the temporary subscription identifier is generated/assigned/maintained..

According to this solution, upon decryption, the UE's subscription identifier is known only to the authorized entity (the current serving network). This permits the serving network to satisfy the requirements of lawful interception, i.e. allowing the serving network to perform lawful interception without the home network's assistance or visibility.

Note that the privacy requirement to have the randomized encryption property is intrinsically ensured by the ABE schemes.

The solution conceals the UE's subscription identifier from all network entities on the path between the UE and the serving network including attackers on the air interface, IMSI-catchers, and attackers in the serving networks (untrusted/unauthorized network entities).

Protection of subscription identifier between a serving network and the home network is not provided and relies on the deployment of additional mechanisms like IPsec. An alternative option (Option 2) is presented to extend the subscription identifier protection also on the interface between a serving network and the home network.

5.7.4.14.2.3 Option 2

During an Initial Attach the UE encrypts its subscription identifier by using the global public key and two attributes: (i) the one received in broadcast over the air (identifying the serving network to which the UE is currently connected to) as in option 1, and (ii) the second one being the home network's attribute.

Differently from the first option, the use of the home network attribute permits the serving network to forward the encrypted long-term subscriber identifier to the UE's home network ensuring the privacy protection also on the interface in between. Before forwarding the encrypted subscription identifier, the serving network needs to decrypt the subscription identifier in order to retrieve the MCC and MNC for determining the corresponding home network from which to get the authentication data.

A feature of this option is that the subscription identifier shall be decrypted both at the serving network and the home network, but no additional protection mechanism like IPsec is then needed for subscription identifier protection (IPsec may however still be recommended to protect transfer of AV etc).

5.7.4.14.3 Evaluation

The solution presented here has the following properties:

- The solution protects the entire long-term identifier (MCC, MNC and MSIN) over the air in both the options. In Option2 it also provides e2e protection to the home network of the IMSI. Therefore the solution can discourage the fake BTS attack scenarios.

- The solution is lawful-interception-friendly, since the current serving network obtains the entire UE long-term subscriber identifier by decryption in both options. This is subject to the VPLMN being provided with the correct Key.

- The solution does not require the deployment of a PKI infrastructure. It is based only on an initial setup when the global public key is generated and bound to a Universe set of attributes. The Universe set also includes some redundancy for each authorized entity, i.e., reserve attributes for revocation, which can be identified by different indexes.

Editor's Note: It is FFS to clarify what kind of other infrastructure, if not PKI, is required to handle revocation and addition of new authorized entities, and if it is feasible to do so.

- The UE needs to be provisioned with only one public key, called global public key, used by the UE to encrypt its long-term identifier, independently of the serving network to which it is connected to at a given time. This provides protection also in case of roaming scenarios and avoids the need to update the UE in case where the subscription changes.

- An entity is able to decrypt the UE's subscription identifier only if it is authorized by having been provisioned with a valid private key and a valid attribute. The solution requires one global public key and "N" private keys where "N" comprises all the authorized entities (e.g., the MNOs). In this context, a serving network to which the UE can be connected is an authorized entity (e.g., as specified by the roaming agreement). Note that both Options 1 and 2 use the same set of "N" private keys.

Lenovo Ex. 1007
Page 375

- The solution permits to encrypt the subscription identifier by using more than one attributes (combined according to the "or" logic) allowing in this way different authorized entities to decrypt it, as in Option 2. The advantage is that in this combined logic the private keys do not change.

- Depending upon the encryption scheme, the encrypted identifier could increase the size of the messages, which could impact the bandwidth. The ABE schemes based on elliptic curve pairings are rather efficient if the number of attributes effectively used in encryption is small. Note, however, that the encrypted identifier is rarely used, namely, only when a pseudonym does not exist or the communication/UE is out-of-sync.

5.7.4.15 Solution #7.15: Encrypting IMSI based on Elliptic Curve Integrated Encryption Scheme (ECIES)

5.7.4.15.1 Introduction

This solution addresses the key issue #7.3 "Concealing permanent or long-term subscription identifier" by providing a way to conceal the IMSI using public key encryption based on Elliptic Curve Integrated Encryption Scheme (ECIES).

This solution may stand on its own or be an enabler for other solutions that use public key encryption such as the ones in clauses 5.7.4.2 and 5.7.4.3. The size of the message to send encrypted IMSI is in the order of 320 bits.

5.7.4.15.2 Solution details

This solution is based on the Elliptic Curve Integrated Encryption Scheme (ECIES). The ECIES is a public key encryption scheme that uses Elliptic Curve Cryptography (ECC) and constitutes of various functions like key agreement, key derivation, hash, encryption, and MAC. The encryption function in the ECIES is symmetric; however, the key used in the encryption is generated using the ECC public/private key pairs of the communicating parties.

The ECIES may also be taken as a so-called "hybrid" cryptosystem in the sense that it can be used to encrypting the keying data. In a traditional hybrid cryptosystem, the information data is actually encrypted using a symmetric encryption, but the keying data (used in the symmetric encryption) is encrypted using the asymmetric encryption. The ECIES is flexible in the sense that it can be used either similarly as a traditional hybrid cryptosystem to encrypt the keying data or to encrypt the information data using the keys derived from key agreement and symmetric encryption. The solution does the later, i.e. the information data, which is IMSI, is encrypted.

The SECG SEC1 specification [70] may be referred for the description of the ECIES along with the cryptographic primitives that are used in the ECIES. The authors of [67] have summarized the list of functions in the ECIES as specified in more than one standards including ANSI X9.63, ISO/IEC 18033-2, and SECG SEC1. The SECG SEC1 specification [70] and the report from ECRYPT [68] state that the ECIES is secure to be used with key size ≥ 256.

The encryption and decryption process of this solution are illustrated in Figure 5.7.4.15.2-1 and Figure 5.7.4.15.2-2 respectively.

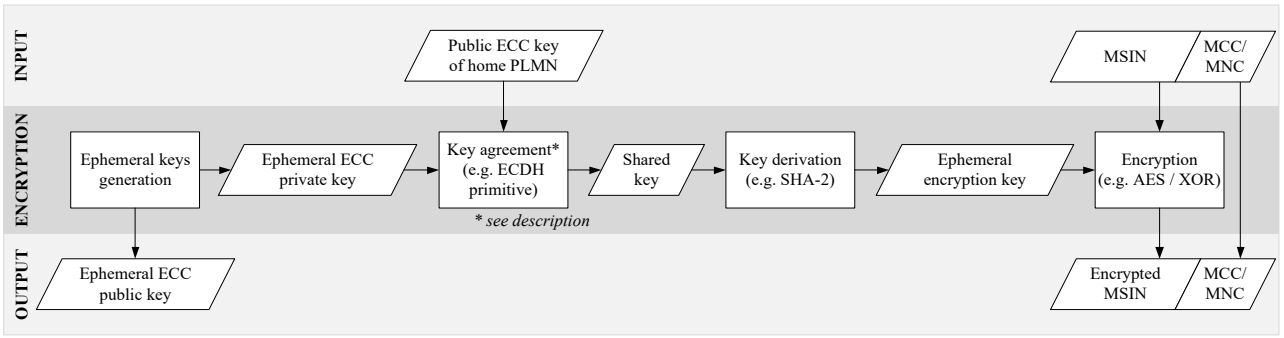


Figure 5.7.4.15.2-1: Encryption at the UE side (based on ECIES)

Lenovo Ex. 1007
Page 376

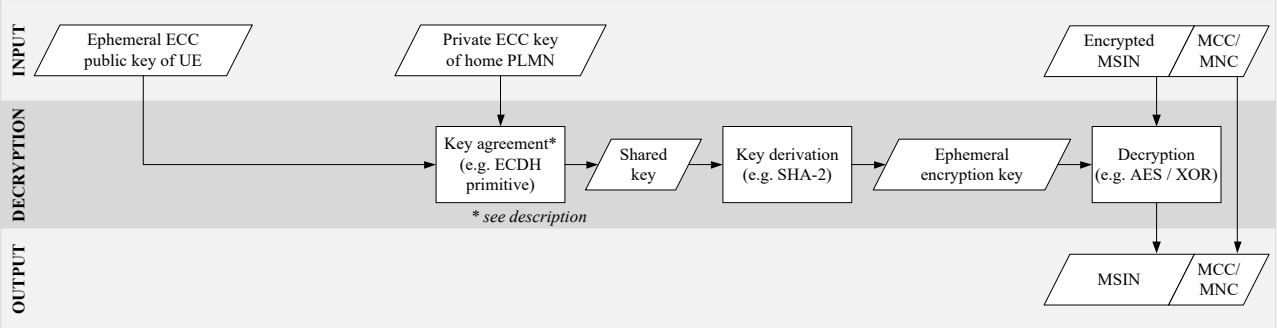


Figure 5.7.4.15.2-2: Decryption at the network side (based on ECIES)

This solution has followings specifics:

1) In the ECIES, the Elliptic Curve Diffie-Hellman (ECDH) primitive shown in the diagram is basically used to generate a shared key from a private key owned by one party (UE or home PLMN) and a public key owned by another party (home PLMN or UE). The ECDH is a variant of the well-known Diffie-Hellman key agreement protocol using ECC.

2) The public keys used in the ECDH can be either static (but trusted) or ephemeral. The solution is compatible with both.

3) When the public key of only one of the parties is static (but trusted), there is no need to run the full DH exchange and therefore, the other party is able to send the encrypted information data directly in the first message. For example, when the public key of the home PLMN is already available to the UE (e.g. solution in clause 5.7.4.3), the UE is able to send the encrypted IMSI in the very first attach request. In other words, the public key of the home PLMN is static (but trusted) while the public/private key pair of the UE is ephemeral.

4) However, the solution is also compatible with a full DH exchange, for example to be used with the solution in clause 5.7.4.2, where the UE has some way to obtain and verify the public key of the network.

5) The symmetric encryption key is ephemeral, because at least the public/private ECC keys of the UE are always ephemeral, which means that different keys are used to encrypt the same IMSI at different times.

6) The size and format of the encrypted MSIN can be kept the same (which is 40 bits at max with 0-9 digits) for example, by using format preserving encryption (FPE) (e.g. FPE using AES as described in [69]). If format is not an issue, the size of the encrypted MSIN can be kept the same (40 bits) for example, by using block cipher in stream mode (e.g. AES in CTR mode). Since the encryption key is ephemeral and used only once, the XOR function is equally suitable alternative to the AES. The XOR function provides support for size and format preserving as well.

7) The MAC function which is also provided by ECIES is proposed to not be used because the keys of the UEs are ephemeral and therefore an integrity tag does not serve any necessary purpose. The extra benefit is that the size of the message is also decreased.

As shown in Figure 5.7.4.15.2-1, the size of the output includes the ephemeral public key of the UE in addition to the encrypted IMSI. When a 256 bits elliptic curve with point compression is used, the size of the ephemeral public key that needs to be transferred is 256 bits plus sign indication. The IMSI is 15 digits at max or 60 bits at max in BCD encoding (i.e. MCC/MNC is 24 bits long at max and the MSIN is 40 bits long at max). Therefore, the total size of the encrypted IMSI message is in the order of 320 bits.

Editor's Note: Only the EC curve, the underlying field, and the ECIES functions that are proven to be secure shall be used. Whether the EC curves, the underlying fields, and the ECIES functions are standardized by 3GPP or not is FFS.

5.7.4.15.3 Evaluation

a) The solution is well-proven and actually has a formal security proof, see e.g. [68, 71].

b) The solution may stand on its own or be an enabler for other solutions that use public key encryption such as the ones in clauses 5.7.4.2 and 5.7.4.3.

Lenovo Ex. 1007
Page 377

c) The ECIES uses elliptic curve cryptography (ECC) which is good choice for mobile devices because of faster computation time (meaning longer battery time) and shorter key size (meaning less radio resource).

d) The solution supports preserving the format and the size of the encrypted MSIN.

e) The size of encrypted IMSI is in the order of 320 bits. At a first sight, sending 320 bits over the air might appear as a problem. But, it is not a problem because:

- It is a fair assumption that similar to the current LTE system, the NR might as well have size restriction for the messages that are transferred in RACH and SRB0 (c.f. LTE RRC connection request) due to physical layer transport block size. But, note that it is the S-TMSI that is transferred in SRB0 (c.f. LTE RRC connection request).

- The IMSI, however, is neither transferred in RACH nor SRB0 (c.f. LTE RRC connection request). The IMSI is transferred after a radio resource is assigned to the UE (c.f. LTE NAS Attach Request tunnelled in LTE RRC connection setup complete message). The LTE RRC connection setup complete message is transferred in SRB1 with RLC AM that supports segmentation.

- Therefore, the size of encrypted IMSI is not limited by the physical layer transport block size.

f) The solution does not use a tag unlike in normal ECIES. There might be concerns that an attacker:

- guesses valid IMSI and sends it encrypted: The scenario is same as today in case of plain-text IMSI. The network will send authentication challenge to which the attacker cannot provide valid response.

- captures an encrypted IMSI over the air and replays it: The scenario is same as today in of plain-text IMSI. However, the network may keep track of the IMSI and its encrypted values or the ephemeral public key that were used in the past. Or, the SQN value may also be used since it is supposed to be changing after each authentication.

g) The solution provides identifier privacy at the cost of additional computational overhead in the core network function that does the IMSI decryption. However, since the encrypted IMSI itself is random every time, no additional complexity is required in the core network function for generation and management of separate temporary identifiers such as pseudonyms. Having said that, the solution is also compatible to be used along with pseudonyms to save radio resources, such as the one in clause 5.7.4.3.

h) It is also worth noting in general that the number of bogus attach-requests that an attacker can send to the core is limited by the physical radio resource. For example, in case of LTE, the number of RACH requests, necessary to get the UL grant, is limited by the physical radio resource allocated for RACH, i.e. PRACH configuration.

5.7.4.16 Solution #7.16: Mechanism for temporary identifier assignment

5.7.4.16.1 Introduction

This solution addresses the key issue #7.4 "Using effective temporary or short-term subscription identifiers".

In the current LTE system, the serving PLMN (c.f. MME) uses GUTI as a temporary subscription identifier. However, the home PLMN (c.f. HSS) uses only a permanent subscription identifier, i.e. IMSI. The GUTI is primarily used to minimize the exposure of the IMSI over the air.

In order to completely thwart the IMSI Catcher attacks, it is likely that in the NextGen system, the home PLMN itself will use a temporary subscription identifier during the UE authentication (say $IMSI_{Pseudo}$). When there is an $IMSI_{Pseudo}$ in place, the GUTI might look redundant at first. However, re-authenticating the UE is not required during all communications and therefore, for optimization, the serving PLMN may assign a GUTI to the UE. In this solution, the term "temporary identifier" is used to denote both the $IMSI_{Pseudo}$ and the GUTI.

The other solutions addressing the different key issue #7.1 generally have a trigger that starts the temporary identifier refreshment. It is not in the scope of this solution to decide when to trigger the refreshment of the temporary identifier (e.g. $IMSI_{Pseudo}$ at authentication request, GUTI at Tracking Area Updating request). However, this solution presents a mechanism of how the UE and the network share the common temporary identifier to be used the next time, and is therefore an enabler for the solutions belonging to the key issue #7.1.

Lenovo Ex. 1007
Page 378

5.7.4.16.2 Solution details

This solution adopts the already existing mechanism in LTE where the network assigns a new temporary identifier to the UE in a confidentiality and integrity protected message, e.g. in ATTACH ACCEPT, TRACKING AREA UPDATE ACCEPT, or GUTI REALLOCATION COMMAND. It is left up to the network to decide which method to use for generating the next identifier, e.g. using output from a pseudo random permutation with a constant key and sequence, using new or pre calculated non-conflicting random values, or using new or pre calculated sequences, etc.

However, since a poor implementation and/or policy configuration of the network could assign the same identifier repeatedly to the UE, the UE could be tracked using the "non-changing" temporary identifier causing a threat to subscriber privacy. Therefore, the solution enhances the existing mechanism in LTE by requiring that the new identifier assigned to the UE is not the same as the last one or two identifier(s) assigned to the same UE.

In addition to requiring the network to not assign the last assigned identifier, it is crucial to specify the behaviour of the UE as well. Because, in absence of the UE's involvement, the network could, in practice, not follow the specification. Therefore, in this solution, the UE verifies that next temporary identifier assigned to it is not the same as the last one or two.

Editor's Note: It is FFS to determine how many of last assigned temporary identifiers are sufficient for the UE to check to enhance the privacy.

If the UE determines that the verification has failed, it may react, for example by reattaching to the network, or by performing some self-crippling functions like refusing to use network slice, user plane data etc. Doing so will, on one hand, encourage the networks to ensure that the identifier is new. On another hand, implementation for toggling a fixed set of temporary identifiers (which is not good) will require even more considerations (e.g. more memory and processing to maintain the set and its state for each UE) and therefore will be discouraged.

Editor's Note: It is FFS to determine if the user will be provided with options on what specific actions to take when verification fails (related to visibility and configurability).

5.7.4.16.3 Evaluation

The temporary identifiers are supposed to be used in clear-text over the air and the whole purpose of using the temporary identifier is so that the subscription behind the temporary identifier is not identifiable.

It should be carefully noted that predicting a temporary identifier and identifying the subscription behind the predicted temporary identifier are two different things. While identifying the subscription behind the temporary identifier is clearly a privacy issue, just predicting a temporary identifier that cannot be linked to any subscription is not a privacy issue.

For example, consider that it becomes mandatory to reassign GUTI after every TAU procedure. In order to make minimal changes to the existing implementation, if some networks send the same old GUTI back to the UE, the GUTI can be linked to the same subscription and therefore becomes a privacy issue. However, if the UE makes sure that the newly assigned GUTI is not the same as the old GUTI, then it becomes unfeasible for an attacker to link the two GUTIs together even if as simple as a counter is used to generate next GUTI. The reason is explained next.

In terms of LTE, the GUTI is unique per subscription in the MME and typically one MME may handle hundreds of eNBs and several millions UEs. The two consequent GUTIs assigned by the MME might end up in eNBs or UEs geographically very far from each other. Therefore, first of all, it is physically unfeasible for an attacker to record all the GUTIs covered by the MME, in order to be able to predict the next GUTI. Second, even if the attacker may predict the next GUTI, it is unfeasible to link it to any particular UE when there are more than one UE in the area. Note that if there is only one UE in the area, then no matter how random the next GUTI is, all the GUTIs point to the same UE anyway. The attack becomes even more unfeasible in case of $IMSI_{Pseudo}$ because the $IMSI_{Pseudo}$ is unique per subscription in the HSS, and the HSS covers the whole PLMN.

It also seems unnecessary to impose any other complexity, e.g. good random, for the temporary identifier generator. For example, when something like a hash function is used with some UE specific and freshness parameter, it is possible but not practical for the network to know in advance what value is generated next. The network needs to verify that the newly generated value is not already assigned to another UE. If the value is already assigned, the network must generate another value and again perform the verification. This process needs to be repeated until an unused value is generated. Such a process, while being possible, is not practical because as the number of currently assigned values increase, the chance of generating an unassigned value decreases. It means that the time for generating new temporary identifiers increases for every new assignment.

Lenovo Ex. 1007
Page 379

Therefore, it seems necessary and sufficient to assure that a newly assigned temporary is not the same as the old temporary identifier.

The solution addresses both the requirements in the key issue #7.4.

The solution is also an enabler for the solutions that address the key issue #7.1 "Refreshing of temporary subscriber identifier".

5.7.4.z Solution #7.z: <solution name>

5.7.4.z.1 Introduction

Editor's note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the security area.

5.7.4.z.2 Solution details

5.7.4.z.3 Evaluation

5.7.5 Conclusions

Editor's note: This clause will contain the evaluation between the solutions, and the conclusions made by SA3.

5.8 Security area #8: Network slicing security

NOTE: Network slice related terms should be referred to work of other WGs, for example, TR 23.799 [2], TS 23.501 [74], and TS 23.502 [83] and otherwise, it should be understood as general terms.

5.8.1 Introduction

Network slicing will be an important component of the Next Generation network. It enables the operator to create networks customised to provide optimized solutions for different market scenarios which demands diverse requirements, e.g. in the areas of functionality, performance and isolation. A network slice is composed of a collection of logical network functions that supports the communication service requirements of particular use cases.

Functionalities and capabilities within 3GPP scope that enables the next generation system to support the Network Slicing and Network Slicing Roaming requirements are defined in TR 22.864 [6]. Solutions for the network slicing which include architecture and functionality are defined in TR 23.799 [2].

Among the features related to network slicing in TR 23.799 [2], several have potential security implications such as the sharing of network functions and the isolation between the different slices. In particular, in relation to isolation, in some of the security requirements of [6] it is mentioned that network slices might be potentially open for 3rd parties to run their own functions or even might be entirely managed by external parties such as an enterprise or a public safety organization.

Other requirements and use cases from TR 22.864 [6] indicate that the service access model is different in the Next Generation systems. UEs are not only able to access the services through different types of access networks: 3GPP, non-3GPP, trusted and less trusted, but also able to simultaneously access services provided by different network slices. All these capabilities combined lead to a proliferation in the number of possible deployment scenarios for example depending on which functions are shared, which type of network access is used, what is the trust relationship between the service provider and the network operator, etc.

5.8.2 Security assumptions

Editor's Note: This clause will document security assumptions related to network slicing.

In order to better capture the security assumptions for network slicing, the following aspects need to be taken into consideration:

Lenovo Ex. 1007
Page 380

- Network function sharing;
- Access network sharing;
- Access from less trusted networks;
- Coexistence within a network slice with 3rd parties' network functions;
- Coexistence between network slices with different security assurance requirements;
- Simultaneous UE connections to multiple network slices;
- Simultaneous UE connections through different access technologies.
- Possible deployment scenarios and trust relationship between the network operator and the service provider, e.g. third party application server.
- Initial access by UE to the network by including a network slice selection parameter, if UE has such a parameter provisioned.
- UE authentication by network
- network and/or network slice authentication by the UE
- Network selection of network slice and assignment to UE, based on the network selection parameter.

Editor's Note: This list may not be exhaustive and may be revised depending on the progress in the other working groups.

5.8.3 Key issues

5.8.3.1 Key Issue #8.1: Security isolation of network slices

5.8.3.1.1 Key issue details

NOTE: The security isolation of network slice instances needs to consider both physical and logical aspects.

Isolation between slices is a basic requirement of slicing network. TR 22.864 ([6] , clause.5.1.2.1) and TR 22.891([7], clause.5.2.3) have given some specific requirements about isolation.

The network may host different network slices for differentapplications or organizations. Each network slice instance may have a Slice/Service Type to indicate the type of functions it is hosting within it. To take care of high traffic load conditions or administrative purposes, the network may increase the capacity of network slice or instantiate multiple instances of the same network slice template. In all scenarios, isolation between network slices are important. For example, elasticity and change of slices or the communication in one slice cannot have impact on services served by other slices. If a slice is compromised, it should not negatively impact the performance and security of any other network slice. If it is possible to access one slice from another slice, then this access may be utilized to launch attack.

NOTE: Network slice related terms should be referred to work of other WGs, for example, TR 23.799 [2] and otherwise, it should be understood as general terms (e.g. tenants, slice type).

Network slices need to be isolated from each other in robust way. It should be possible for each network each slice to have independent security policy in accordance with the defined functionality of the network slice requirement.UEs may get assigned to different instances of the network slice based on subscription data, network policy and capability. Security isolation between different slices, irrespective of whether they are of the same type or belong to the same network operator (or third party) are needed.

NOTE: Key issue details are general description for consideration of security aspects, and exact rule and procedure of UE assignment to the network slice instance will be specified in TR 23.799 [2], TS 23.501 [74], and TS 23.502 [83]

It is expected for a single NG-UE to be able to access more than one slice. In this case, it should be taken into account that data leakage, data integrity breaches, and data confidentiality breaches might be possible on the network side and on the NG-UE side.

Lenovo Ex. 1007
Page 381

5.8.3.1.2 Security threats

Without isolation, attackers who have access to one slice may launch an attack to other slices. For example, capacity elasticity of one slice may consume the resources of other slices, which causes lack of resources and cannot support the services of others. Attackers may utilize this to launch a DoS attack to slices. Attackers can also steal data by having illegal access to functions in other slices or covert channel attack.

Attacks on data confidentiality (e.g., data leakage between network slices) and integrity are possible when a single NG-UE is accessing more than one network slice. In the particular case where one slice is serving a UE over a non-3GPP access (i.e., less trustworthy) and one slice is serving the UE over a 3GPP access, it is important to maintain the isolation between the slices on the UE.

5.8.3.1.3 Potential security requirements.

-NOTE: Security isolation of network slice considering NSI (Network Slice Instance) identifier, including slice selection and roaming cases, will be specified in normative phase.

-

Platforms supporting network slice should be able to ensure that resource of network slice instances is not impacted from each other (e.g. by reserving resource per network slice instance).

- The 3GPP System shall have the capability to provide a level of isolation between network slices which confines a potential cyber-attack to a single network slice.

- It should be possible to isolate slices from one another, to minimize attacks on data confidentiality (e.g., data leakage between network slices) and integrity when a single NG-UE is accessing services over more than one network slice.

NOTE: This requirement is applicable to network elements and functions. Isolation of network slices within UE may be considered in normative phase, if it needs to be addressed in 3GPP specifications.

5.8.3.2 Key Issue #8.2: Security mechanism differentiation for network slices

5.8.3.2.1 Key issue details

The next generation network will be a service-oriented network and different services have different requirements, including security. As proposed in TR 22.891 (ref.[7] 5.2.3), the 3GPP System shall have the capability to conform to service-specific security assurance requirements in each single network slice, rather than the whole network, which means every slice can have service-specific security mechanisms(including e.g. policy, protocols and functions and so on) configured.

- On eMBB services, we could reuse or optimize the mechanism in LTE, i.e. to keep the authentication and credential management entities within the core network and use IMSI as the user's only credential.

- On IoT services, the more quick access authentication protocol should be considered to meet the requirement of large amount devices visit "AN" (e.g. RAN node or common function node), the lighter cryptographic algorithms or/and protocols should be considered to meet low cost and low battery situation on IoT devices.

  On CriC services, the quick access and strong authentication protocol, encryption algorithms, or/and credential management etc. should be considered to meet the low latency and high reliability requirement in critical communications.

The NG-UE when it does network attach is supposed to include a network slice selection parameter if it has one. Based on the network selection parameter a slice selection function will make a choice and assign the NG-UE to a dedicated network tenant or to a application-specific network slice . Each network slice can define its own security policies and security mechanisms.

5.8.3.2.2 Security threats

Different network slice tenants may have different access authentication requirements. In addition, network slices hosting application specific functions may have access security as well as session security demanded by the application. In the absence of a proper level of security for each network slice, both access and sessions can be compromised.

Lenovo Ex. 1007
Page 382

5.8.3.2.3 Potential security requirements

To satisfy security requirements from different types of network slices, the 3GPP System shall have the capability to conform to service-specific security assurance requirements in a single network slice, rather than the whole network. Different security mechanisms shall be supported to meet the slice specific requirement.

The 3GPP system shall support the security mechanism differentiation in authentication methods, types of credentials, subscriber repository, controlling policies and security policies. Security policies may include isolation policies, encryption algorithms, integrity protection algorithms, the lengths of keys, and the policies of key expiration.

It should be possible to define different access security mechanisms as well as session security mechanisms (e.g. control plane, user plane, handover etc) for every network slice.

5.8.3.3 Key Issue #8.3: Security on UEs' access to slices

5.8.3.3.1 Key issue details

The fact that several network slices might be available in Next Generation systems requires a selection procedure in order to direct UEs to corresponding slices. To ensure that slices can be selected and accessed correctly for UEs, how to protect the security of such procedure should be addressed.

Editor's Note: The selection procedure is still being studied in other working groups. The text above should be revised based on their progress

Besides the slice selection security, it is expected that the Next Generation systems are able to provide access to services in different ways. A UE can simultaneously access multiple services delivered by different network slices. It can also access the services through different types of access networks, 3GPP and non-3GPP, trusted and less trusted. Furthermore, in the context of the IoT, it is expected that there will be a proliferation in the types and the number of connected devices (UEs) such sensors and smart wearables.

There are potentially several vulnerable links over which the access to the network slice and hence the service can take place (see Figure 5.8.3.3-1).

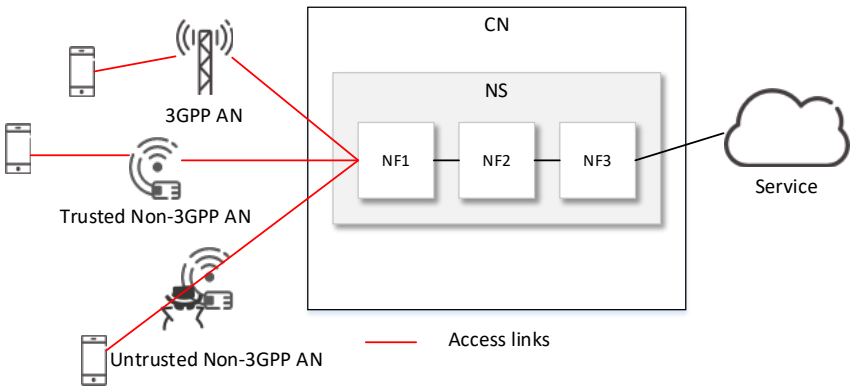


Figure 5.8.3.3-1: Access links in Next Generation systems

Solutions for this key issue should aim to be generic to the extent possible in order for the authentication and authorization mechanism to support such variety in access/device type and also to be future proof.

As observed by 3GPP TR 22.864, services offered by the network slice could either belong to the MNO or a 3rd party service provider. When the slice is allocated to a 3rd party service provider, the ability of the provider to verify and ascertain the identifier of the subscription, trying to gain access to the slice, becomes a critical security component to be addressed.

For the attach procedure of UEs' access to network slices, following scenarios should be considered:

Lenovo Ex. 1007
Page 383

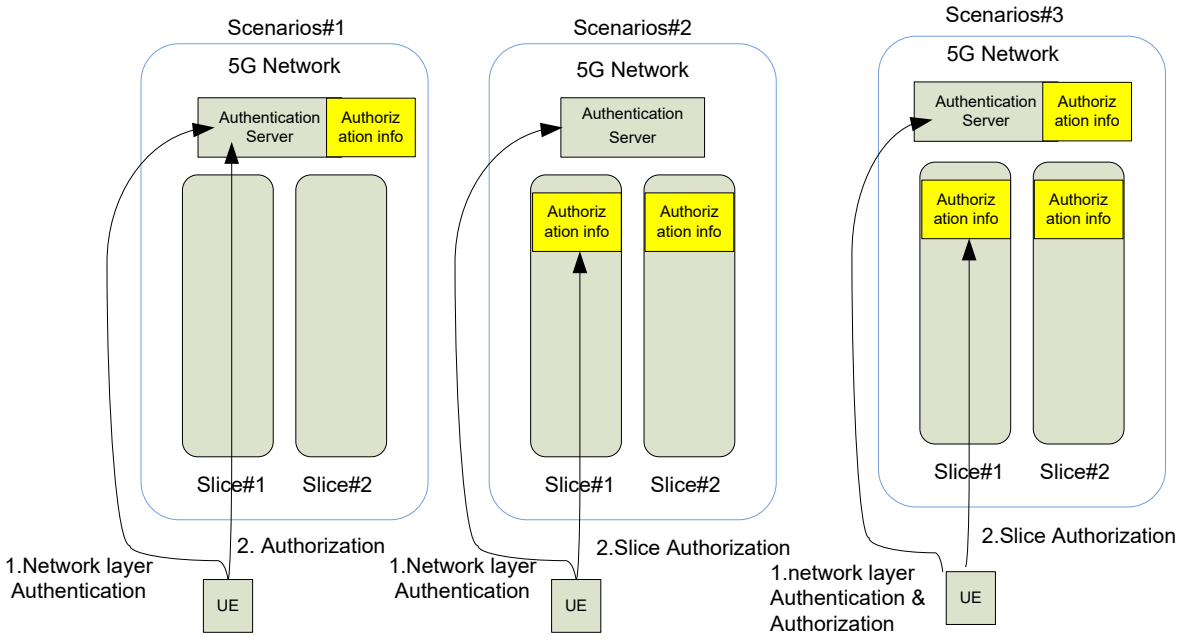


Figure 5.8.3.3-2

Scenario#1: UE is authenticated and authorized by MNO. 3rd party provider entirely relies on MNO for authentication and authorization.

Scenario#2: UE is authenticated by MNO. 3rd party provider relies on MNO authentication but provides authorization to the UE.

Scenario#3: UE is authenticated and authorized by MNO. 3rd party provider relies on MNO authentication and provides additional authorization to the UE.

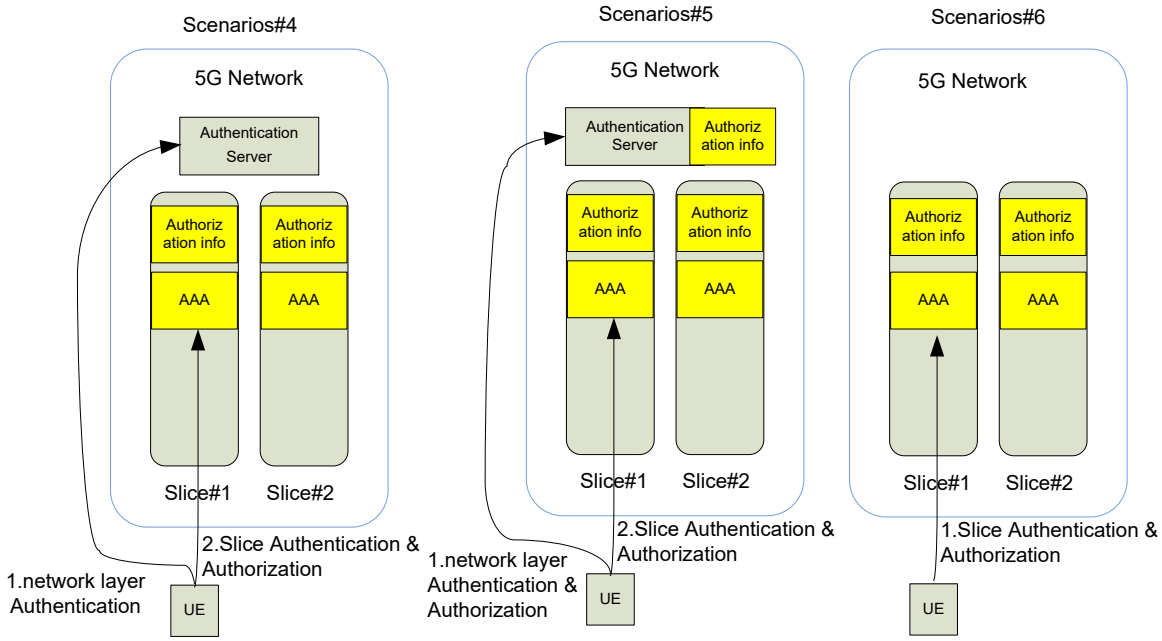


Figure 5.8.3.3-3

Scenario#4: UE is authenticated by MNO. 3rd party provider performs secondary authentication and provides authorization to the UE.

Scenario#5: UE is authenticated and authorized by the MNO. 3rd party provider performs secondary authentication and provides secondary authorization.

Lenovo Ex. 1007
Page 384

Scenario#6: There is no primary authentication and authorization of the UE by the MNO. 3rd party provider performs authentication and authorization of the subscription.

Editor's Note: The requirements by SA1 and SA2 on which all scenarios rest, require further clarification.

For authentication of UEs' access to network slices, if methods based on key sharing between UE and network are used, then keys for integrity and confidentiality are derived from intermediate keys (e.g. Kasme and Kenb in LTE), which are also derived from long-term/root keys directly or indirectly. Keys can be grouped as CN keys and AN keys, and further be divided into intermediate keys, CP keys (keys for integrity and confidentiality for C-Plan), and UP keys (keys for integrity and confidentiality for U-Plan). Following scenarios for key sharing between slices should be considered (intermediate keys not shown explicitly):

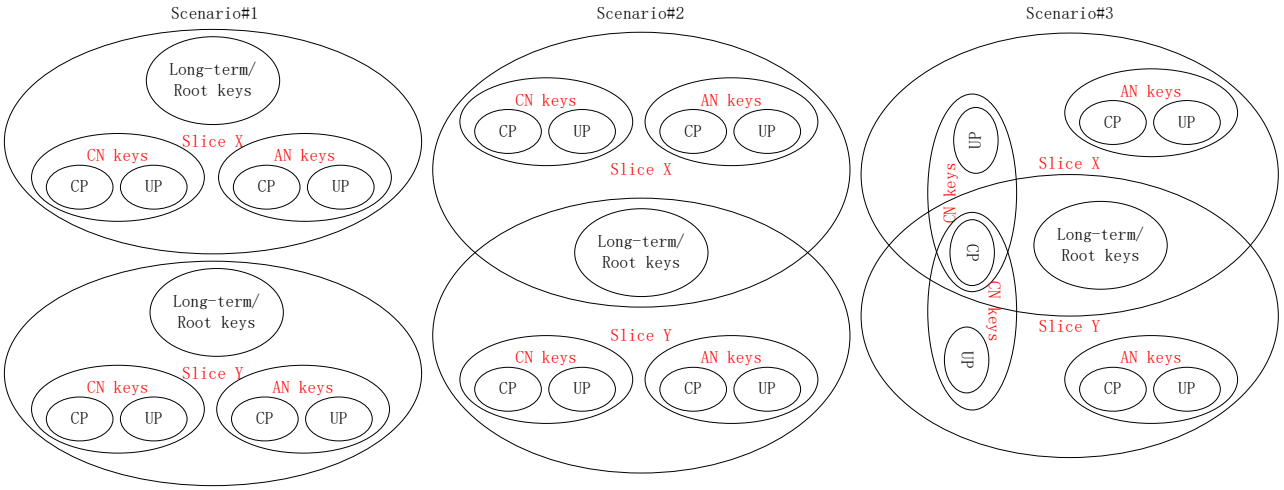


Figure 5.8.3.3-4

Scenario#1: No key is shared between slices.

Scenario#2: Long-term keys and root keys are shared between slices.

NOTE1: Intermediate keys may be partially or fully shared between slices for scenario#2.

Scenario#3: Long-term keys, root keys, and CN-CP keys are shared between slices.

NOTE2: Intermediate keys for deriving AN keys and CN-UP keys may be partially or fully shared between slices for scenario#3.

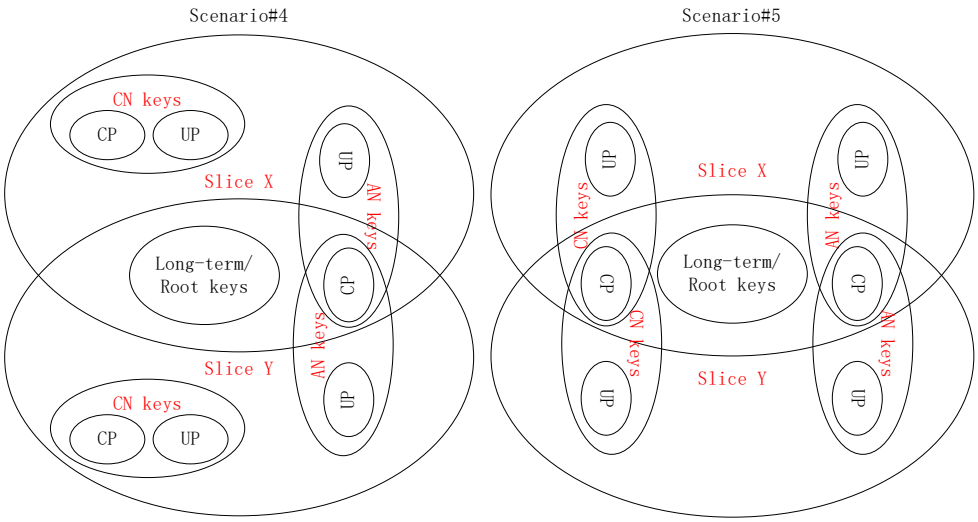


Figure 5.8.3.3-5

Scenario#4: Long-term keys, root keys, and AN-CP keys are shared between slices.

Lenovo Ex. 1007
Page 385

NOTE3: Intermediate keys for deriving CN keys and AN-UP keys may be partially or fully shared between slices for scenario#4.

Scenario#5: Long-term keys, root keys, CN-CP keys, and AN-CP keys are shared between slices.

NOTE4: Intermediate keys for deriving CN-UP and AN-UP keys may be partially or fully shared between slices for scenario#5.

5.8.3.3.2 Security threats

Data used for slice selection may be tampered or forged, which leads to an incorrect slice selection result so that UE cannot obtain service from a right slice or un-subscribed UE may be allocated to slices.

User's privacy information used in the network slice selection procedure may be intercepted or eavesdropped.

If UEs are not authenticated and authorized for their usage of a particular network slice, unauthorized UEs may get connected to the network slice and consume resources

If there is no proper authorization mechanism for service access, then this opens up for different types of attacks such as impersonation and denial of service. Impersonation attacks can lead to fraudulent charging and can potentially leak sensitive information on the victim UE. On a larger scale such as the massive IoT, efficient denial of service attacks could be mounted causing fast resource depletion and consequently loss of service, money and reputation.

If unprotected, an attacker eavesdropping on the access links can get hold of sensitive service or even access related information. In addition, a skilful attacker can hijack the ongoing session and inject his own data packets. The attacker can as well replay intercepted packets causing an unnecessary overload in the system that may affect availability and service quality.

5.8.3.3.3 Potential security requirements

- There shall be means to guarantee that the appropriate network slices are assigned to the appropriate subscriptions.
- The 3GPP System shall provide the capability to protect the authenticity, integrity and confidentiality of messages exchanged in the procedure of slice selection.
- There shall be means to prevent unauthorized UEs from gaining access to services.
- There shall be means to prevent authorized UEs from misusing their access rights.
- There shall be means to authenticate UEs for access authorization.
- There shall be means to secure the communication over the access link, that is, between the access network and the network slice over 3GPP and trusted non-3GPP accesses or between the UE and the network slice over untrusted non-3GPP accesses.

5.8.3.4 Key Issue #8.4: Security on sensitive network elements

5.8.3.4.1 Key issue details

There are some sensitive network elements which contain sensitive data or perform security related functions, e.g. HSS contains customers' profiles and their credentials. Security is a fundamental requirement of these sensitive elements. Slicing architecture can increase the risk of network elements getting attacks. Solutions for this key issue will study:

The type and form of sensitive network elements in slicing network;

The mechanism for protecting a sensitive network element.

5.8.3.4.2 Security threats

Editor's Note: Proposed security threats description is "Slicing architecture can increase the risk of network elements getting attacks. For example, virtualization can lead to lack of physical boundary protection and sensitive NEs located in every slice may increase the attack interfaces".

Lenovo Ex. 1007
Page 386

5.8.3.4.3 Potential security requirements

- Sensitive network elements should be protected from other entities.

Editor's Note: It is FFS how to define other entities.

5.8.3.5 Key Issue #8.5: Security on management of slicing

Editor's Note: It should be clarified with SA2 and SA5 which are (if any) the interfaces used for the management of network slices and whether they are in scope of SA3. The same applies to Key Issue #8.6.

5.8.3.5.1 Key issue details

The 3GPP system provides capabilities for operators to manage slices e.g. set parameters for resource sharing or dynamically create network slice. The capabilities should be under control of authorized operators.

5.8.3.5.2 Security threats

Attackers may illegally obtain capabilities to manage slices or on-going services and launch attacks to slices (e.g. terminate a slice or compromise a critical network function).

5.8.3.5.3 Potential security requirements

- The capabilities to manage network slices should be under control of authorized operators.

5.8.3.6 Key Issue #8.6: Security on interacting with third party

5.8.3.6.1 Key issue details

The 3GPP systems provide capabilities for authorized third parties to create, manage a network slice configuration (e.g. scale slices) via suitable APIs. These interfaces can be utilized to launch attacks by unauthorized third parties.

5.8.3.6.2 Security threats

Attackers may utilize 3rd party APIs to attack slices.

5.8.3.6.3 Potential security requirements

- The APIs should be accessed by authorized third parties.

5.8.3.7 Key Issue #8.7: Security of inter slice communications

5.8.3.7.1 Key issue details

There are different network slices, default network slice or dedicated network slices for particular tenants and application specific network slices hosting whole network functions or network slices hosting only dedicated functions. When network slices implement dedicated network functions, inter slice communications are inevitable. Between default network slice and other network slices, there is signalling involved. Between RAN network slices and core network slices there is signalling and traffic plane involved. In all inter network slice communications it is necessary to protect the interface against any attacks.

Editor's Note: Further explanations are required about inter slice communication.

5.8.3.7.2 Security threats

The interface between network slices can be attacked and functionality of network slices could be hampered if inter slice communication is not protected. Attacks on the control plane at the inter slice interface can hijack the communication of one or more UEs. It may be possible to make the whole network slice dysfunctional or manipulate it to behave in a different way than it is intended. Thus, it may have serious consequences to the service if the interfaces

Lenovo Ex. 1007
Page 387

are not protected. Attacks on the user plane can destroy the user traffic or divert the user traffic served by the network slice affecting one or more or group of UEs.

5.8.3.7.3 Security requirements

- Inter network slice interaction needs to be secured maintaining the sanctity of restrictions of the slice.
- Interfaces between the network slices need to be protected similar to the current Network Domain Security.
- Inter network slice interfaces and communication should be protected based on the sensitivity level of the network slice functions and the requirement of the network tenant.

Editor's Note: sensitivity level of network slice functions need to be defined.

5.8.3.8 Key Issue #8.8: Virtualization security

Editor's Note: It is FFS whether security in virtualization is in scope of 3GPP.

5.8.3.8.1 Key issue details

The Virtualization Security identifies the key issues related to the adoption of virtualisation technology in the Next Generation Network to identify the security mechanisms, which need to be supported to ensure for example, traffic segregation, control of the allocated Virtual Network Functions (VNF) and limitation of their reachability/visibility.

In particular this security area deals with concerns such as:

- Lack of logical and physical isolation between distinct VNF hosted by the same hypervisor
- Lack of authentication between network virtual functions
- DoS effects, e.g. starvation of resources allocated to virtual network functions or network slices,
- Integrity of hypervisor and hosted VNFs.

5.8.3.8.2 Security threats

TBA

5.8.3.8.3 Security requirements

TBA

5.8.3.y Key issue #8.y: <key issue name>

5.8.3.y.1 Key issue details

5.8.3.y.2 Security threats

5.8.3.y.3 Potential security requirements

5.8.4 Solutions

5.8.4.1 Solution #8.1: Security isolation of network slices, Security mechanism differentiation

5.8.4.1.1 Introduction

This solution addresses several key issues of #8.1 Security isolation of network slices and #8.2 Security mechanism differentiation for network slices.

Lenovo Ex. 1007
Page 388

5.8.4.1.2 Solution details

As a prerequisite the UE must be preconfigured with the slice IDs to be used and those must match to the ones configured in the network. The Slice Security Server (SSS) is a repository for the different slice security requirements and provides those to the HSS on request for selecting the appropriate security algorithm per slice. The SSS may be collocated with the HSS.

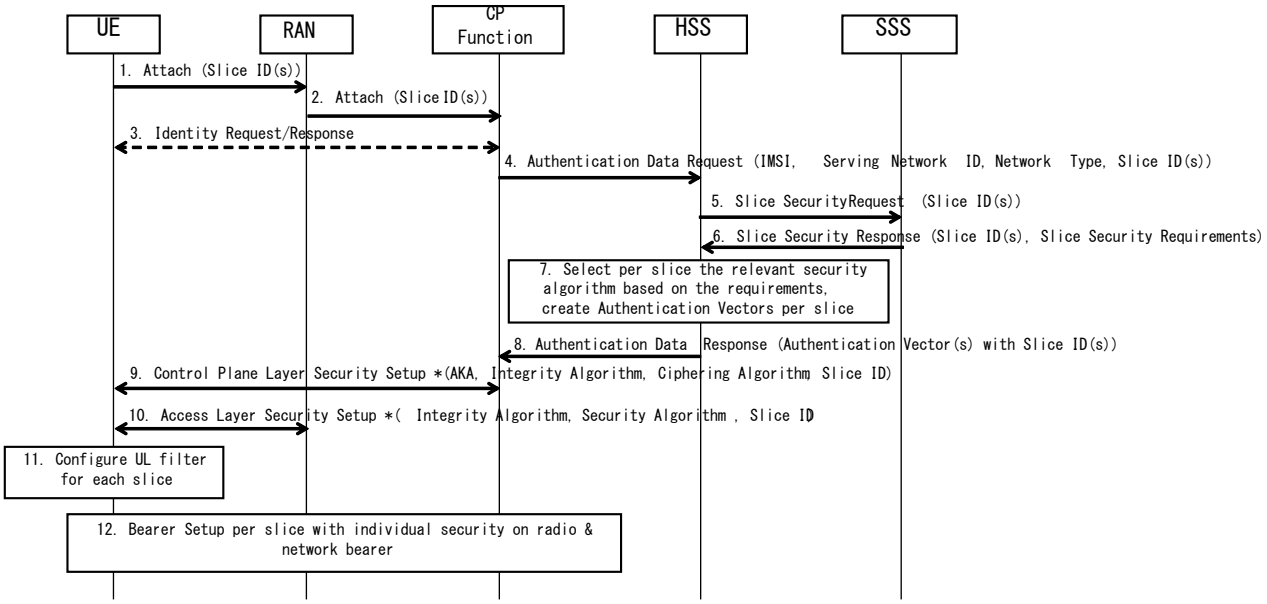


Figure 5.8.4.1.2-1 Attach Procedure with one RRC connection for all slices

Step 1: The UE sends an Attach Request to the RAN including a list of all desired slice IDs.

Step 2: The RAN selects the CP Function and forwards the Attach Request including the list of slice IDs.

Step 3: The CP Function may request the UE identifier.

Step 4: The presence of the slice ID list is indicating the CP Function the UE capability to handle several slices with different security requirements. The CP Function requests the Authentication Data from the HSS and includes the list of requested slice IDs, if available. The CP Function may further check based on the subscription profile whether the UE is eligible to access to the network slice(s) associated with the list of slice IDs.

Step 5: The HSS sends a Slice Security Request to the SSS including the slice ID list received from the CP Function. If no slice IDs are indicated in the message from the CP Function, then the HSS checks the subscription profile whether the terminal subscribed to any specific services that require special treatment and includes them (i.e. subscribed slice IDs) in the request to the SSS.

Step 6: The SSS provides the security requirements per slice ID. The security requirements could already indicated the algorithm to be used or indicate a level, e.g. high security, middle security, low security, or they could point to a predefined security profile out of a set of predefined profiles. Those predefined security profiles could be available in all network nodes, i.e. known to all CP Functions and RAN nodes, HSS etc., so that only a pointer to the profile ID is required in the security requirements.

Step 7: According to the received security requirements, the HSS executes the security procedures per slice and selects the corresponding security algorithms per slice. The HSS may take the UE capabilities into account as well as the operator policies. Under the security procedures, the HSS creates individual Authentication Vectors per slice and creates a binding with the corresponding slice IDs. Step 8: The HSS sends the set of Authentication Vectors and slice IDs to the CP Function in the Authentication Data Response.

Step 9: The CP Function sets up the Control Plane layer security per slice and performs authentication and key agreement (AKA). The messages may not belong to any slice and shall contain the UE security capabilities and per slice ID the selected algorithms for ciphering and integrity, or the security profile ID. The UE verifies the integrity of the message from the CP Function and starts integrity protection and ciphering/deciphering with this security context and sends an acknowledgement message to CP function ciphered and integrity protected.

Lenovo Ex. 1007
Page 389

Step 10: The RAN sets up the radio access layer security for user plane and control plane and sends the selected algorithms for integrity and ciphering per slice.

Step 11: The UE configures the uplink filters in order to map uplink traffic from the application to the right Data Radio Bearers (DRB) on the corresponding slices.

Step 12: The UE finalizes the bearer setup per slice towards the User Plane Function with individual security.

If a UE would like to attach to a slice not included in the ATTACH request of step 1, then the UE would be required to send another ATTACH request with the slice ID it would like to be attached to. The CP Function detects that the UE is already attached to the network and would not perform authentication with the UE, but still query the SSS for the security requirements of the slice and slice authorization.

Editor's note: The solution needs to describe the behaviour of the system when a mismatch occurs between the network slice ID requested by the UE and those available in the network.

Editor's note: Privacy aspects related to the network slice ID are FFS.

Editor's note: The solution needs to describe how the roaming scenarios are handled.

Editor's note: Security profile ID role and definition are to be described. Furthermore, it is unclear which entity of the NextGen system this security profile ID is related to.

Editor's note: It's FFS to consider the detailed procedures and interface between HSS and SSS, including how the UE is authenticated if the UE doesn't include the list of requested slice IDs in Step4, how to provision all security nodes with security profiles for all network slices, in Step 6 and how to support a RAN network slice in Step 10.

Editor's note: It's FFS to consider the case when legacy UEs without any awareness of network slicing would access the next generation network with network slicing.

Editor's note: It's FFS whether the security procedures are executed by HSS in Step 7.

5.8.4.1.3 Evaluation

FFS

5.8.4.2 Solution #8.2: UE Authentication only by AUSF

5.8.4.2.1 Introduction

This solution addresses key issue #8.3. It assumes that AUSF only has interface with ARPF (equivalent to HSS in LTE)

5.8.4.2.2 Solution details

To describe the UE Authentication by AUSF, we propose a possible procedure, which is compatible to the Network Slice Architectures in clause 6.1.1, 6.1.2, and 6.1.3 of TR 23.799

Lenovo Ex. 1007
Page 390

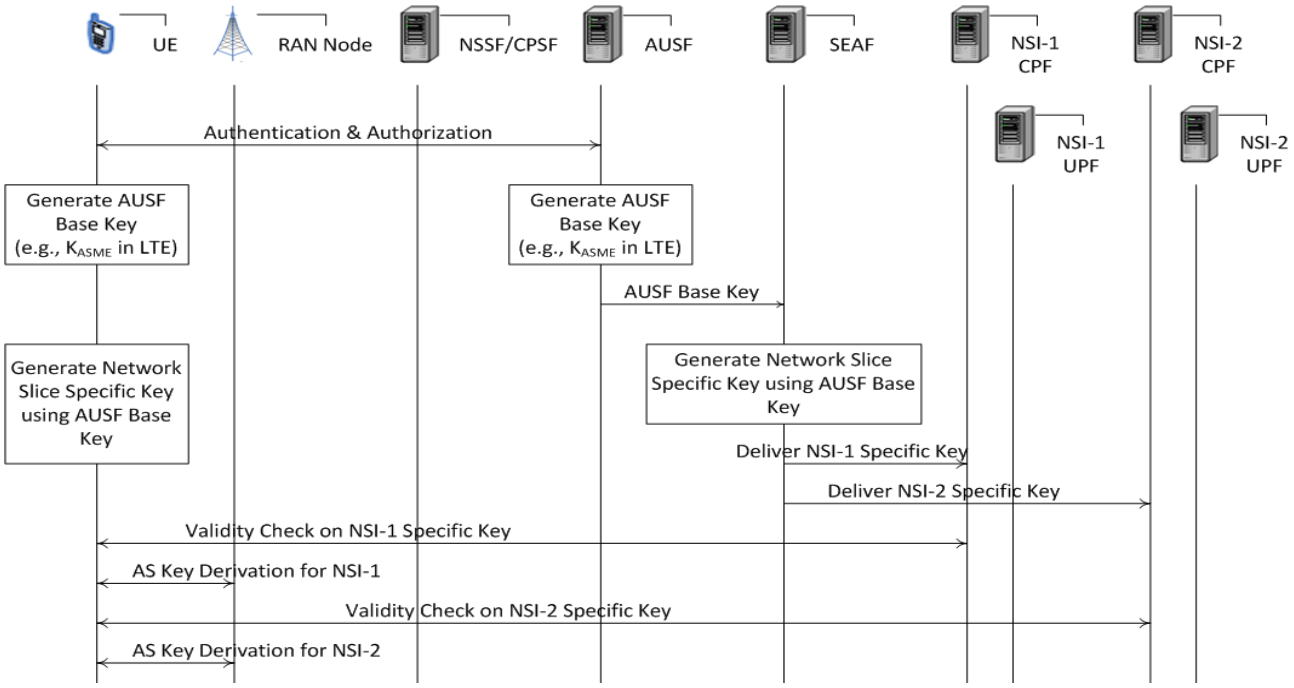


Figure 5.8.4.2.2-1: UE Authentication by AUSF

1. UE and AUSF perform mutual authentication.

2. UE and AUSF derive AUSF Base Key. (AUSF Base Key indicates a key corresponding to the K_{ASME} in LTE)

Editor's note: How the AUSF Base Key is derived is FFS.

3. AUSF provides AUSF Base Key to SEAF.

4. SEAF generates NSI-specific keys using AUSF Base Key and sends it to each NSI. UE also derives NSI-specific keys in the same way as in SEAF. NSI-specific keys can be derived using the AUSF Base Key and NSI specific information such as Network Slice ID, etc.

Editor's note: It is assumed that the Network Slice ID is preconfigured in UE as part of the parameters consisting NSSAI (Network Slice Selection Assistance Information). The set of parameters of NSSAI may be defined based on the SA2 discussions on Network Slicing.

5. UE and NSI-1perform the mutual validity check on NSI-1 specific key and then derives AS (Access Stratum) key respectively. The validity check on NSI-1 specific key can be performed during the session establishment toward NSI-1. For the mutual validity check on NSI-1 specific key, UE and NSI-1 can calculate and verify the message authentication code for NSI-1 specific key respectively. During the session establishment, UE can also provide its own security capability (security algorithms, etc) to NSI-1. Based on the information, NSI-1 can decide the proper security configuration (e.g., security algorithm, key size, etc) and send it back to UE. UE can then use such information for AS key derivation for NSI-1.

6. UE and NSI-2 perform the mutual validity check on NSI-2 specific key and then derives AS (Access Stratum) key respectively. The validity check on NSI-2 specific key can be performed during the session establishment toward NSI-2. For the mutual validity check on NSI-2 specific key, UE and NSI-2 can calculate and verify the message authentication code for NSI-2 specific key respectively. During the session establishment, UE can also provide its own security capability (security algorithms, etc) to NSI-2. Based on the information, NSI-2 can decide the proper security configuration (e.g., security algorithm, key size, etc) and send it back to UE. UE can then use such information for AS key derivation for NSI-2.

Editor's note: How the AS Key is derived is FFS.

Editor's note: AUSF in this solution corresponds to AU in 6.1.1 and 6.1.3, and Authentication & Authroization in 6.1.2 of TR 23.799 [2].

Lenovo Ex. 1007
Page 391

5.8.4.3.3 Evaluation

5.8.4.3 Solution #8.3: UE Authentication by AUSF and NSI

5.8.4.3.1 Introduction

This solution addresses key issue #8.3. It assumes that AUSF and NSI has interface with ARPF (equivalent to HSS in LTE).

Editor's note: Whether AUSF and NSI has interface with the same ARPF or not is FFS.

5.8.4.3.2 Solution details

To describe the UE Authentication by AUSF and NSI, we propose a possible procedure, which is compatible to the Network Slice Architectures in clause 6.1.1, 6.1.2, and 6.1.3 of TR 23.799 [2].

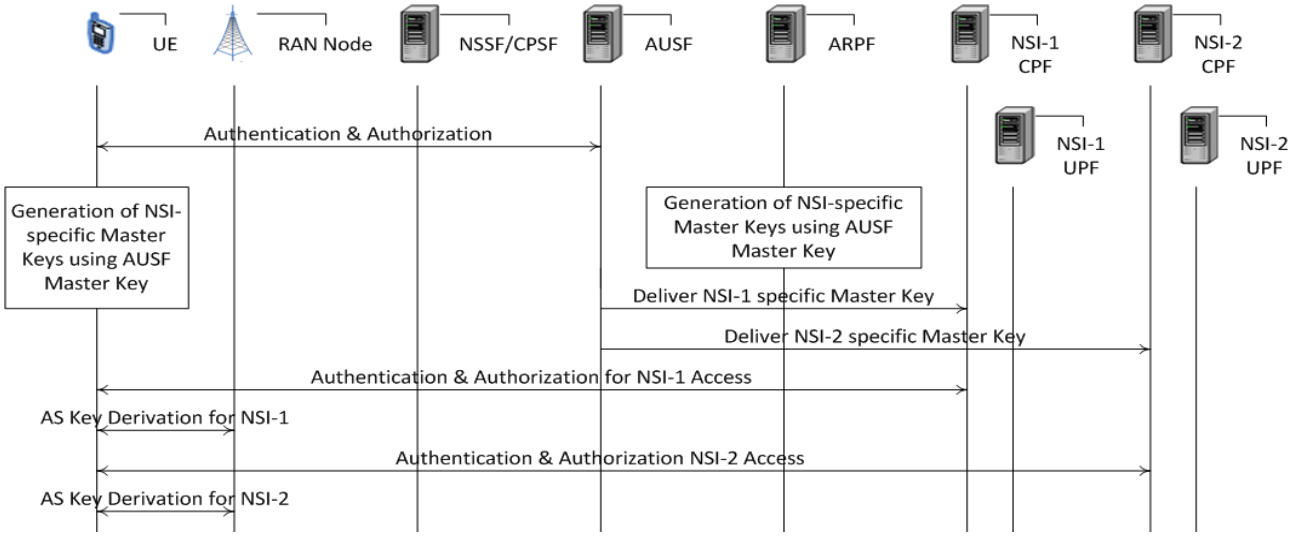


Figure 5.8.4.3.2.1: UE Authentication by AUSF and NSI

1. UE and AUSF perform mutual authentication for Network Access.
2. UE and AUSF derive AUSF Base Key. (AUSF Base Key indicates a key corresponding to the K_{ASME} in LTE)

Editor's note: How the AUSF Base Key is derived is FFS.

3. ARPF generates NSI-specific Master Keys using ARPF Master Key and sends it to each NSI via AUSF. (ARPF Master Key indicates a key corresponding to the K_i in LTE) UE also derives NSI-specific Master Keys in the same way as in ARPF. NSI-specific Master Keys can be derived using the ARPF Master Key and NSI specific information such as Network Slice ID, etc.

Editor's note: It is assumed that the NSI-specific Master Key is derived and sent to each NSI by ARPF since the Master Key (e.g., K_i in LTE) is stored and used for authentication only in ARPF.

Editor's note: It is assumed that the Network Slice ID is preconfigured in UE as part of the parameters consisting NSSAI (Network Slice Selection Assistance Information). The set of parameters of NSSAI may be defined based on the SA2 discussions on Network Slicing.

4. UE and NSI-1perform mutual Authentication for Slice Access and then derives AS (Access Stratum) key respectively. The mutual authentication can be performed during the session establishment toward NSI-1. As a result of successful authentication, UE and NSI-1 can derive the intermediate key for AS key derivation. During the session establishment, UE can also provide its own security capability (security algorithms, etc) to NSI-1. Based on the information, NSI-1 can decide the proper security configuration (e.g., security algorithm, key size, etc) and send it back to UE. UE can then use such information for AS key derivation for NSI-1.
5. UE and NSI-2perform mutual Authentication for Slice Access and then derives AS (Access Stratum) key respectively. The mutual authentication can be performed during the session establishment toward NSI-2. As a

Lenovo Ex. 1007
Page 392

result of successful authentication, UE and NSI-2 can derive the intermediate key for AS key derivation. During the session establishment, UE can also provide its own security capability (security algorithms, etc) to NSI-2. Based on the information, NSI-2 can decide the proper security configuration (e.g., security algorithm, key size, etc) and send it back to UE. UE can then use such information for AS key derivation for NSI-2.

Editor's note: How the AS key is derived is FFS.

Editor's note: AUSF in this solution corresponds to AU in 6.1.1 and 6.1.3, and Authentication & Authroization in 6.1.2 of TR 23.799 [2].

Editor's note: It is assumed that the Authentication for Slice Access is tied to the SM (Session Management) Function (e.g., during the session establishment). How the result of authentication, e.g., NSI-specific keys, can be provided to the MM (Mobility Management) Function is FFS.5.8.4.3.3 Evaluation

5.8.4.4 Solution #8.4: UE Authentication by NSI

5.8.4.4.1 Introduction

This solution addresses key issue #8.3. It assumes that NSI has interface with User Profile Repository (equivalent to HSS in LTE).

Editor's note: Whether different NSIs have interface with the same User Profile Repository or not is FFS.

5.8.4.4.2 Solution details

To describe the UE Authentication by NSI, we propose a possible procedure, which is compatible to the Network Slice Architectures in clause 6.1.1, 6.1.2, and 6.1.3 of TR 23.799 [2].

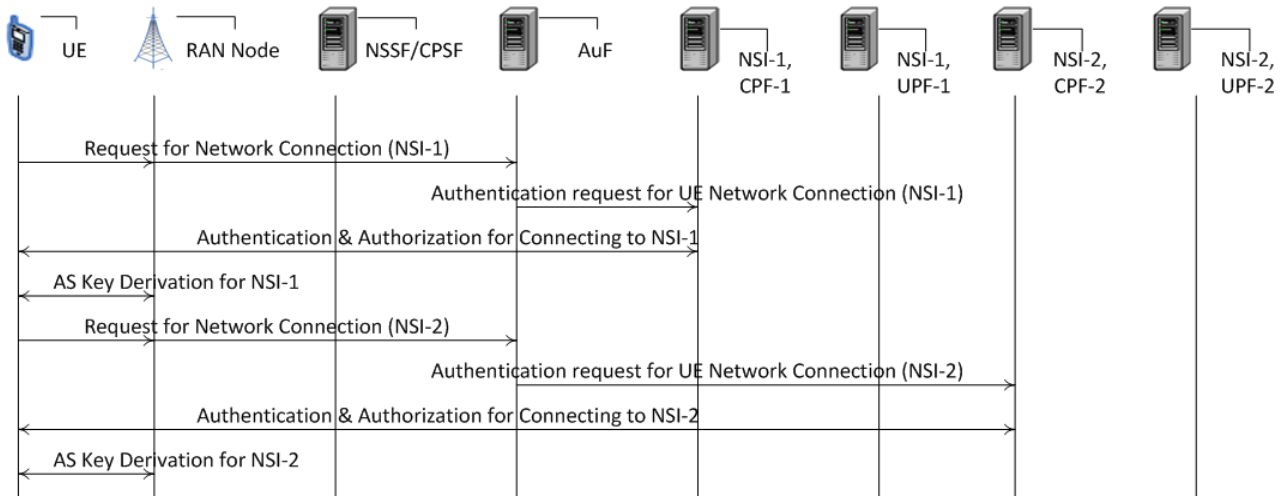
1. UE requests network connection for NSI-1 to AuF.
2. AuF forward the network connection request for authentication toward NSI-1 access toward NSI-1.
3. UE and NSI-1 perform mutual authentication and derives AS (Access Stratum) key respectively.

Editor's note: How the AS Key is derived is FFS.

4. UE requests Network Connection for NSI-2 to AuF.
5. AuF forward the UE network connection request for authentication toward NSI-2 access toward NSI-2.
6. UE and NSI-2 perform mutual authentication and derives AS (Access Stratum) Key respectively.

Editor's note: How the AS Key is derived is FFS.

Editor's note: AuF in this solution corresponds to AU in 6.1.1 and 6.1.3, and Authentication & Authroization in 6.1.2 of TR 23.799 [2].



Lenovo Ex. 1007
Page 393

Figure 5.8.4.4.2-1: UE Authentication by AuF and NSI

5.8.4.4.3 Evaluation

5.8.4.5 Solution #8.5: UE access network and slices

5.8.4.5.1 Introduction

This solution addresses key issue #8.3 Security on UEs' access to slices and #8.2 Security mechanism differentiation for network slices.

SA2 introduces a solution (clause 6.1.2 of TR 23.799) for network slicing architecture as following:

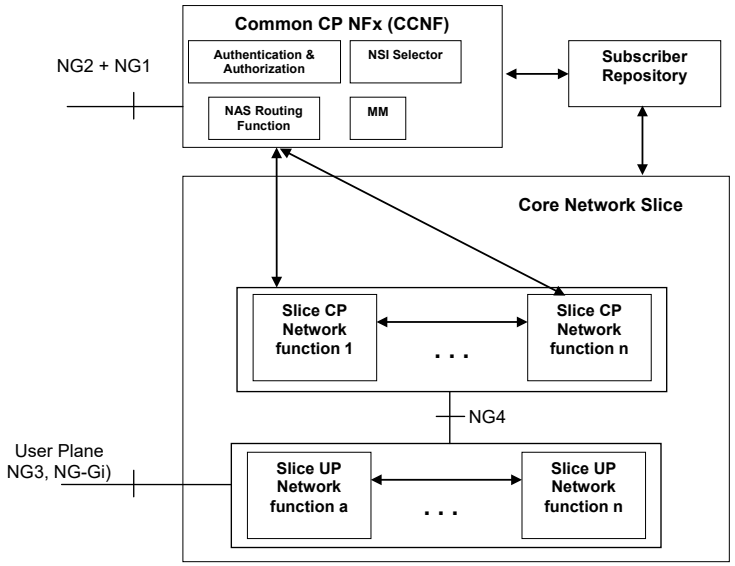


Figure 5.8.4.5.1-1: Core Part of Network Slicing concept

The Network Slice Architecture in clause 6.1.2 of TR 23.799 assumes that NG-UE can only simultaneously access multiple CN slice instances via a single CCNF, which is indicated by Temporary ID. And in clause 6.1.2.2.3.1 and clause 6.1.2.2.3.2 of TR 23.799, the initial access procedure and subsequent NAS signalling (generic) are depicted as following:

Lenovo Ex. 1007
Page 394

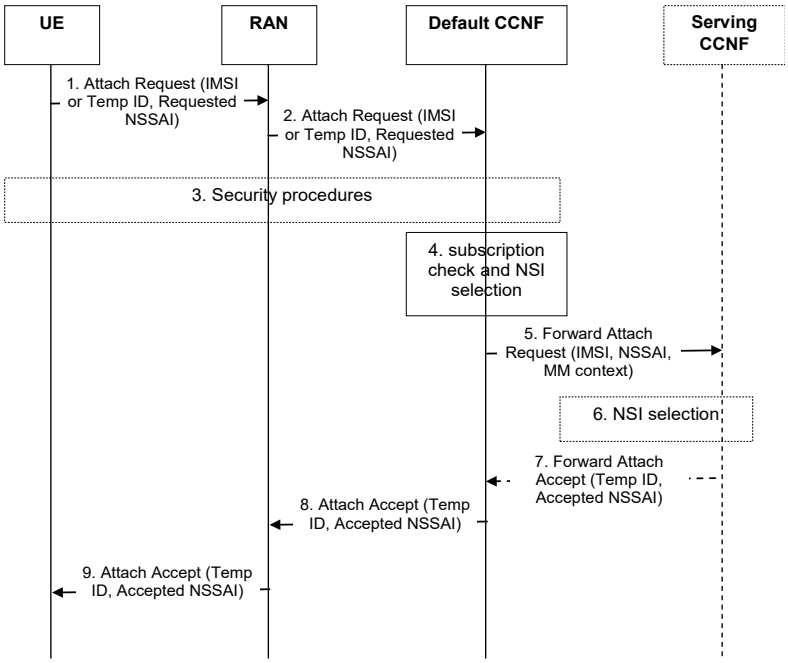


Figure 5.8.4.5.1-2: Initial Access

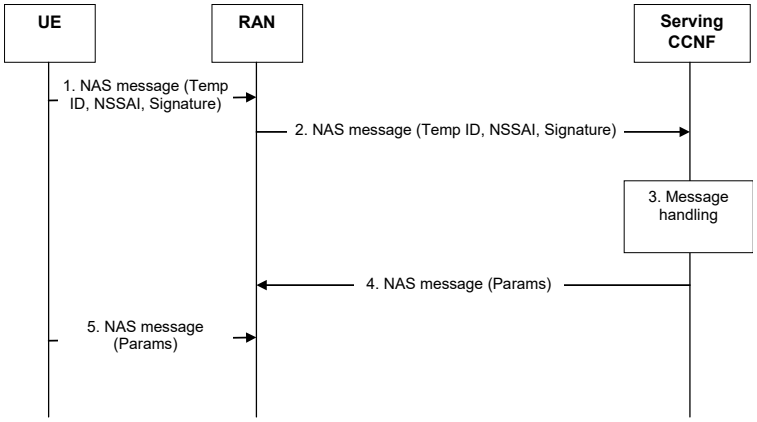
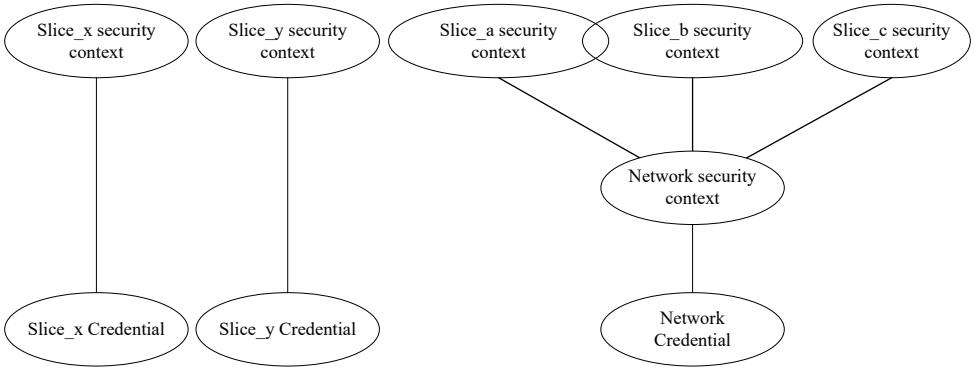


Figure 5.8.4.5.1-3: Subsequent NAS Network Slicing Procedures

The security procedure such as authentication procedure and NAS SMC procedure need to be updated, and the handling of signature needs to be defined.

5.8.4.5.2 Solution details

This solution is compatible to the Network Slice Architecture in clause 6.1.2 of TR 23.799. The following figure 5.8.4.5.2-1 shows the relationship of security contexts per UE:



Lenovo Ex. 1007
Page 395

Figure 5.8.4.5.2-1 Relationship of security contexts per UE

The security context has CN part and AN part, and each part has intermediate keys (e.g. Kasme or Kenb in LTE), CP keys (keys for integrity and confidentiality for C-Plan), and UP keys (keys for integrity and confidentiality for U-Plan).

5.8.4.5.2.1 Attach procedure

Following figure 5.8.4.5.2.1-1 shows the attach procedure for UE access network and slices:

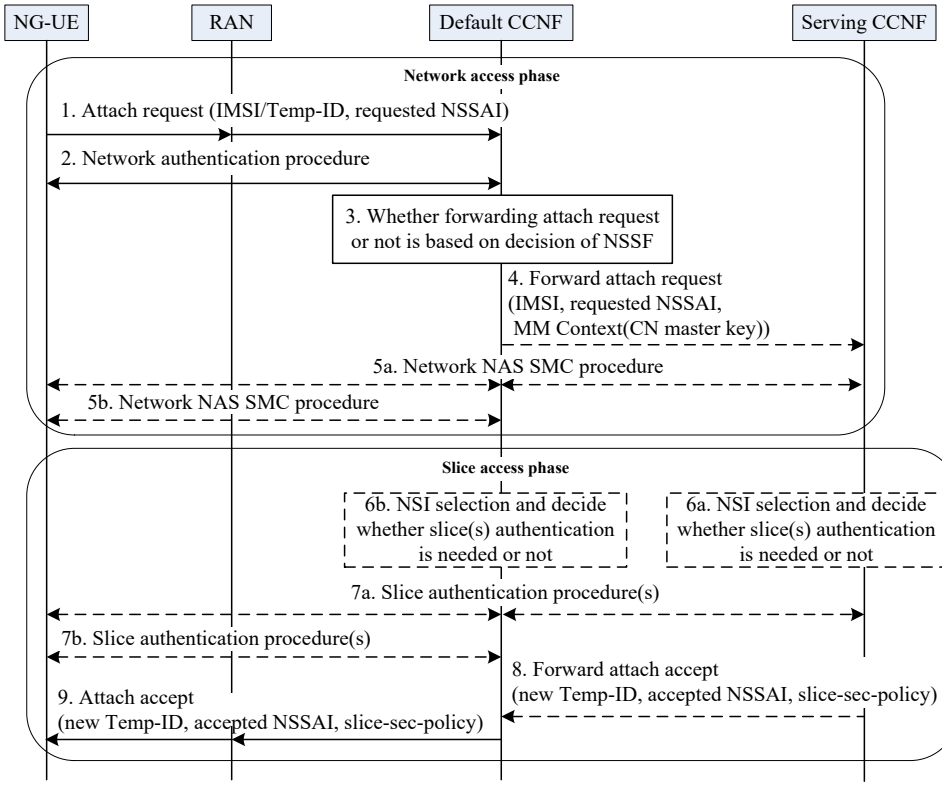


Figure 5.8.4.5.2.1-1 Attach procedure

Step 1: The NG-UE sends an Attach Request (IMSI/Temp-ID, requested NSSAI) message to the RAN, carrying IMSI if Temp-ID is not available, or Temp-ID if available. NSSAI is network slice selection association information. RAN forwards the attach request to the Default CCNF.

Step 2: The Default CCNF performs network authentication procedure with the NG-UE. If authentication is successful, then continue, otherwise, stop.

Step 3: The Default CCNF determines whether to forward the attach request to a Serving CCNF or not based on the decision of the network slice selection function (NSSF). If not, Default CCNF becomes Serving CCNF and skip step 4, and proceed to 5b, 6b and 7b.

Step 4: The Default CCNF sends a Forward Attach Request (IMSI, requested NSSAI, MM Context) message to the Serving CCNF. The MM Context includes CN master key (similar as Kasme in LTE), proceed to 5a, 6a and 7a.

Step 5a/b: The Serving CCNF performs network NAS SMC procedure, i.e. Security Mode Command does not include slice information. The NG-UE and the Serving CCNF derive CN keys of the network security context per the NG-UE. The following NG1 messages will be integrity and confidentiality protected with the network security context.

Step 6a/b: Based on the security mechanism policy of the slice(s) selected by the NSSF, the Serving CCNF determines whether slice authentication procedure(s) are needed or not. If not, then continuing to step 8 or 9 based on whether the attach request is forwarded or not

Step 7a/b: The Serving CCNF performs optional slice authentication procedure(s) with the NG-UE (e.g. the selected slice(s) have a dedicated AAA).

Lenovo Ex. 1007
Page 396

Step 8: If the Serving CCNF received the attach request which is forwarded by the Default CCNF as described in step 4 above, then the serving CCNF sends a Forward Attach Accept (new Temp-ID, accepted NSSAI, slice-sec-policy) message to the Default CCNF of which the new Temp-ID is assigned by the Serving CCNF.

Step 9: The CCNF sends/relays an Attach Accpet (new Temp-ID, accepted NSSAI, slice-sec-policy) message to the NG-UE. The slice-sec-policy indicates how to derive slice specific keys per the NG-UE, it includes information that whether a slice specific key needs to be derived and corresponding derivation parameter, and it may indicate length of keys per slice, and so on.The slice security context(s) per the NG-UE for the selected slice(s) are not available at this moment, i.e. keys for integrity and confidentiality protection per slice are not generated.

5.8.4.5.2.2 Subsequent NG1 signalling with NAS SMC procedure (generic)

When NG-UE initiates a NG1 signalling, NAS SMC procedure may need to be performed. Following figure 5.8.4.5.2.2-1 shows the subsequent NG1 signalling with NAS SMC procedure flow:

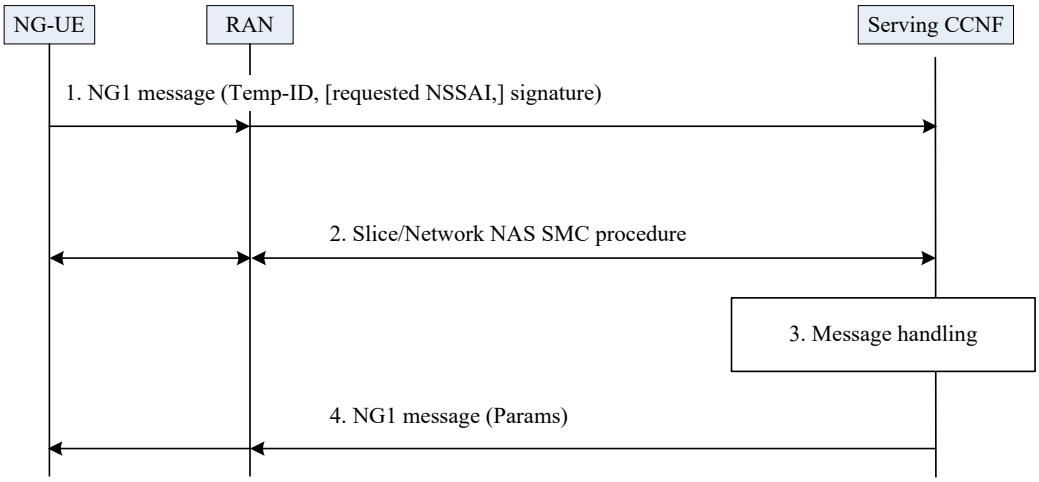


Figure 5.8.4.5.2.2-1 Subsequent NG1 signalling with NAS SMC procedure

Step 1: The NG-UE sends a NG1 message (Temp-ID, [requested NSSAI,] signature). The requested NSSAI is included if a specific NSI or a set of NSI(s) need to be addressed by the NAS procedure. If the procedure is not slice-specific, the requested NSSAI may not be included. If the requested NSSAI indicates a specific slice, and CN-CP integrity key for the specific slice are derived, then the signature is generated using the slice security context relate to the specific slice, otherwise, the signature is generated using the network security context. The message is routed by RAN to a proper Serving CCNF.

Step 2: The Serving CCNF verifies that the NG1 message is using the rule for handling signature as indicated in step 1, and determines the selected slices based on the requested NSSAI.

A) If there're some selected slices, then the slice SMC procedure is performed, i.e. the Security Mode Command additionally includes information of the selected slices (e.g. accepted NSSAI/NSIs, and algorithms per slice);

   a). If there's only one selected slice, the Security Mode Complete is protected using slice security context related to the selected slice;

   b). Otherwise, the Security Mode Complete is protected using network security context;

B) Otherwise, the network SMC procedure is performed.

Step 3: The Serving CCNF handling the NG1 message.

Step 4: The Serving CCNF sends a NG1 message (params) to the NG-UE. If there's only one selected slice, then information of the selected slice (e.g. accepted NSSAI/NSI) is included in the underlayer NG2 message, and the NG1 message is integrity and confidentiality protected by the slice security context related to the selected slice, otherwise, information of selected slices (e.g. accepted NSSAI/NSIs) may be included in the underlayer NG2 message, and the NG1 message is integrity and confidentiality protected by the network security context.

Lenovo Ex. 1007
Page 397

5.8.4.5.3 Evaluation

FFS

5.8.4.6 Solution#8.6: UE authentication and initial attach to a network slice using NSSAI

This solution presents UE authentication and initial attach to a network slice using the NSSAI presented by the UE.

NOTE 1: This security solution described here addresses the SA2 network slice solution 6.1.2 in TR 23.799.

The call flow and steps are described below.

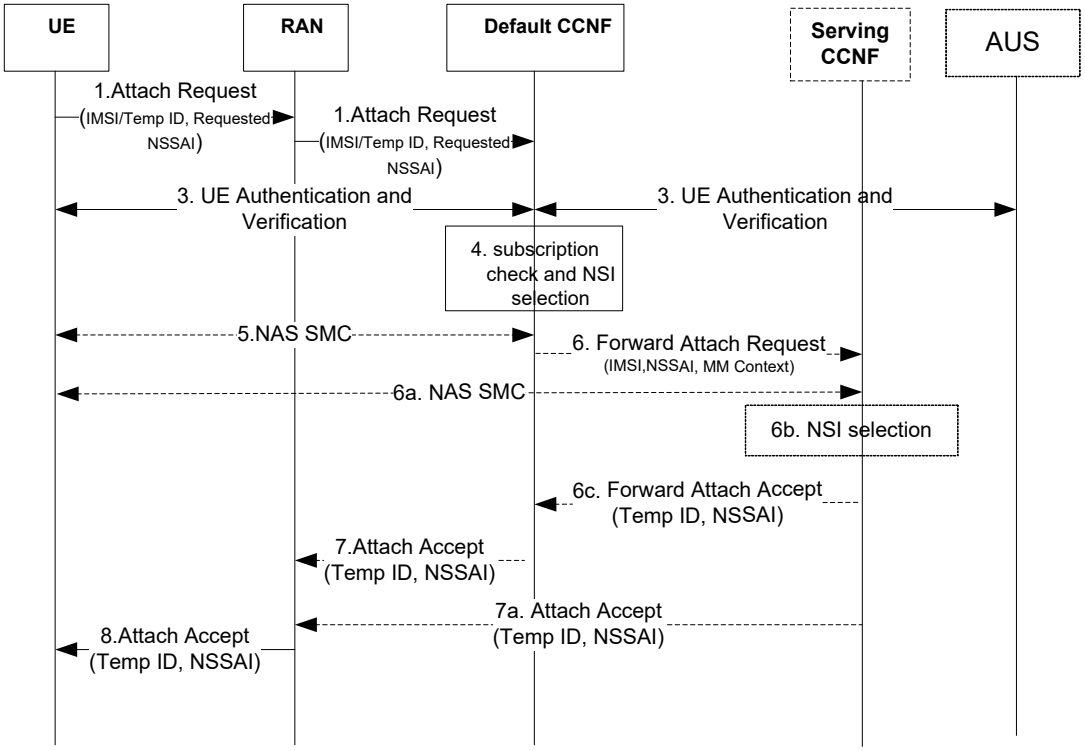


Figure 5.8.4.6-1

1. The UE sends an Attach Request message including the IMSI if a Temporary ID for the UE is not available. If temporary ID is available, the UE includes it, and the RAN routes the message to a suitable handler in the core.

   The UE requests one or a set of slices by including a requested NSSAI. The NSSAI would be used in the RRC layer to enable the access to a suitable RAN resources.

2. The RAN forwards the Attach Request to the Core based on the routing criteria. If the IMSI is present, a default CCNF is selected. If the Temporary ID is available for the selected PLMN, the corresponding CCNF is selected by the RAN for routing the Attach Request.

3. The CCNF/SEAF proceeds with the Authentication of the UE. In the Initial Attach scenario with IMSI, the CCNF requests Authentication of the UE with the Authentication Server (AUS). The default CCNF completes the authentication and verification of the UE.

Editor's Note: Derivation of NAS specific keys with network slice isolation is FFS.

4. After successful UE authentication, its subscription data is checked and the CCNF is verified if it is an appropriate handler for the UE. If not, this step is skipped and continues to step 6. The CCNF decides the initial set of Network Slice Instances (NSI(s)) for the UE based on an evaluation of the Requested NSSAI, subscribed

Lenovo Ex. 1007
Page 398

NSSAI, UE capabilities, UE's subscription policy, UE's serving RAN type etc.
- if the UE did not provide a NSSAI, the network assigns the UE to the default NSI (s)
- if the UE did provide the a NSSAI, the network assigns the UE to the NSI(s) that the UE is authorized to use among the requested NSI(s).

Editor's Note: It is FFS whether the default CCNF does the NSI selection at this step.

5. The default CCNF initiates NAS Security Mode command and instantiates NAS security context. The default CCNF functions as the anchor for the NAS messages even after network slice is selected and assigned. If the UE is forwarded to a serving CCNF, this step does not happen. The procedure continues from step 7.

6. If the UE is not suitably handled by the (default) CCNF where the Attach Request was routed to, this CCNF may redirect the UE to a new Serving CCNF that is more optimal (or less loaded) for the selected slices. The default CCNF forwards the attach request to the new Serving CCNF with an indication that it is a forwarded attach together with IMSI , the MM context , NSSAI etc in order to indicate that the UE has been authenticated for NSI(s) Assignment as described in step 4. (If the UE is not forwarded to a serving CCNF, this step doesn't happen.)

Editor's Note: Any Network Slice specific UE authentication or 3rd party authentication is FFS.

6a. The serving CCNF initiates NAS Security Mode command and instantiates NAS security context. (If the UE is not forwarded to a serving CCNF, this step doesn't happen.).

NOTE 2: in this step the new CCNF includes in the transport layer message it received.

6b. The Selected Serving CCNF performs the NSI selection as described in step 4 above.

6c. The serving CCNF acknowledges the default CCNF that the UE forward request has been accepted and UE has been assigned a network slice. The procedure continues from step 7a.

7. The default CCNF responds to the UE with Attach Accept message to the RAN node. Assigned Temp ID, assigned NSSAI, any vectors specific to the network slice etc are sent to the UE. The procedure continues from step 8.

7a. If the UE was forwarded to a serving CCNF, the serving CCNF would send the UE with the Attach Accept message to the RAN node.

Editor's Note: Redirection of NAS from the default CCNF to the serving CCNF and informing it to the UE and RAN nodes are FFS.

8. The RAN node forwards the Attach Accept received in step 7 or 7a to the UE.

5.8.4.7 Solution #8.7: Security architecture for network slice

5.8.4.7.1 Introduction

This solution addresses Key Issue #8.3: Security on UEs' access to slices. It assumes that UE is authenticated and authorized by the MNO and the slice may perform slice authentication and/or authorization in a network slice instance. In this case a corresponding security function shall be designed for this purpose.

Editor's note: The assumption that every slice contains an instance of the SEAF should be checked against the latest agreements on the SA2 architecture.

5.8.4.7.2 Solution details

5.8.4.7.2.1 Architecture

This solution describes a high level security architecture that supports network slicing. The relationship between the network functions and the UE functions for the security architecture for network slicing is described in figure 5.8.4.7.2.1-1.

Editor's note: The security architecture for network slicing should be checked against the latest agreements on the SA2 architecture.

Lenovo Ex. 1007
Page 399

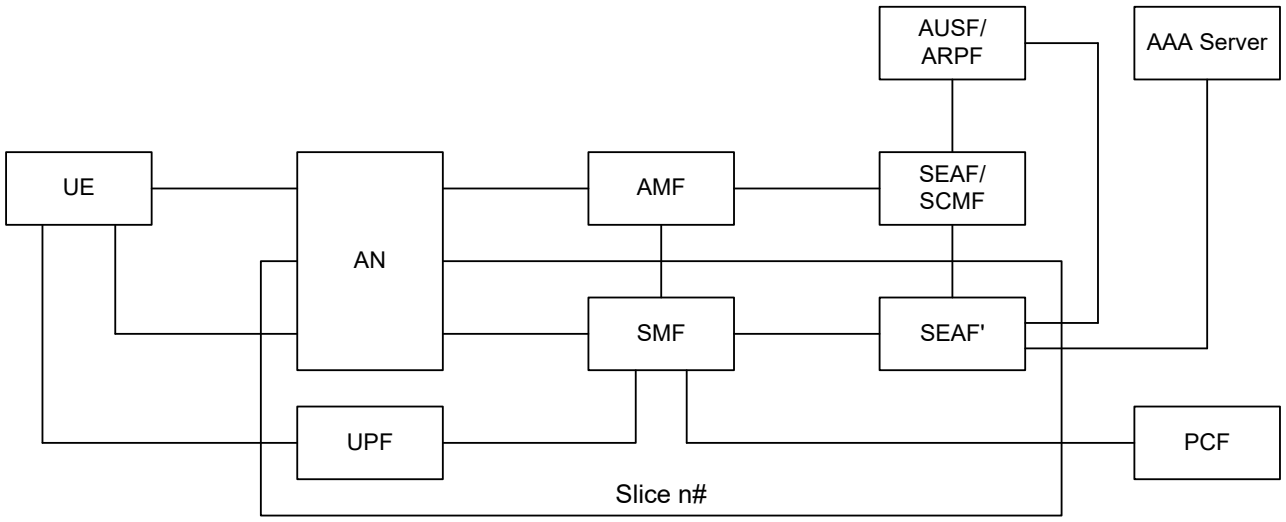


Figure 5.8.4.7.2.1-1: Security architecture for network slicing

Besides the functions defined in clause 5.2.1.2, the new defined or redefined functions are described as follows:

Security Anchor Function (SEAF)

Besides the functions defined in clause 5.2.1.2, the SEAF also interacts with the Security Anchor Function' (SEAF') residing in a slice instance for providing slice security root key. The slice security root key is used to derive the keys for the user plane protection in a network slice instance.

Security Anchor Function' (SEAF')

An authentication function resides in a network slice instance in the core network. The SEAF' is responsible for deriving user plane protection keys based on the slice security root key provided by the SEAF. In case of need, the SEAF' is also responsible for performing slice authentication and authorization to the UE in a network slice instance.

A generic security procedure of network slicing is described as follows:

1. UE and SEAF perform mutual authentication. A successful authentication results in an authentication session root key.
2. Based on the authentication session root key, the keys for NAS security, CP-AN signalling protection and network slice security are derived.
3. The NAS security key and CP-AN signalling protection key are passed to the corresponding CCNFs (Common Control Network Functions), and the network slice security root key is passed to the SEAF' in the network slice instance that is assigned to the UE.
4. Based on the slice security policy obtained from the Policy Control Function (PCF), the SEAF' may perform slice authentication and/or authorization procedure with the UE.
5. The SEAF' and UE derive user plane protection keys for CN and AN security.

5.8.4.7.2.2 Key Hierarchy

A key hierarchy for the NextGen system is shown in Figure 5.8.4.7.2.2-1. They are described as follows:

- K: The subscription credential that is held in the UE and ARPF.
- K_{SEAF}: The anchor key for the authentication session from which subsequent keys, i.e. K_{NAS}, K_{ANCP} and K_{NS}, are derived.
- K_{NAS}: The control plane key that is used to derive NAS integrity and encryption protection keys, i.e. K_{NASint} and K_{NASenc}.
- K_{ANCP}: The AN signalling protection key that is used to derive AN signalling integrity and encryption protection keys, i.e. K_{RRCint} and K_{RRCenc}.

Lenovo Ex. 1007
Page 400

- K_{NS}: The slice security root key that is used to derive user plane protection keys for CN and AN in a slice instance, i.e. K_{CNUP} and K_{ANUP}.

- K_{CNUP}: The user plane protection key that is used to derive user plane integrity and encryption protection keys for CN security in a slice instance, i.e. $K_{CN\text{-}UPint}$ and $K_{CN\text{-}UPenc}$.

- K_{ANUP}: The user plane protection key that is used to derive user plane integrity and encryption protection keys for AN security in a slice instance, i.e. $K_{RRC\text{-}UPint}$ and $K_{RRC\text{-}UPenc}$.

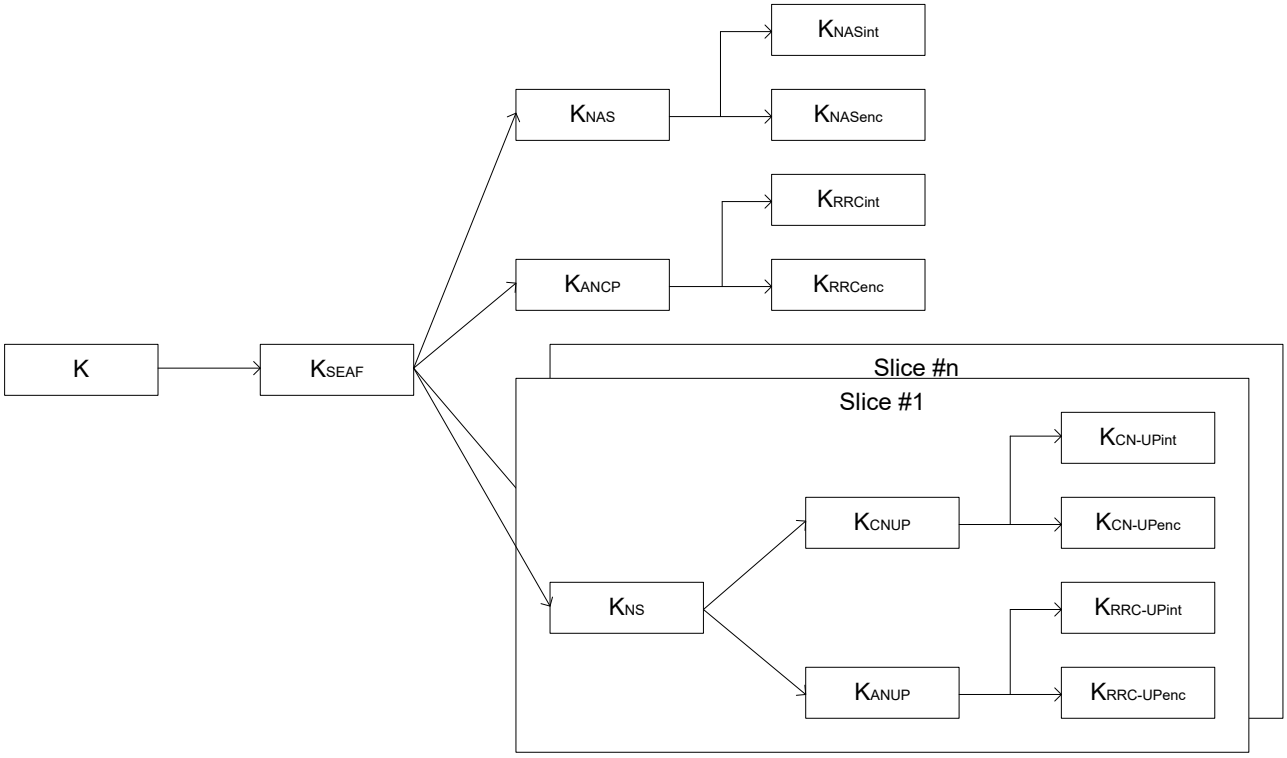


Figure 5.8.4.7.2.2-1: Key hierarchy of the NextGen system

5.8.4.7.2.3 Procedure

A general slice security procedure that includes a slice authentication is shown in figure 5.8.4.7.2.3-1.

Lenovo Ex. 1007
Page 401

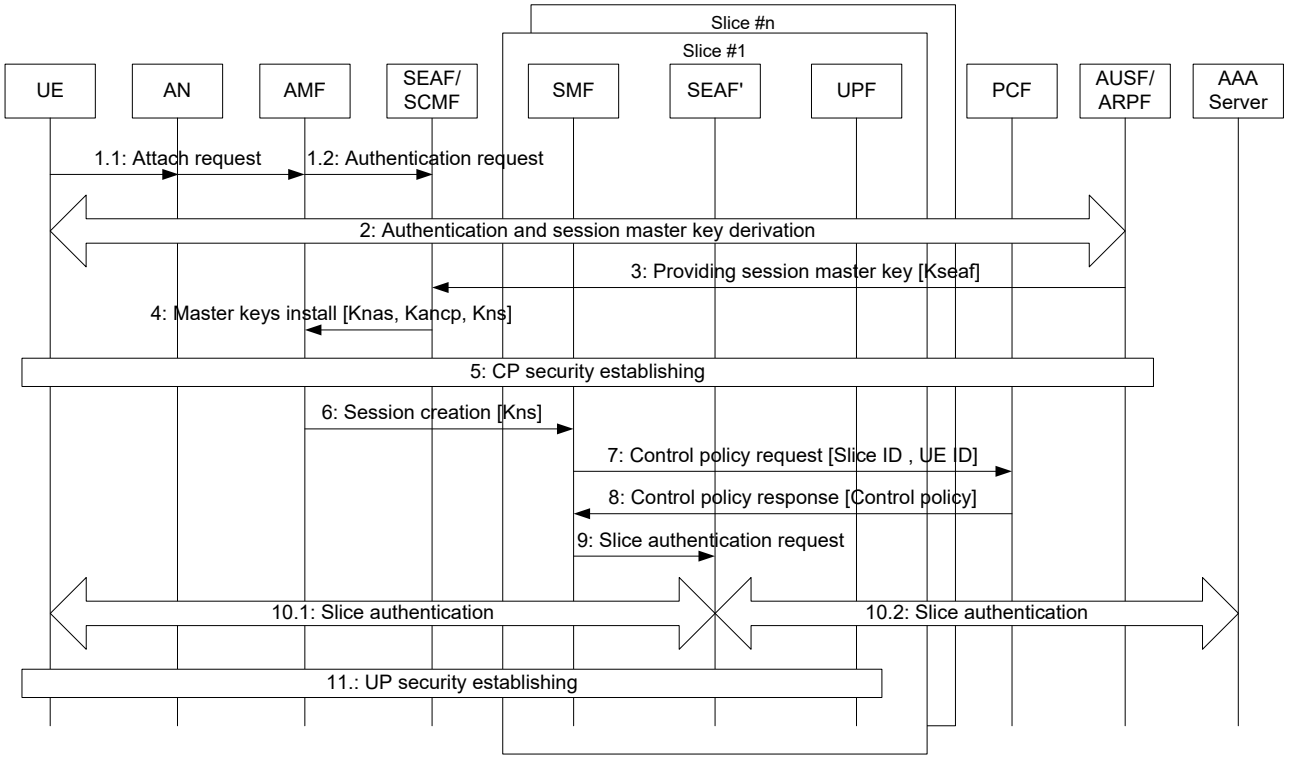


Figure 5.8.4.7.2.3-1: General slice security procedure

1. The UE sends an attach request to the network. The attach request is routed to the AMF based on a certain network function selection rule (e.g. AMF selection at AN). The AMF triggers the authentication procedure.

2. The UE and AUSF/ARPF perform mutual authentication. The exact details of the flows here depend on the authentication method being used.

3. Successful authentication will result in a session master key (i.e. Kseaf) at UE and AUSF. The AUSF provides the session master key to the SEAF.

4. The SEAF derives the control plane master keys (i.e. Knas, Kancp) and the slice security master key (i.e. Kns), and then provides these keys to the AMF.

5. The UE and AMF derive NAS signalling protection keys (i.e. KNASenc and KNASint) using Knas and derive AN signalling protection keys (i.e. KRRCenc and KRRCint) using Kancp respectively. These keys are then be used for establishing CP security.

6. The AMF sends session establishment message including the Kns to the SMF in the slice selected for the UE.

7. The SMF sends control policy request to the Policy Control Function (PCF) with the identity information of UE and slice.

8. The PCF retrieves the control policy applicable to the UE and then returns it to the SMF.

9. The SMF sends authentication request to the SEAF' if the slice authentication is requested by the control policy,.

10. The UE and AUSF/ARPF or UE and AAA Server perform mutual authentication via SEAF'. The exact details of the flows here depend on the authentication method being used.

11. The UE and SMF derive UP protection master keys (i.e. Kanup and Kcnup) using Kns, and then derive UP-AN protection keys (i.e. KRRC-UPenc and KRRC-UPint) and UP protection keys (i.e. KCN-UPenc and KCN-UPint). These keys are then be used for establishing UP security.

Lenovo Ex. 1007
Page 402

5.8.4.7.3 Evaluation

5.8.4.8 Solution #8.8: UE access network and slices

5.8.4.8.1 Introduction

This solution addresses some of the requirements addresses of key issues #8.1 and #8.2, e.g. the ability to isolate slice in terms of the security applied to a slice and to have different security policies per slice.

5.8.4.8.2 Solution overview

This solution provides a description of using user plane security that terminates in the core network to provide unique security to each slice so that from the user plane perspective the slices are isolated from each other. It also allows a different security policy to be applied to each slice.

The solution achieves the isolation by using a SEAF (that is separate from other core network nodes) to separate keys to the MMF and for the end points of the user plane security. Not allowing a separate SEAF means that a new authentication may be required when moving between MMFs that may or may not be allowed to be part of particular slices.

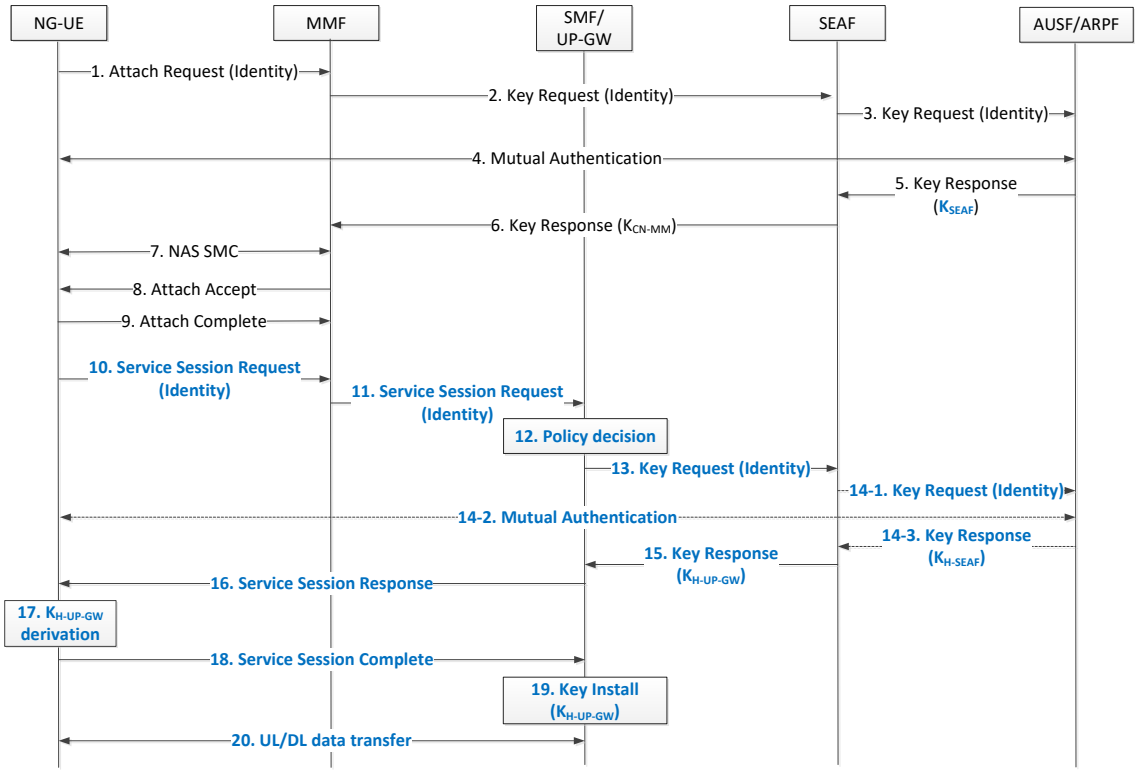
Editor's note: The underlying trust model for this soluiton require further clarification.

Editor's note: The relationships between MMFs and slice need further clarification in light of expected response LS.

5.8.4.8.3 Non-roaming case

Figure 5.8.4.8.3-1 shows the flows for an NG-UE attaching to the network and establishing a service session that terminates with user plane security that terminates at a particular UP-GW.

If the NG-UE subsequently initiates a steps 10 to 20 again but for a different slice, then the UE ends up with different keys and possible a different security policy. Hence the user planes data in each slice is isolated from that in the other slice.



Lenovo Ex. 1007
Page 403

Figure 5.8.4.8.3-1 Establishment of a slice that uses core network UP security

1 – 9. The NG-UE performs an attach procedure to the NextGen network. At the successful completion of the mutual authentication (at step 4), the AUSF provides the SEAF with $K_{H\text{-}SEAF}$, from which other subsequent keys (e.g., NAS keys, AS keys) are derived.

NOTE: The SEAF may be collocated with the AUSF.

10. The NG-UE sends a service session request message to the NextGen network to establish a service session in which the user plane (and the user plane security) terminates at the UP-GW. The request includes the UE identity that is associated with K_{SEAF} in the SEAF and an indication of security termination at UP-GW.

11. The MMF, upon receipt of the service session request from the NG-UE, determines the SMF that can establish a service session for the NG-UE.

12. The SMF determines whether the NG-UE is allowed to create the service session based on the NG-UE subscription profile.

Editor's note: How the SMF makes this policy decision is FFS.

13. The SMF sends a key request for the user plane security protection (i.e., $K_{H\text{-}UP\text{-}GW}$) to the SEAF.

14-1 – 14.3. The SEAF, upon the receipt of the key request, checks whether it has a valid security context (K_{SEAF}) for the NG-UE. If the SEAF does not have a valid K_{SEAF}, the SEAF sends a key request to the AUSF. If the SEAF determines that a fresh authentication is required (e.g., due to the key expiry), the SEAF triggers the authentication by sending a key request with an indication of fresh authentication to the AUSF. The AUSF sends a K_{SEAF} to the SEAF.

NOTE: if the SEAF already has a valid K_{SEAF} obtained during the prior authentication, the steps 14-1 to 14-3 are skipped.

15. The SEAF derives a $K_{UP\text{-}GW}$ from the K_{SEAF} and sends the $K_{UP\text{-}GW}$ to the SMF in the key response message.

Editor's Note: Whether SM message protection is necessary in addition to NAS protection and how to protect SM messages are FFS.

16. The SMF sends a service session response message to the NG-UE via the MMF. The SMF may change the user plane security configuration at UP-GW for this session and inform the NG-UE of the configuration change in the service session response.

17. The NG-UE derives $K_{UP\text{-}GW}$ from K_{SEAF} and starts protecting the user plane traffic for the service session based on the service session response from the H-SMF.

18. The NG-UE sends the service session complete message to the SMF to acknowledge the receipt of the response message.

19. The SMF applies the user plane security configuration and installs $K_{UP\text{-}GW}$ at UP-GW.

20. UL/DL data transfer for the session is protected using $K_{UP\text{-}GW}$.

Figure 5.8.4.8.3-2 shows the key hierarchy for the above flows. In the key hierarchy, it is possible to have multiple copies of K_{UP_GW} (and key derived from this) that represent the different keys used to protect the different UP slices.

Lenovo Ex. 1007
Page 404

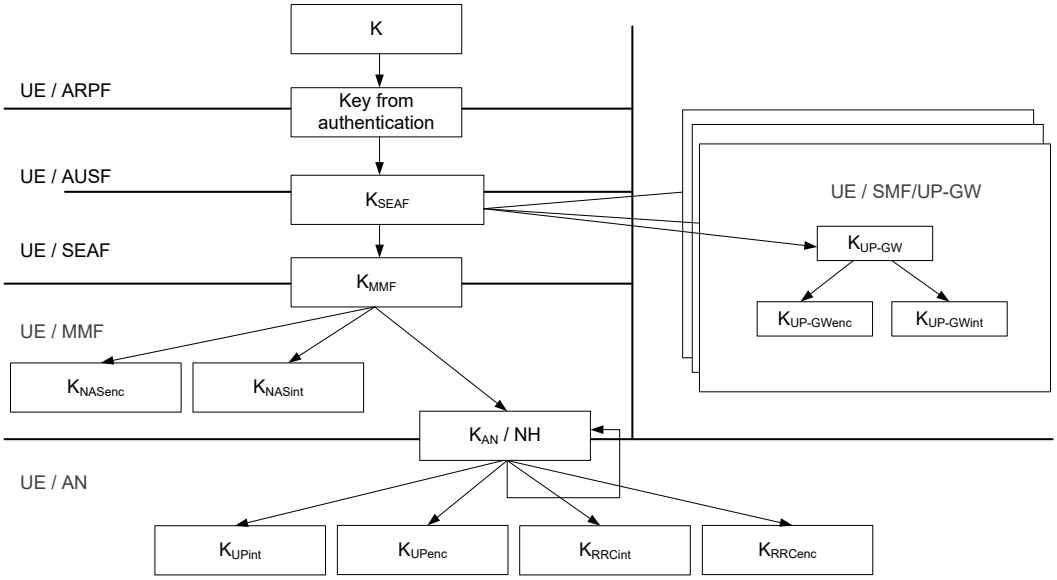


Figure 5.8.4.8.3-2 Key hierarchy with multiple slices protected using core network UP security

5.8.4.8.4 Roaming case

The roaming case is very similar to the non-roaming case. The main difference is that there may be user plane bearer that terminate in an UP-GW for the HPLMN. Protecting such bearers to the HPLMN would require a key in the HPLMN. An additional authentication run to create such a key could be avoided by leaving a key in the HPLMN when the NG-UE is authenticated in the roaming network.

5.8.4.9 Solution #8.9: Security mechanism differentiation for network slices

5.8.4.9.1 Introduction

This solution addresses the key issue #8.2: Security mechanism differentiation for network slices.

5.8.4.9.2 Security mechanism differentiation in authentication

The 3GPP System should be able to support multiple authentication protocols. Different slices may use different authentication protocols. Among all the authentication protocols used in a 3GPP network, a UE may use one or a few authentication protocols. An AU, dedicated for a slice or common to multiple slices may also use one or more authentication protocols and may not support all the authentication protocols used in a 3GPP network. In cases that a UE supports multiple authentication protocols, the UE should report its authentication capabilities (e.g. through reporting the identifiers of supported authentication protocols) to the network, and the network should select AU(s), either dedicated for a slice or common to multiple slices, for UE authentication to slices, taking into consideration the UE's authentication capabilities. Furthermore, the network should select an authentication protocol from those supported by the slice to use, if the UE supports multiple authentication protocols.

The figure below illustrates AUSF selection and authentication protocol selection in an attach procedure.

Lenovo Ex. 1007
Page 405

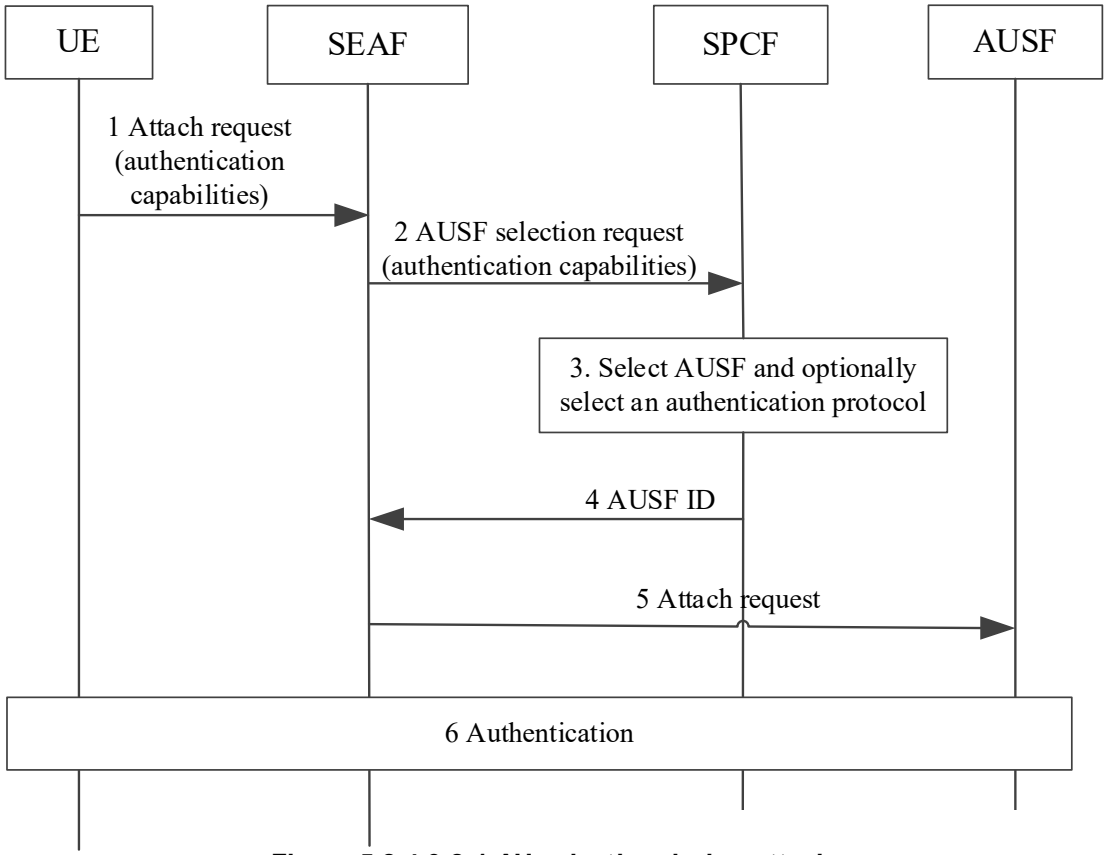


Figure 5.8.4.9.2-1 AU selection during attach

The description of above procedure is as below:

1. A UE sends an attach request to SEAF. The request contains the UE's authentication capabilities, i.e., the authentication protocols the UE supports.

2. SEAF sends an AU selection request to SPCF. The request contains the UE's authentication capabilities.

NOTE: Please refer to clause 5.2.1.2 for SPCF definition.

3. SPCF selects an AU considering the UE's authentication capabilities. If the UE's authentication capabilities include multiple authentication protocols, SPCF needs to select a protocol as well.

4. SPCF returns the selected AUSF's ID to SEAF.

5. With selected AUSF's ID, SEAF forwards the UE's attach request to the selected AUSF.

6. UE and AUSF authenticates to each other. If the UE supports multiple authentication protocols, the authentication protocol is the one selected by SPCF in step 3.

5.8.4.9.3 Security mechanism differentiation in confidentiality and integrity protection

Different types of slices are optimized for different services. They may have different requirements on the encryption and integrity protection algorithms of UE-CN signalling, UE-AN signalling and/or user plane traffic. For example, an eMBB slice may prefer a heavy encryption algorithm with a longer key length, while an mIOT slice may prefer a lightweight encryption algorithm and a shorter key length. In addition to the encryption algorithms and key lengths, slices may differ in integrity algorithms and/or key re-keying/refreshing settings as well. Therefore, for UE-CN signalling, UE-AN signalling and user plane traffic, different slices may have different security policies on the selection of encryption algorithms, the selection of integrity algorithms, key lengths and key re-keying/refreshing settings. Further, as a slice may provide several kinds of services, or services with different settings, its security policy should also consider the security differentiation of user plane traffic inside slices as well.

Lenovo Ex. 1007
Page 406

The encryption algorithms and integrity algorithms should be determined by the network. Usually, a key length is closely related to an encryption algorithm. Therefore, the selection of encryption algorithms and key lengths may be performed together by SPCF.

The selection of encryption algorithms for UE-CN signalling and UE-AN signalling should be performed by the SPCFs of CN and AN respectively after a successful mutual authentication between UE and AUSF. The security algorithm selection for user plane traffic should be performed after the UE is authorized to transmit and receive data. This selection may be implemented inside a slice, and the mechanism could be customized for different slice types.

Besides, the selection of security policies should also consider a UE's security capabilities and the network's security capabilities. The figure below illustrates the selection of encryption/integrity algorithms and key lengths.

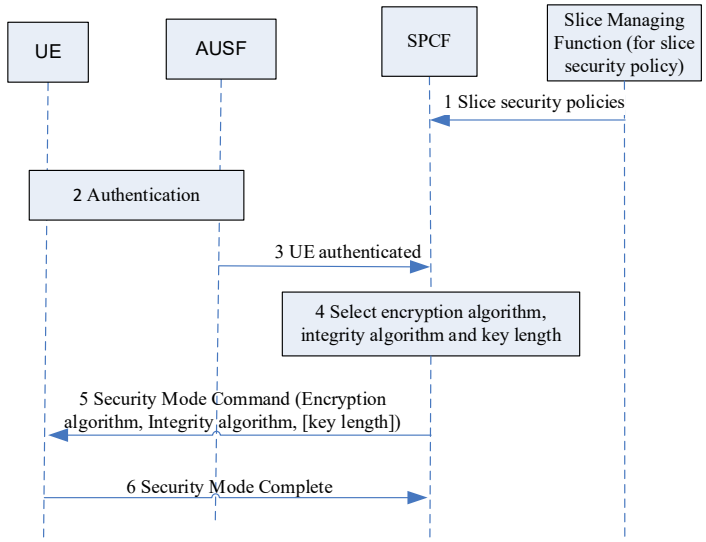


Figure 5.8.4.9.3-1 Encryption and integrity algorithm selection for signalling protection

The description of above procedure is as below:

1. SPCF obtains one or more security policies from the slice manager responsible for the security policy control.

NOTE: Slice managing function is an NF maintaining updated security policies for encryption algorithms, integrity algorithms, and key lengths and distribution of the security policies

2. UE and AUSF authenticate each other.

3. AUSF notifies SPCF that UE has been authenticated.

4. SPCF selects an encryption algorithm, integrity algorithm and key lengths considering the slice security policy, UE's security capabilities and network's security capabilities.

5. SPCF notifies UE the selection results (Security Mode Command in LTE could be reused here).

6. UE acknowledges the selection results.

5.8.4.9.4 Evaluation

5.8.4.10 Solution #8.10: Network authentication supporting network slices

5.8.4.10.1 Introduction

This solution addresses the key issue #8.3: Security on UEs' access to slices.

As observed by 3GPP TR 22.864, services offered by a network slice could either belong to the MNO or a 3rd party service provider. This solution addresses the attach procedure of UEs' access to network slices with following scenarios, defined under key issue #8.3:

Lenovo Ex. 1007
Page 407

Scenario#1: UE is authenticated and authorized by MNO. 3rd party provider entirely relies on MNO for authentication and authorization.

Scenario#5: UE is authenticated and authorized by the MNO. 3rd party provider performs secondary authentication and provides secondary authorization.

5.8.4.10.2 Solution details

This solution presents initial attach and UE authentication, together with authorization, to a network slice.

NOTE 1: In this solution, some terms, e.g. SSF or Common CP NF, are in line with the SA2 network slice architecture in 6.1.1 in TR 23.799.

Editor's note: It is ffs whether this solution is aligned with SA2 architecure. Otherwise, amend the solution to make it aligned.

The call flow figure and steps are described as follows:

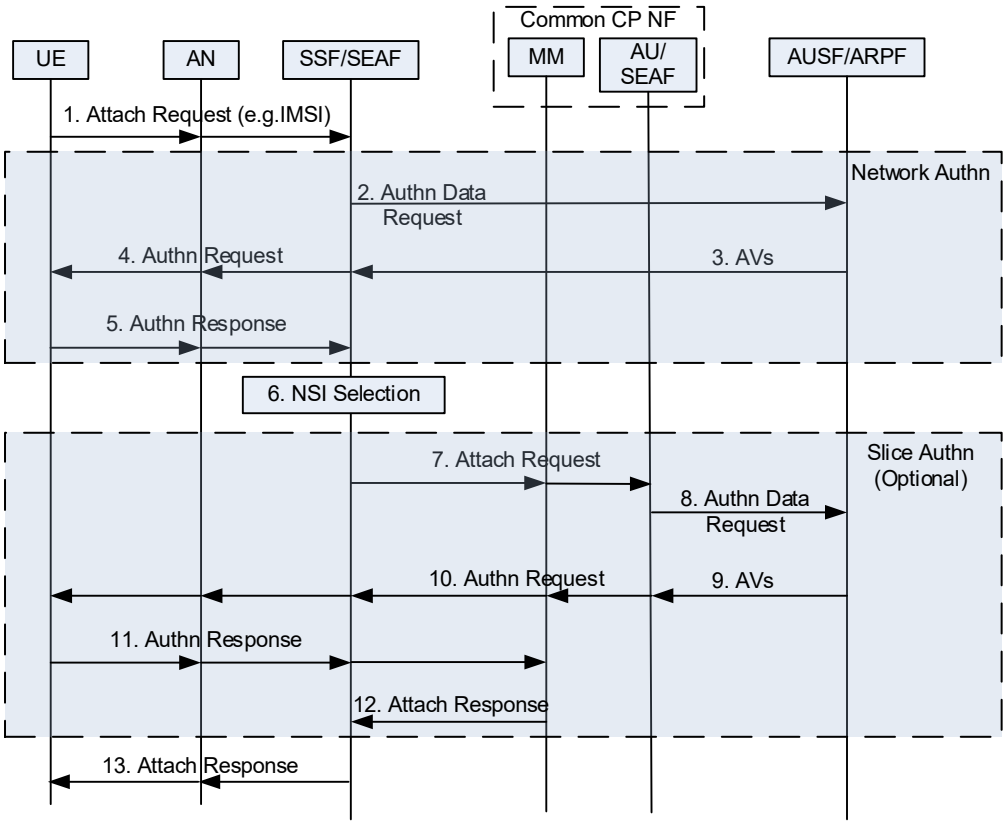


Figure 5.8.4.10.2-1 Initial attach procedure

Step 1: The NG-UE sends an Attach Request message to the AN, carrying IMSI and other assisting slice authentication information if available. RAN forwards the attach request to the SSF (either with SEAF function or co-located with SEAF)

Step 2: The SSF forwards IMSI, together with other information, to AUSF/ARPF for network authentication

Step 3: AUSF/ARPF returns authentication vectors (AVs) to SSF

Steps 4-5: SSF sends Authentication Request to the UE, which replies with Authentication Response after authenticating the network

Step 6: SSF selects an appropriate slice for the UE based on the UE's subscription information, UE capabilities, and/or service type etc, if available

Lenovo Ex. 1007
Page 408

Step 7: SSF sends an Attach Request message to MM, forwared to AU/SEAF associated with the selected slice. MM and AU/SEAF belong to Common CP NF

Step 8: AU/SEAF sends to Authentication Data to AUSF/ARPF associated with the selected slice for slice authentication

Step 9: Slice AUSF/ARPF returns the Slice AVs to the AU/SEAF in Slice.

Steps 10-11: Slice AU/SEAF sends Slice Authentication Request to the UE, which replies with Slice Authentication Response after authenticating the network.

Step 12: MM sends an Attach Response message to SSF, destinated to UE.

NOTE: Steps 7-12 are optional, depending on whether Slice Authentication is required

Step 13: SSF sends Attach Response to UE.

5.8.4.10.3 Evaluation

FFS

5.8.4.11 Solution #8.11: Slice Authentication

5.8.4.11.1 Introduction

This solution addresses the key issue #8.3: Security on UEs' access to slices.

As observed by 3GPP TR 22.864, services offered by a network slice could either belong to the MNO or a 3rd party service provider. This solution addresses the attach procedure of UEs' access to network slices without primary authentication of the UE by the MNO. The slice manager (either MNO or 3rd party provider) performs authentication and authorization of the subscription.

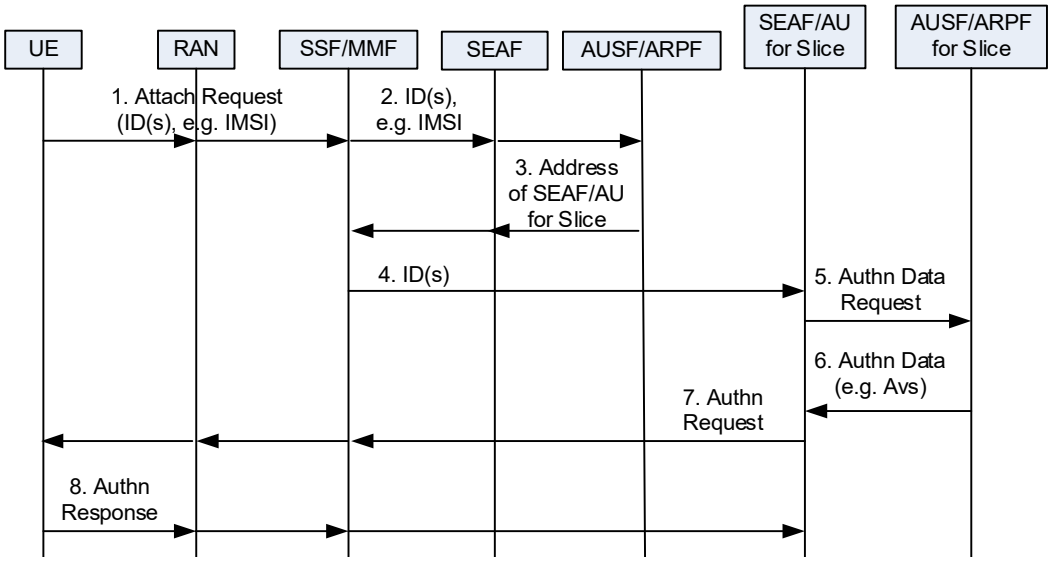
5.8.4.11.2 Solution details

This solution presents initial attach and UE authentication, together with authorization, to a network slice.

Editor's note: It is ffs whether this solution is aligned with SA2 architecure. Otherwise, amend the solution to make it aligned.

NOTE: The terms SSF and AU, are in line with the definition in SA2 network slice architecture in 6.1.1 in TR 23.799.

The call flow figure and steps are described as follows:



Lenovo Ex. 1007
Page 409

Figure 5.8.4.11.2-1 Initial attach procedure

Step 1: The NG-UE sends an Attach Request message with ID(s), e.g. IMSI to the RAN, which forwards the attach request to the SSF (either co-located with MMF or includes MMF function)

Step 2: SSF/MMF acquires ID(s) in Attach Request and sends ID(s) to SEAF, to AUSF/ARPF confirms an appropriate slice for the UE

Step 3: AUSF/ARPF finds the address information of the SEAF/AU for the slice handling the UE and sends to SSF/MMF

Step 4: SSF sends a message with IDs to the SEAF/AU for the slice.

Step 5: SEAF sends Authentication Data to AUSF/ARPF associated with the slice for slice authentication

Step 6: AUSF/ARPF returns Authn Data (e.g. AVs) to the SEAF/AU for the slice.

Steps 7-8: SEAF/AU for the slice sends Authentication Request to the UE, which replies with Authentication Response after authenticating the slice.

5.8.4.11.3 Evaluation

FFS

5.8.4.12 Solution #8.12: PCO based authentication and authorization for Slice access

5.8.4.12.1 Introduction

LTE has defined a mechanism where the P-GW may use Diameter based authentication [RFC 7115] to authenticate a user with a non-3GPP AAA Server connected to it over the SGi interface.

The user provides the PAP/CHAP user credentials in the Protocol Configuration Options (PCO) IE during an initial attach. When the P-GW receives the NAS session management message (for ex., PDN Connectivity Request) with the user provided PAP/CHAP credentials in the PCO IE, the P-GW sends encodes this authentication information in a AA-Request Diameter message (cf. TS 29.061) and forwards it to the APN-specific external AAA server over the SGi interface.

The AAA server checks whether the user can be accepted. When the P-GW receives a positive response from the AAA server, it shall complete the initial access procedure.

The proposed solution uses PCO based mechanism to provide user authentication for slice access.

PCO is used as a container to carry authentication protocol messages between the UE and the external server. The AAA server is connected to the slice over the NG6 interface. Diameter protocol is used for carrying authentication messages between the slice and the external AAA server.

Lenovo Ex. 1007
Page 410

5.8.4.12.2 Solution details

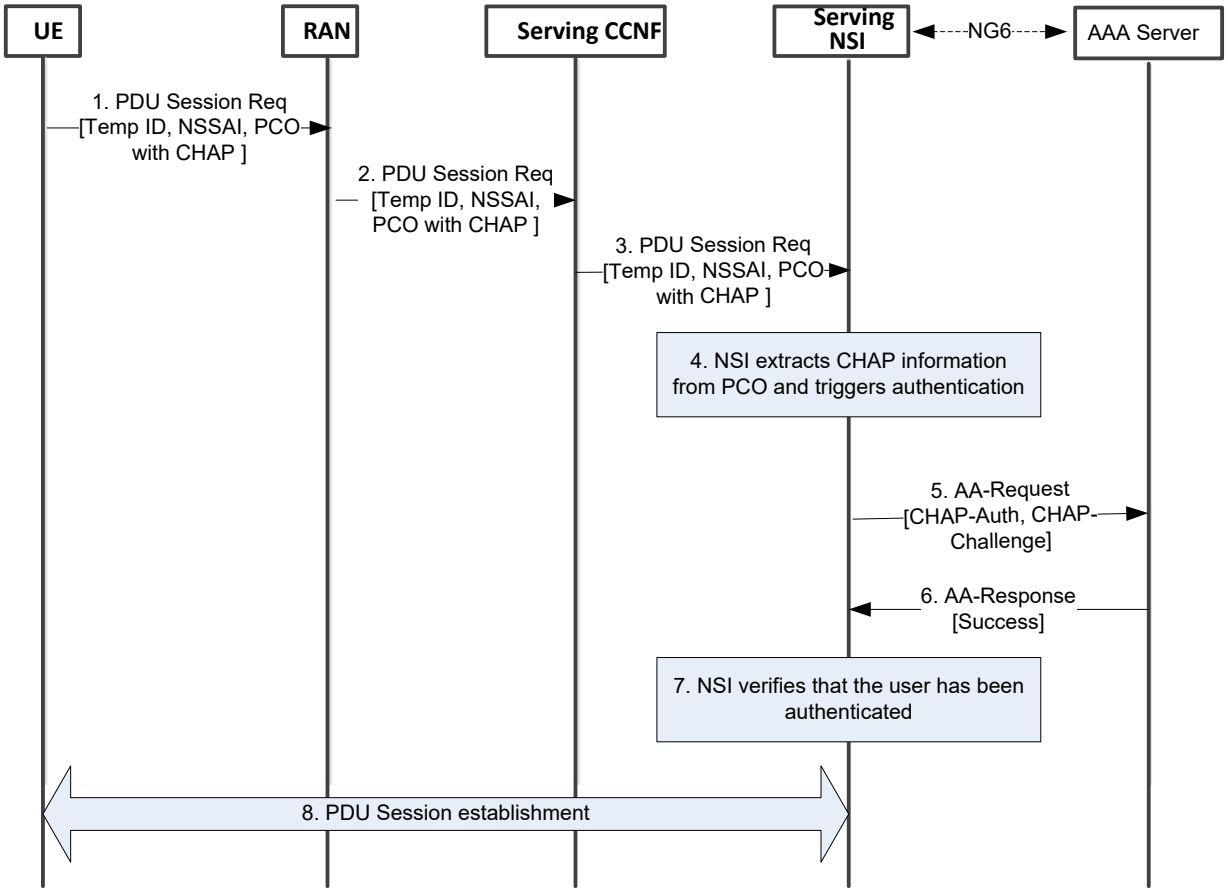


Figure 5.8.4.12.2-1 PCO based user authentication based on CHAP authentication protocol

In the following sequence, CHAP based authentication is used to illustrate PCO based authentication. As a container, PCO could be used to carry other authentication methods applicable directly between the UE and the external server.

1. The UE initiates the PDU Session Request SM message to establish a PDU session via the SMF. UE includes the Temp ID, Accepted NSSAI and a Protocol Configuration Option (PCO) IE with user's CHAP credentials.

2. RAN routes and forwards the NAS message to the proper CCNF based on information in step 1.

3. The Serving CCNF forwards the PDU Session Request to the target NSI.

4. The NSI extracts CHAP related information from the PCO IE in the NAS message, and triggers user authentication.

5. The NSI initiates a Diameter based AA-Request message to the AAA Server. This message will contain CHAP-Auth and CHAP-Response (RFC 7115) parameters carrying user provided CHAP details.

6. The AAA server checks whether user's CHAP credentials and responds with a AA-Response message with Result-Code set to success if verification succeeds.

7. NSI verifies that the user is authenticated and continues with the PDU Session establishment procedure.

The AAA server is connected to the NSI GW over the SGi interface.

5.8.4.12.3 Evaluation

FFS

Lenovo Ex. 1007
Page 411

5.8.4.13 Solution #8.13: Slice-specific NAS keys

Editor's note: It is ffs whether there will be a single security termination point for NAS messages, cf. S3-162047. If so, then this solution will not apply

5.8.4.13.1 Introduction

This solution addresses the key issue #8.1: Security isolation of network slices. If one slice is compromised, it should not negatively impact the performance and security of any other network slices. If it is possible to access one slice from another slice, then this access may be utilized to launch attacks. Isolation between slices is the basic requirement of network slicing, especially when a single NG-UE is accessing more than one slice.

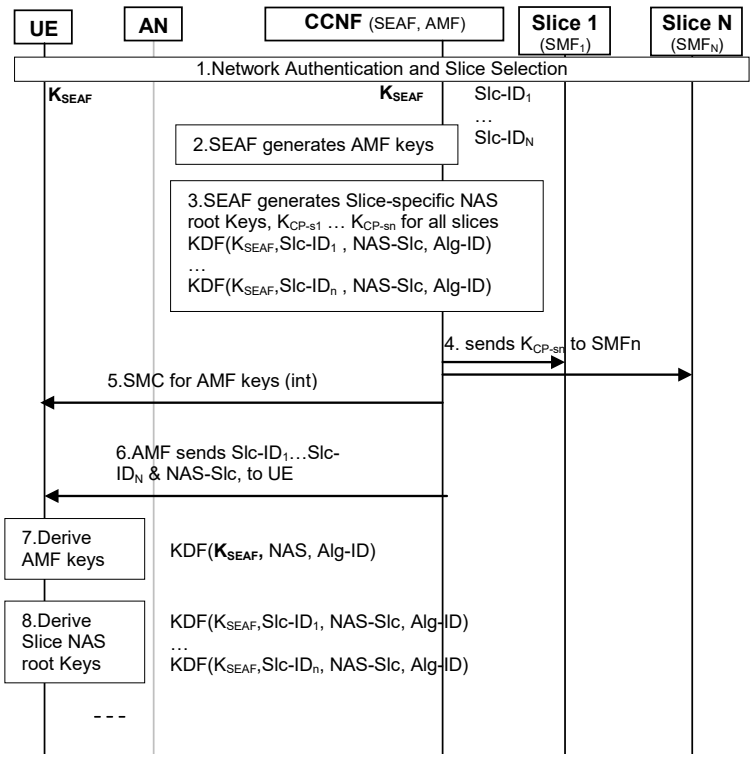
In 3GPP TR 23.799 V14.0.0 (2016-12), it has been agreed that "*A UE may access multiple slices simultaneously via a single RAN. In such case, those slices share some control plane functions, e.g. AMF*". On the other hand, SMF is slice-specific and "*AMF and SMF functions should be standardized as separate functions with standardized interactions NAS*" and "*SM messages are routed by AMF*". In short, SMF is a slice-specfic function and the NAS messages should be protected by different NAS keys (or slice-specific CP keys).

This solution achieves the security isolution of slices in control plane, in addition to the user-plane slice isolation.

5.8.4.13.2 Solution details

Slice-specific CP (or slice-specific NAS) keys shall be defined. In addition, slice-specific NAS keys shall be distributed by SEAF, instead of AMF, independent of the physical locations of AMF and SEAF.

Figure 5.8.4.13.2-1 shows a call flow and steps for the slice-specific NAS key derivation and distribution, where SEAF and AMF are assumed to be co-located:



5.8.4.13.2-1: Call flow for slice-specific NAS key derivation and distribution

1. After mutual authentication between UE and CN (SEAF or slices), K_SEAF is generated and UE is allocated with slice IDs for all slices to access, e.g., Slc-ID$_1$…Slc-ID$_N$

2. SEAF genearates AMF keys (common CP NF or CCNF)

Lenovo Ex. 1007
Page 412

3. SEAF derives all slice-specific NAS keys $K_{CP\text{-}S1}$… $K_{CP\text{-}SN}$, with slice IDs (e.g. in Step 1) as inputs to the key derivation functions (KDF). The inputs may also contain slice-specific CP (or NAS) algorithm type (e.g. NAS-Slc), algorithm ID (Alg-ID), RAND etc. SEAF sends inputs to AMF (not shown as it is assumed co-location of SEAF and AMF)

4. SEAF sends slice-specific NAS keys (e.g. $K_{CP\text{-}S1}$… $K_{CP\text{-}SN}$) to SMFn, corresponding to slice n, respectively. SMF may return acknowledgement messages (not shown).

5. AMF sends parameters for deriving AMF keys (or CCNF keys) to UE (through AN)

6. AMF sends parameters for deriving slice-specific NAS keys (e.g. Slc-ID1…Slc-ID_N and NAS-Slc) to UE (through AN)

7. UE derives AMF/CCNF keys, with parameters received at step 5

8. UE derives slice-specific NAS keys, with pararmeters received at step 6 (e.g. KDF(**K_{SEAF},Slc-ID_1**, NAS-Slc, Alg-ID) for slice n's)

5.8.4.13.3 Evaluation

5.8.4.z Solution #8.z: <solution name>

5.8.4.z.1 Introduction

Editor's note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the security area.

5.8.4.z.2 Solution details

5.8.4.z.3 Evaluation

5.8.5 Conclusions

Editor's note: This clause will contain the evaluation between the solutions, and the conclusions made by SA3.

5.9 Security area #9: Relay security

5.9.1 Introduction

In next generation systems connectivity over relays need to be supported to cover varied scenarios. The remote UE which needs the connectivity may have different capabilities in terms of radio, power and communication resources. Such devices could be regular UEs or UEs such as wearable and constraint devices. The device may connect to the relay UE using 3GPP technology or any other technology. Whatever technology is used for the D2D interface, this interface needs to be secured.

5.9.2 Security assumptions

The UE of wearable device, which can be connected to the 3GPP network directly or via another UE, should have a subscription associated to its own subscriber's identifier (e.g. IMSI) with mobile operator. If there is no separate subscription permanent identifier or a temporary identifier cannot be established, individualized services may not be possible for the device.

Lenovo Ex. 1007
Page 413

5.9.3 Key issues

5.9.3.1 Key Issue #9.1: Mutual authentication of remote UE and network over a relay

5.9.3.1.1 Key issue details

Whether the remote UE is in direct connection or in indirect connection, it should be possible for the UE and the network to mutually authenticate. Since the remote UE may be constrained device, the procedure should be as efficient as possible.

5.9.3.1.2 Security threats

If network doesn't authenticate devices accessing over a relay, it may result in unauthorized access of 3GPP network over relays and such UEs may consume precious network resources.

If remote UEs accessing network over the relay doesn't authenticate the network, these UEs may be connecting to fake networks and may lose their data or may get hacked.

5.9.3.1.3 Potential security requirements

- It shall be possible to uniquely identify an UE (e.g. wearable device), when it is connected to the network via another UE (e.g. smart phone).
- It shall be possible to mutually authenticate the remote UE and the network when the remote UE is in direct network connection or in indirect network connection.

5.9.3.2 Key Issue #9.2: Integrity and confidentiality protection of remote UEs

5.9.3.2.1 Key issue details

If the network is able to identify the remote UE uniquely and provide a unique connection to it, then this connection should be integrity protected and confidentiality protected from eve droppers.

5.9.3.2.2 Security threats

Without integrity protection of signaling messages the remote UE session over relays could be manipulated and hijacked.

Without confidentiality remote UE data to and from it could be manipulated.

5.9.3.2.3 Potential security requirements

- It shall be possible to provide integrity and confidentiality protection for the remote UE at the access layer.
- The relay UE shouldn't be able to intercept any data passing over it, irrespective of any security at the IP layer.

5.9.3.3 Key Issue #9.3: Remote UE session continuity

5.9.3.3.1 Key issue details

The remote UE may move from direct network connection to indirect network connection or change connectivity from one relay UE to another relay UE (ie one indirect connection to another indirect connection), conveniently available nearby. During such connection changes, it should be possible to continue ongoing communication sessions. Otherwise the communication session is lost for the remote UE.

5.9.3.3.2 Security threats

Without session identification and protection for the remote UE, session continuity cannot be provided.

Lenovo Ex. 1007
Page 414

Ongoing sessions could be hijacked by other UEs.

5.9.3.3.3 Potential security requirements

- It shall be possible for the 3GPP network to recognize the remote UE behind a relay at the access layer and should be able to provide seamless mobility and service continuity when the UE moves between direct and indirect network connection.
- The 3GPP Network should be able to authorize the remote UE to provide appropriate service level at QoS as the remote UE is eligible.
- The 3GPP shall support dedicated accounting for the remote UE when it communicates over a relay UE.
- The 3GPP shall support LI of the remote UE when it communicates over a relay UE.

5.9.3.y Key issue #9.y: <key issue name>

5.9.3.y.1 Key issue details

5.9.3.y.2 Security threats

5.9.3.y.3 Potential security requirements

5.9.4 Solutions

5.9.4.z Solution #9.z: <solution name>

5.9.4.z.1 Introduction

Editor's note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the security area.

5.9.4.z.2 Solution details

5.9.4.z.3 Evaluation

5.9.5 Conclusions

Editor's note: This clause will contain the evaluation between the solutions, and the conclusions made by SA3.

5.10 Security area #10: Network domain security

5.10.1 Introduction

The present security area focuses on the key issues related to the signalling protocols such as the lack of authentication and integrity mechanisms in the core network and between networks or service providers. This security area also covers issues like the signalling overload and the mechanisms which need to be integrated in the network to avoid or at least limit the impact due to, for example, DoS attacks towards the network infrastructure or against others devices/users.

In particular this security area deals with concerns such as:

- The overload of control plane messages.
- The lack of native support of authentication and integrity mechanisms in the core network signalling messages.
- Architectural security issues coming from the interconnection network.

Lenovo Ex. 1007
Page 415

5.10.2 Security assumptions

Editor's Note: This clause will document security assumptions related to each security area.

It is assumed that an operator takes the full responsibility of securing his network elements e.g. by usage of IPSec according to TS 33.210 [43]. For the interconnection network, the situation is different. Usually, an operator does not have direct connection with each of his roaming partners, and the usage of IPX roaming providers is a common business approach. Many operators and service providers have not embraced IPSec and a global PKI infrastructure is missing for that purpose.

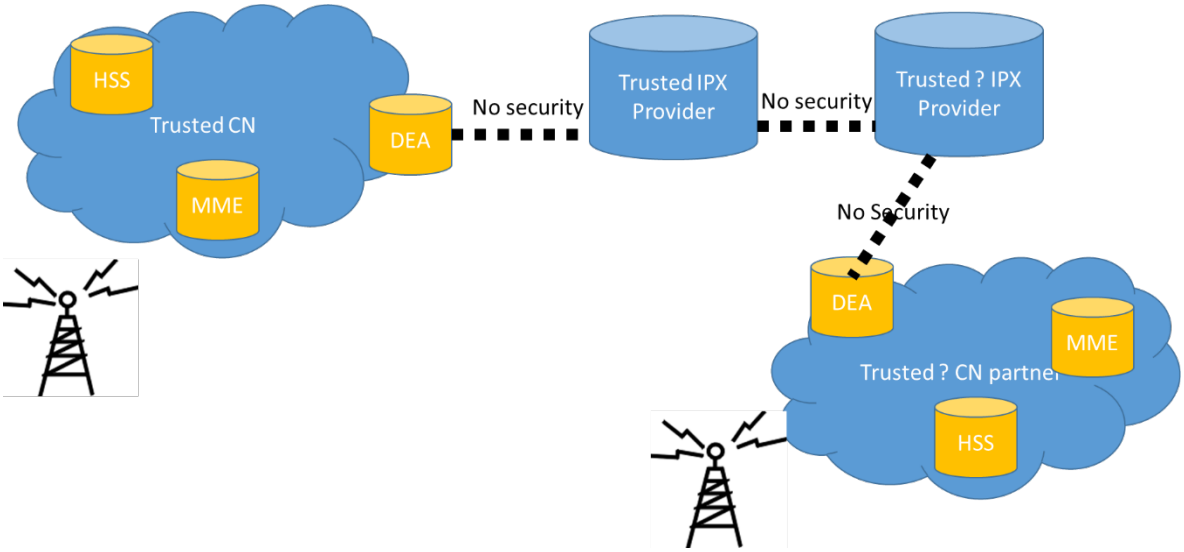


Figure 5.10.2 Simplified Interconnection example with low security links

In LTE networks, the main signalling protocol used on the interconnection network is Diameter. The Diameter base protocol specification RFC 6733 [47] defines security protection between direct (i.e. neighboring) Diameter nodes and these peer connections must be protected by TLS/DTLS or IPsec. These security protocols do not provide end-to-end security in the Diameter context unless the Diameter nodes are neighboring Diameter nodes. The current Diameter security is realized hop-by-hop and the need to also offer additional security protection between non-neighboring Diameter nodes should be addressed. This need has been recognized by IETF DIME group and the Internet-Draft [48] defines requirements for developing a solution to protect Diameter AVPs end-to-end between non-neighboring Diameter nodes. This document is still a draft to be approved and defines some scenarios and requirements. In an interconnection scenario, this solution may still not solve all problems since not all partners and service providers on the interconnection network are fully trustworthy and adhere to the same security principles e.g. when renting out their interconnection access.

Therefore, even when end-to-end security is applied, the real practical trustworthiness of messages is often questionable as the trustworthiness of the end point may be questionable.

5.10.3 Key issues

5.10.3.1 Key Issue #10.1: Network and NE communication security

5.10.3.1.1 Key issue details

The service evolution, network evolution and infrastructure virtualization brings new challenges on current widely deployed network domain protection and IPsec tunnel implementation.

Lenovo Ex. 1007
Page 416

5.10.3.1.2 Security threats

In LTE network, the core network is normally regarded as the secure network domain and the access network part are normally regarded as the unsecure domains. In next generation mobile networks, some network functions or some parts of the network functions of the core network could possibly be deployed in the unsecure domain.

Editor's Note: It is ffs whether network functions of the core network could or should be deployed in the unsecure domain and, if so, which the security implications would be. It is noted that a different choice of the security protocol would not help if the endpoint is insecure.

Thus it increases the risk of communication between the RAN parts and the CN parts, as well as the inter-communication between the CN elements located in secure and unsecure domain.

For the network secure domain protection model, IPsec are widely deployed to enable the NE in unsecure domain accessing the secure domain, and to enable the NE in different domain securely connecting to each other. In next generation mobile network, the network domain partition is complicated and the number of IPsec tunnels will be significantly large, therefore configuring IPsec tunnel will be a big challenge. The virtualized network infrastructure makes the condition worse, since the network elements and functions could be deployed dynamically in different location. Also, the fast deployment of next generation mobile network brings difficulties of IPsec management.

Editor's Note: It is ffs whether security functions inbuilt in a virtualised infrastructure / cloud environment could help to solve this problem.

Although IPsec could be configured as quintuple, i.e. (source-IP, destination-IP, protocol, source-port, destination-port), most realization deploys only IP level policies or even any-to-any policy. In next generation mobile network, the dynamic service and dynamic network will make such any-to-any or IP-to-any configuration much more common, since the IP and ports are changing along with the service orchestration. It is hard to maintain access control in case of any-to-any policy widely deployed. The IPsec tunnel mode sometimes makes the packet forward path longer than a direct connection. In delay critical application, both the forwarding path and the encryption/decryption could deduce the experience of service. For example, the communication between adjacent access points might have the path of AP-1 - SecGW1 - SecGW2 - AP-2, which brings significant forwarding delay and 2 times of encryption and decryption computation.

Editor's Note: It should be noted that already LTE allows protecting X2 connections using IPsec directly between eNBs. The star configuration described above is just one option. In case two adjacent base stations are in different security domains it needs further study from a security point of view whether it is desirable to have a direct IPsec connection between them.

Current IPsec deployments mainly use certificate as the authentication credential. The certificate requires a PKI system, which is a big cost. In addition, PKI systems meet difficulties in initial certificate application, certificate revocation and the periodical revocation list updating brings risk to the network. The online certificate status validation protocols, like OCSP, could help to solve this problem, however it is not widely used so far. In virtual infrastructure, certificate management could be much more difficult because of the virtual network functions are dynamically deployed.

Editor's Note: It is ffs whether the use of a PKI incurs higher or lower cost compared to other approaches, e.g. pre-shared secrets. It is ffs whether security functions inbuilt in a virtualised infrastructure / cloud environment could help to solve this problem.

5.10.3.1.3 Potential security requirements

As discussed in upper sections, the network and communication security in the next generation system should consider the following requirements:

Editor's Note: It is ffs whether more security protection methods, e.g. at transport layer or application layer, should be supported and whether more authentication methods, besides certificates (and PKI), should be supported to authenticate the communications between NE.

- The security mechanism should be applicable for the initial deployment of network elements and network functions, as well as the dynamic network orchestration, for example, if Network Functions Virtualization (NFV) technologies are introduced to build a NextGen network.

Lenovo Ex. 1007
Page 417

5.10.3.2 Key issue #10.2: Interconnection Security

5.10.3.2.1 Key issue details

Security aware operators are deploying security protocols, firewalls, filters, hardening standards and adhere to high level of security for renting out their access, while other interconnection partners will be less diligent. Therefore, the security landscape is very inhomogeneous on the interconnection network. Screening of everything is quite resource intensive, but other "selective" screening approaches have currently the high risk of missing attacks e.g. due to spoofed origin in messages. Some of them may even pull a network down with one message.

5.10.3.2.2 Security threats

The known interconnection security attacks include:

- DoS against users [44], [28]

- DoS against network nodes [44]

- Eavesdropping [28], [29]

- SMS interception (including password recovery code messages for social network services or e-mail accounts) [29]

- Location tracking [44], [45], [28], [29], [30]

- Fraud (incl subscriber profile modification) [44], [28], [29]

- Subscriber credential theft or session key theft [44], [30]

- IMEI whitelisting [46]

In most of those attacks, the attacker impersonates a network node e.g. of a partner operator MME in an LTE network. While some of them are today only really well-known for SS7, many of them have already be confirmed to apply also for the successor protocol Diameter. Hence we add:

- Network node impersonation

- Source address spoofing in signalling messages (used to realize impersonation at various protocol layers)

Key theft attacks in the AKA protocol:

An attacker could obtain keys in several different ways:

4. by passively eavesdropping on the communication between an HSS sending authentication vectors (AVs) to a genuine serving node. Attack 1 is not commonly described in the literature as an attack on SS7 networks (which does not, of course, mean that it could not be performed.);

5. by impersonating a genuine serving node towards the HSS and obtaining AVs in this way; [28, 29]

6. by impersonating a genuine serving node towards another serving node to obtain a current security context (e.g. sending a forged context request between SGSNs or MMEs used in handovers or idle mode mobility) [30]

Re-routing attack: The attacker could also impersonate a genuine serving node by sending a forged Location Update message to the HSS [30]. In this way, the downlink traffic could possibly be re-routed towards the attacker's serving node.

Editor's Note: Key theft attacks and re-routing attacks are identically described in clause 5.3.3.1.2. Consider replacing them there with a reference to here, once the present contribution has been accepted.

The security threat is based on the fact that the origin of a message cannot be assured 100 %. There are often several interconnection providers in the communication chain. If security is deployed, it is hop-by-hop and no global infrastructure is supporting it. Some less stringent partners rent out their access without really validating that the tenants behave according to the contractual agreement and do not misuse the rented accounts for illegal activities (note, that some of the mentioned attacks might in some countries not be illegal at all) and, hence, even end-to-end security as defined in [48] does not yet completely address these threats.

Lenovo Ex. 1007
Page 418

Some operators invest heavily in their security infrastructure to provide their customers a reliable and trustworthy service.

5.10.3.2.3 Potential security requirements

Communication security requirements for interconnection networks:

- Source address spoofing in signalling messages should be prevented by origin authentication.
- Signalling messages should be protected from unauthorized modification.
- Signalling messages should be protected from replay attacks.
- Transmitted keys should be confidentiality-protected.

Security assurance requirements on nodes in interconnection networks:

- Nodes should support security monitoring of signalling protocols.
- Nodes should support security filtering of signalling protocols, cf. e.g. TS 33.117 [36].
- Nodes should be hardened according to pertinent specifications, cf. e.g. TS 33.117 [36].

Examples of signalling protocols that may be used in the NextGen interconnection network include DIAMETER and GTP.

Migration aspects for interconnection networks:

- A solution should not expect, that all operators and interconnection service providers deploy high level security measures in the NextGen interconnection network in one go. A solution should therefore allow growing of security and trust in a gradual manner.

Operational aspects for interconnection networks:

Operators and interconnection service providers should

- deploy security monitoring of signalling protocols
- deploy security filtering of signalling protocols
- follow good practises on access to the interconnection network, e.g. not give third parties uncontrolled access.

If operators and interconnection providers have to interact with legacy systems, e.g. SS7, corresponding measures need to be taken for the legacy systems, also to avoid bidding down attacks.

Editor's Note: Requirements on operational aspects may be added to a 3GPP guidance document in a 900-series TR or informational Annex of a TS, or they may be communicated to the GSMA, once the NextGen work has been completed.

Editor's Note: Note that the above categories of requirements are complementary as secure products can be deployed and operated in an insecure manner.

Lenovo Ex. 1007
Page 419

5.10.3.y Key issue #10.y: <key issue name>

5.10.3.y.1 Key issue details

5.10.3.y.2 Security threats

5.10.3.y.3 Potential security requirements

5.10.4 Solutions

5.10.4.1 Solution #10.1: Circles of Trust

5.10.4.1.1 Introduction

This solution addresses the problem of weak security on the interconnection link introduced in Key Issue#10.2. More precisely, it addresses the requirement on migration aspects: "A solution should not expect, that all operators and interconnection service providers deploy high level security measures in the NextGen interconnection network in one go. A solution should therefore allow growing of security and trust in a gradual manner."

Editor's Note: It is ffs whether this solution should be added to a 3GPP guidance document in a 900-series TR or informational Annex of a TS, or they may be communicated to the GSMA, once the NextGen work has been completed.

5.10.4.1.2 Solution details

The underlying fundamental idea is to allow the growing of secure islands of trusted operator groups which adhere to high security principles. Those islands can then slowly be enlarged and grow together over time.

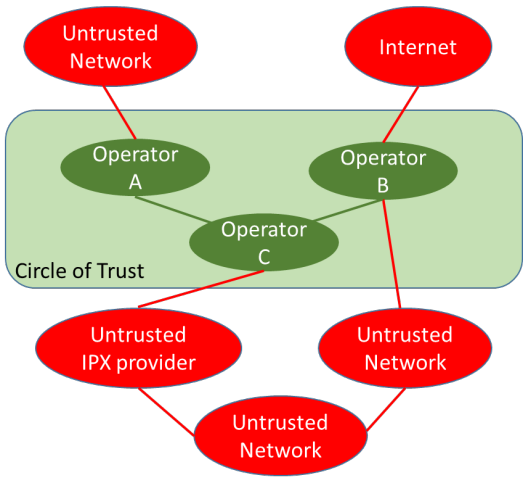


Figure 5.10.4.1.2-1: Circle of Trust among operators

The general approach is to classify messages or sessions according to the trustworthiness of its assumed origin (we take into account that the attacker will try impersonation). An operators who is security aware, should know the security status of his own core network. This would pose the innermost circle of trust.

Inside one trust circle, trust is assumed to be transitive, i.e. every node trusts every other node.

The home network circle (home circle)

The home network consists of nodes that communicate securely with each other using TS 33.210 and follow the pertinent security assurance standards (e.g. SCAS). Each message coming from one of the home network nodes can prove its authenticity to another node of the home network. The edge nodes do not accept messages coming over the

Lenovo Ex. 1007
Page 420

interconnect link and claim to be from the home network. The edge nodes also deploy proper interface separation and validates that interface in an interface cannot be done e.g. using two DIAMETER application ids.

Large international operators may have centralized some part of their operation in one country for OPEX reasons. This operators sometimes use the interconnect link to exchange messages between their network elements. It is a pre-requisite for the present solution that, for this purpose, no third-party interconnection providers are utilized. The network operator is able to equip all his nodes with the needed credentials to prove the authenticity of another node in the home network group.

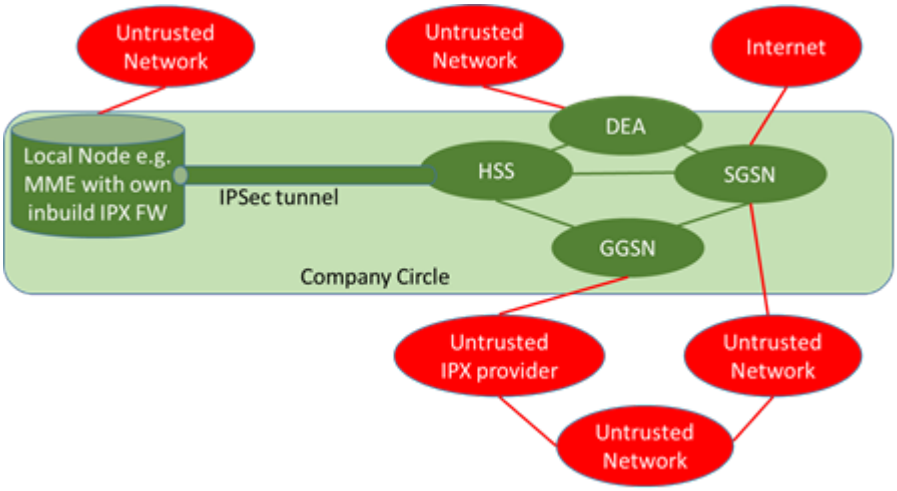


Figure 5.10.4.1.2-2: Home Network Group

Also, local nodes that are exposed to the interconnection network need to follow the full security requirements of the circle to avoid "backdoors" into the company group circle.

The home network group (company circle)

In addition to the previous home circle, the nodes receiving messages from other parts of the home network group can not only validate that this message is really coming from the other node, but they also have to have their own protection mechanisms since they are now all now edge nodes.

The next circle of trust would consist of very trusted partners, where the operator has a direct linkage with the other operator, i.e. no interconnection provider and hop-by-hop security is used.

Direct trusted partners (direct circle)

This is the case, when one network communicates with another trusted partner directly through a secured link and no interconnection providers are in between. It is important that edge nodes of those two networks know that direct trusted partners should send message ONLY through that secured link and not otherwise (else, some attacker can impersonate a trusted partner easily). The direct trusted partners would adhere to the same security quality level to ensure the resilience of their networks also against hacks and other malicious activities (e.g. renting out to untrustworthy parties).

Lenovo Ex. 1007
Page 421

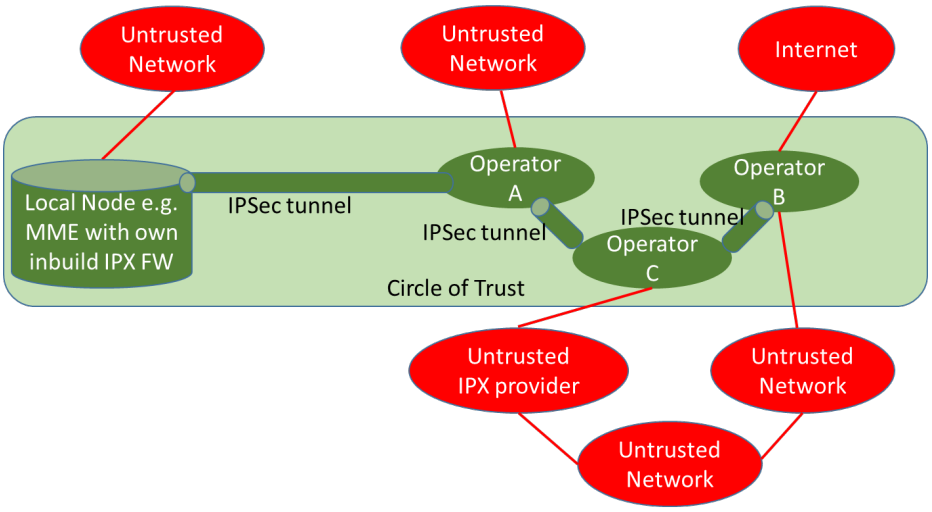


Figure 5.10.4.1.2-3: Trust circle with direct linkage

Untrusted partners (outside company circle and direct circle)

The last circle is the "other". It includes all roaming partners that are not part of the company circle nor direct circle. This does not imply that the security of the networks of untrusted partners is necessarily weak; it just means that the operator cannot be sure about the security status of these other networks, for whatever reason. This implies that the other networks may be such that the origin of messages sent from them and their authenticity cannot be ensured and the risk of being a potential fraud, eavesdropping, location tracking or other type of attack may be quite high.

An operator may also take security circles into account for its

- Risk management
- International revenue share model
- Screening frequency of messages

On a practical deployment level, the following methods can be deployed to support the circle model above:

- HSS takes care that it issues authentication vectors with serving network identities relating to networks inside the Circle of Trust only to entities that the HSS can verify as belonging to the trust circle. Being in the trust circle implies that all entities in it "behave well" (to be specified further) and communication paths inside the trust circle are protected. Behaving well would imply that an MME from the trust circle never impersonates another MME.

- Conversely, an MME can verify in a roaming scenario that an HSS belongs to the trust circle. Being in the trust circle implies that all entities in it "behave well" (to be specified further) and communication paths inside the trust circle are protected. Behaving well would imply that a HSS from the trust circle never impersonates another HSS.

- A UE, or a human user informed by the display of the UE, may also take into account the information whether the current serving network forms part of a circle of trust including the subscriber's home operator, cf. security area #6 "Authorization".

NOTE: The above measures are considered to be complementary to protocol security enhancements, e.g. for DIAMETER or GTP. Editor's note: It's FFS how to define "good behaviour" of an entity belonging to an trust circle and how its trustworthiness can be ensured.

Editor's note: Terminology will have to be updated according to agreements on terms for authentication functions and protocols in the interconnection network.

Lenovo Ex. 1007
Page 422

5.10.4.1.3 Evaluation

5.10.4.2 Solution #10.2: Public-key encryption of keys in authentication vectors

5.10.4.2.1 Introduction

This solution contributes to solving key issue 10.2 "Interconnection Security".

The solution makes the following assumptions:

The serving network that requests an authentication vector from the home network, or requests a security context from a neighbouring serving network, has a private-public key pair. The private key never leaves the serving network. The public key is known to the responding entity, i.e. the home network or the neighbouring serving network.

NOTE: This assumption has been made in various other parts of the present TR, cf. e.g. key issues #1.8 and 2.6.

5.10.4.2.2 Solution details

General approach:

Any key sent between core network entities is encrypted by the sending entity with the public key of the receiving entity. E.g. a field carrying a key in a DIAMETER AVP could be public-key encrypted.

Case 1: The serving network requests an authentication vector from the home network.

Whatever the authentication method, at one point during the authentication procedure, the home network sends an intermediate key to the serving network. Examples are K_{ASME} in EPS AKA and MSK in EAP methods. In the present solution, this intermediate key is encrypted by the home network with the public key of the serving network. In other words, the information element in a message that would contain the intermediate key in the clear now contains this key in encrypted form; all other elements in the message may remain the same.

Case 2: The serving network requests a security context from a neighbouring serving network.

It is expected that security contexts are forwarded between core network nodes also in NextGen. An example from EPS is security context forwarding between MMEs over the S10 reference point. Such security contexts contain keys. In the example of EPS, they include one or two K_{ASME} keys. In the present solution, this key is encrypted by the sending serving network with the public key of the receiving serving network.

Migration aspects:

It may be argued that not all serving networks receiving keys may have a private-public key pair, at least not at the start of NextGen deployment. This issue could be addressed by employing the trust zone concept from solution 10.1 that allows for gradually adding serving networks that do possess a private-public key pair to a home network operator's trust zone.

5.10.4.2.3 Evaluation

This solution addresses the following threats in key issue 10.2:

Key theft by passively eavesdropping on the communication between an HSS sending authentication vectors (AVs) to a genuine serving node: this is no longer possible as the key is encrypted.

Key theft by impersonating a genuine serving node towards the HSS: this is no longer possible as the use of public key encryption implies implicit authentication of the receiver, i.e. only the receiving serving network that holds the corresponding private key can decrypt the received key.

Key theft by impersonating a genuine serving node towards another serving node: this is no longer possible for the same reason as in the preceding point.

An advantage over NDS/IP is that the present solution does not require direct IP connectivity.

Comparison to shared-key based methods:

Lenovo Ex. 1007
Page 423

Instead of using public-key encryption of transmitted keys, it would, of course be also possible to encrypt the transmitted keys with a key shared between sending and receiving core network entity. However, as the relationship among serving networks and home networks is a many-to-many relationship, the use of public key methods seems advantageous. First, the use of shared keys would require n(n-1)/2 agreements among n operators, while the number of public keys only grows linearly. Secondly, the distribution of public keys seems easier from a security point of view as they could be retrieved from a central repository in an integrity-protected way.

NOTE: Addressing scenarios where a serving network requests a key for a UE that is not present in the serving network is an issue orthogonal to the present solution. Such scenarios are addressed by authentication methods with authentication confirmation such as EAP methods or EPS AKA* (cf. solutions 2.21 and 2.22).

5.10.4.z Solution #10.z: <solution name>

5.10.4.z.1 Introduction

Editor's note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the security area.

5.10.4.z.2 Solution details

5.10.4.z.3 Evaluation

5.10.5 Conclusions

Editor's note: This clause will contain the evaluation between the solutions, and the conclusions made by SA3.

5.11 Security area #11: Security visibility and configurability

5.11.1 Introduction

This security area covers visibility and configurability of security features for Next Generation System, where these features and capabilities depend on 3GPP services and operators.

The user or the UE may need to be aware of the security available for a specific service so that they can choose whether this is secure enough for the service use. Without the ability to determine the security level, applications may need to implement their own security features (wasteful in power and space) or there may be opportunities for that service to be hacked.

It should be possible for the user or UE application provider to set minimum security levels for applications.

5.11.2 Security assumptions

Different services or access networks may have different security capabilities, such as confidentiality, integrity, and cryptographic key sizes.

Some of the details might be out of 3GPP scope, such as specific user experience of UE, and implementation details of UEs. However, there could be some minimum requirements for secure network service experience.

Presentation of security to users (of UEs) will be simple and clear enough to understand without prior knowledge, but with possible further options for advanced uses.

It should also be noted that security visibility and configurability can also be used as a means to realize network authorization, cf. security area #6.

Lenovo Ex. 1007
Page 424

5.11.3 Key issues

5.11.3.1 Key Issue #11.1: Service-dependent security requirements

5.11.3.1.1 Key issue details

The level of security that a UE needs, or would prefer, or should expect, may vary depending on what services it is using at the time. Some possible examples:

- There may be some services / applications that, because of their sensitivity, should not run at all in the absence of user plane encryption, or in the absence of user plane integrity.
- There may be some services / applications that, because of their sensitivity, should only run when at least UMTS security is in operation, even though the device supports GSM/GPRS. Or at least LTE security, even though the device supports UMTS. Or at least NextGen security (if NextGen introduces some enhanced security features relative to LTE), even though the device supports LTE.
- There may perhaps be some services / applications that, because of their sensitivity, would benefit from a change of temporary UE identifier happening immediately before the service runs, or immediately after, or both.

5.11.3.1.2 Security threats

There may be a gap between the level of security that a UE needs, or would prefer, or should expect – depending on what services it is using at the time – and what is actually provided, even though the needed / preferred / expected security level is achievable.

5.11.3.1.3 Potential security requirements

- There should be a means for the UE to be aware of the mobile security requirements of individual services / applications, and to act on that knowledge.

Editors' note : it is ffs as to whether this requirement only applies to 3GPP applications.

5.11.3.2 Key Issue #11.2: User awareness of security

5.11.3.2.1 Key issue details

Next generation system is expected to diverse access networks (Section 4.1 of TR 23.799), services (Section 5 of TR 22.891), and UE types. Different networks or services may have different security capabilities, but the implication of it may hardly be understood by users. Since this could mislead users to mistakenly trust or doubt the current service or access networks, and make harmful decision, there should be some way to let users be aware of major security implications (e.g. fallback to weak security).

5.11.3.2.2 Security threats

Attackers could specifically target UEs in access networks or services with weak security, while users do not fully understand the situation, so for users to do sensitive transactions over the less secure environment. In general, this will make UEs more vulnerable.

Active attackers could make a UE move to less secure service or access network (e.g. by jamming the current serving eNB or network). Downgrade of security will make UEs and users more vulnerable.

Active attackers might let user to believe it is attached to a secure service or access network, while it is not the case in reality.

5.11.3.2.3 Potential security requirements

- UEs shall be able to present users of security indication of current services or access networks. In addition, detail information including security capability or parameters may be presented for the advanced users' reference.

Lenovo Ex. 1007
Page 425

- Access networks and services should be able to provide information to UEs, which is necessary to derive security indication for users.
- UEs should be able to collect security capabilities of access networks and services, and derive security indication for users from those parameters.
- UEs should be able to validate security indication related information from network.

5.11.3.3 Key Issue #11.3: User control of security

5.11.3.3.1 Key issue details

Assuming that a user (and/or an NG-UE) becomes aware of some of the security capabilities of access networks or services, whether such information is provided by networks or services, or the NG-UE derives it from other procedures, the user (or the NG-UE) may need to control the security to based on its preferences. For this assumption to work, there has to be a secure mechanism to expose security capabilities of access networks or services. 5.11.3.3.2 Security threats

Although a user may be aware of security level, if the access network or service selection is based on the other factors than security, then the user (and an NG-UE) might have no choice but to use a less secure access network. Attackers could make use of this, and lead users (and NG-UEs) to less secure situations. This will make more secure services or access networks unavailable to NG-UEs.

Attackers could attempt a bid-down attack which and lead an NG-UE, to to use less secure parameters.

The absence of a secure mechanism to expose security capabilities of access networks or services can enable such a bid down attack.

5.11.3.3.3 Potential security requirements

- UEs shall provide users with means to select from available access networks or services, based on security capabilities (or security levels) of access networks or services.
- UEs shall provide users with means to configure minimum (or preferred) security capabilities (e.g. levels or parameters) which UEs shall try to satisfy when UEs choose or negotiate with access networks or services. There might be pre-defined default configuration of minimum (or preferred) security capabilities.
- UEs shall be able to send the preferred security capability (or parameters, possible security levels, if agreed) to access networks or services. Access networks or services should try to meet the request from UE and provide acknowledgement whethere the requested security is achieved or not.
- NextGen system shall be able to securely provide UE’s with an indication of the security capabilities of a network.
- The solution should minimise the risk of accidental connection failures.

5.11.3.4 Key Issue #11.4: On demand security framework

5.11.3.4.1 Key issue details

Next generation mobile network will provide an open service platform for diverse services and applications. The varying characteristics of those services and applications, along with the diverse device capability, requires a flexible and on demand security framework. The requirements come from the following use cases [7]:

- Different services may require different security protection levels
- Application QoS restricts the security level, e.g. security protection should satisfy the processing delay restriction that service required
- The service and end user characteristics require a flexible security framework

Lenovo Ex. 1007
Page 426

- The power consumption of the network and the end user device should be considered in next generation mobile network

- The capability restriction of the end user device requires next generation mobile network a flexible security mechanism

5.11.3.4.2 Security threats

Traditional fixed mechanisms and fixed policies for security are not applicable for all use cases in next generation mobile network, since next generation mobile network will be open to provide a diverse set of services and applications.

Compared to a fixed level of security in current 3GPP networks, in the next generation mobile network, there will be some services that require very high security protection level (e.g., the public safety system). A low level of protection for such a service could cause attackers to issue fake messages, potentially leading to public panic. On the other hand, low cost, low security devices may be denied access to next generation mobile network services if an appropriate/different security protection level is not supported.

Furthermore, a match between the security capabilities of NG-UE, security level requested by the application, and security protection level offered by the serving network provides optimal security for a given network service. An inability to assure such a match may lead to a sub-optimal security level. In such cases, higher than optimal security may lead to possible exhaustion of security resources and lowered ability to react to threats, while lower than optimal security may lead to an increased vulnerability level.

5.11.3.4.3 Potential security requirements

The requirements for the next generation mobile network are:

- Next generation mobile network should have a flexible and extensible security framework to protect diverse services and applications, various devices capabilities.

Security service is configurable and negotiable, when commissioned or upon application deployment, or when user/NG-UE requests a specific service.

- The end user application, end user device and the network should have the capability to change the security policy, security capability and security parameters, when required. The change could be done via parameter configuration or software upgrade.

- Serving / home networks should be able to support variable security to match service requirements.

5.11.3.y Key issue #11.y: <key issue name>

5.11.3.y.1 Key issue details

5.11.3.y.2 Security threats

5.11.3.y.3 Potential security requirements

5.11.4 Solutions

5.11.4.1 Solution #11.1: Device API allowing an application to state security requirements

5.11.4.1.1 Introduction

This solution addresses key issue #11.1.

Lenovo Ex. 1007
Page 427

5.11.4.1.2 Solution details

Editors' note: more details are needed here and also we need to decide if this is in scope of 3GPP. We also need to take care of malware impacts on the network through this API.

The device presents an API that allows individual applications to specify minimum security requirements.

This is described only at a very high level because its detailed specification is not likely to be done by 3GPP.

5.11.4.1.3 Evaluation

TBD

5.11.4.2 Solution #11.2: Security visibility solution using security indication policy

5.11.4.2.1 Introduction

This pCR proposes a solution for key issue #11.2: User awareness of security, particularly the following potential security requirements:

- UEs shall be able to present users of security indication of current services or access networks. In addition, detail information including security capability or parameters may be presented for the advanced users' reference.
- Access networks and services should be able to provide information to UEs, which is necessary to derive security indication for users.

5.11.4.2.2 Solution details

User indication policy (file) of security is downloaded to UICC or protected storage of equipment, through existing OTA mechanism (with protection during OTA). User indication policy of security is specified as following:

- *Security capability item*, (*noticeable value list of items, or changes of item value*)
- Example 1: integrity algorithm, (null, snow 3G based)

  If the integrity algorithm is null or snow 3G based one, a user will be notified.
- Example 2: encryption algorithm, (downgrade)

  When the encryption algorithm is downgraded, a user will be notified.
- Example 3: authentication method, (other than new NG authentication)

  When the authentication method is other than newly specified ones in NG, a user will be notified.

Editor's Note: It is ffs to enlist detail items to be included in the proposed policy within the specification, including distinction of signalling and user data, but this list could be updated later, when there are new security items (from new security features) or needs (newly found vulnerabilities).

Editor's Note: The policy format/syntax should be simple and essential enough to manage. At the same time, it should be flexible to add new item and value later in the future.

The way how to present these security indication to users is an implementation issue (e.g. pop-up, status bar, or icon) and out of 3GPP scope, but the requirement will be mandated for assurance:

- Security indication/notification should be relatively stay. (i.e. if it is pop-up, that should stay on top of the screen of UE, until the user explicitly confirm, not closing after specified period of time.)
- Security indication/notification feature could be turned off by explicit choice of user in the configuration (i.e. setting menu). The default setting is "on".
- Users can configure the security indication policy through configuration/setting menu of UE, which overrides the operator policy.

Lenovo Ex. 1007
Page 428

- The more detail security capabilities are found in the configuration/setting menu of UE, for advanced users or other purposes.

Editor's Note: It is ffs to determine if it is possible or feasible to ensure that the network's security information is actually visible to the human user.

Editor's Note: It is ffs if user policy overrides operator policy, or other alternative is possible such that only stronger/higher policy of user can override except "turn off" option.

Editor's Note: It is ffs in which specification to define the assurance requirement.

Editor's Note: It is ffs when it is presented to the user, but it could be the point that the algorithm/capability is decided after negotiation or exchange between UE and 3GPP system.

5.11.4.2.3 Evaluation

FFS.

5.11.4.3 Solution #11.3: Security configurability solution using security control policy

5.11.4.3.1 Introduction

This pCR proposes a solution for key issue #11.3: User control of security.

5.11.4.3.2 Solution details

Default or standard user control policy (file) of security is downloaded to UICC or protected storage of equipment, through existing OTA mechanism (with protection during OTA). Users can modify this in the configuration/setting menu of UE anytime, and user configuration overrides the default/standard configuration. User control policy of security is specified as following:

- *Security capability item, condition list* (*value list of items, or changes of item value), action(s)*
- Example 1: authentication method, (other than new NG authentication), (retry, reject)

  When authentication method is other than newly specified ones in NG, it is rejected after retry.
- Example 2: encryption algorithm, (any), (prefer maximum security available)

  The preference to the strongest algorithm available is delivered to the system.

Editor's Note: It is ffs if it is feasible that users can understand security capability items suggested.

Editor's Note: It is ffs to how to deliver the preference. One option is to include preference flag/bits in UE security capabilities delivered to the system. Alternative is to include only the strongest algorithm that UE can afford in the UE capability, which is not practical.

Editor's Note: It is ffs to enlist detail items to be included in the proposed policy within the specification, including distinction of signalling and user data, but this list could be updated later, when there are new security items (from new security features) or needs (newly found vulnerabilities).

Editor's Note: The policy format/syntax should be simple and essential enough to manage. At the same time, it should be flexible to add new item and value later in the future.

Editor's Note: It is ffs when UE is to take action (and following recovery action after taking such actions as off/reject of connection).

5.11.4.3.3 Evaluation

FFS.

Lenovo Ex. 1007
Page 429

5.11.4.4 Solution #11.4: UE configuration of key and identifier refresh

5.11.4.4.1 Introduction

This is a solution for key issue #11.3 "User control of security", with the consideration of requirements of key issue #3.2 "Refreshing keys" and #7.1 "Refreshing of temporary subscription identifier".

5.11.4.4.2 Solution details

Key issue #3.2 "Refreshing keys" has following potential requirement.

- The UE should have some ability to trigger a refresh of security keys. Care must be taken not to create network overload, however.
- The UE should not congest the network by frequently requesting the radio interface keys to be refreshed.

Editor's Note: The above requirements will be updated such that UE should not refresh long term keys.

To address requirements, solution #3.2 "UE can request a radio interface key refresh" has proposed.

Key issue #7.1 "Refreshing of temporary subscription identifier" has following requirement.

- Temporary subscription identifiers shall be refreshed regularly with a frequency that avoids their persistent use.

To address the requirement, solution #7.1 "UE can request an update of temporary identifier" has proposed.

Both solutions aforementioned suggest UE's trigger of refresh of key or identifier as a way to ensure minimum security, just in case a network fails to address the requirement. The detail procedures and conditions to trigger the procedure remain for further study, but the method proposed in solution #11.3 "Security configurability solution using security control policy" can provide a tool in configuration aspects.

To address requirements of key issue #3.2 and #7.1, in the aspects of #11.3, similar format could be utilized for key/identifier refresh by UE.

- *Security configuration item, condition list, action(s)*
- Example 1 : radio interface key refresh, (12 hours since refresh), (try, disconnect after retrial)

  If it has passed 12 hours since radio interface key refresh, UE will trigger key refresh request procedure. UE disconnect the connection, if retry fails.
- Example 2: temporary identifier refresh, (6 hours since refresh), (try in next time, disconnect after retrial)

  If it has passed 6 hours since temporary identifier refresh, UE will trigger temporary identifier refresh request procedure, or next signalling available. UE disconnect the connection, if retry fails.

Editor's Note: It is ffs to enlist detail items to be included in the proposed policy within the specification, but this list could be updated later, when some security procedures are considered to be triggered by UE.

As in solution #11.3, this configuration is provisioned by home network, possibly from security policy function. In some circumstances, a user might be able to check and configure it. Since these kind of procedures could affect network resource, configuration by home network might override user setting. For example, if refresh period given by home network has 6 hours, and user setting has 1 hours, the former value might be used. However, user setting has 12 hours, user value could be used.

Editor's Note: It is ffs if there is a case in that user needs to configure key/identifier refresh period (and further show to human user such as "x days since key refresh" in the configuration menu of UE), since the key issues seems to address case of visited network with lax security policy (never refreshing key/identifiers for a longer period time).

Editor's Note: It is ffs whether security policy should also be derived from the security needs of applications on the UE, in addition to being provisioned by the home network.

Editor's Note: It is ffs to determine how a malfunctioning UE or a malware-infected UE can be prevented from overriding the network setting with the local setting.

Lenovo Ex. 1007
Page 430

5.11.4.4.3 Evaluation

FFS.

5.11.4.z Solution #11.z: <solution name>

5.11.4.z.1 Introduction

Editor's note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the security area.

5.11.4.z.2 Solution details

5.11.4.z.3 Evaluation

5.11.5 Conclusions

Editor's note: This clause will contain the evaluation between the solutions, and the conclusions made by SA3.

5.12 Security area #12: Credential provisioning

5.12.1 Introduction

Editor's Note: This clause gives background information on the security area.

5.12.2 Security assumptions

Editor's Note: This clause will document security assumptions related to each security area.

5.12.3 Key issues

5.12.3.1 Key issue #12.1: Credential provisioning

Editor's Note:some aspects of credential provisioning are addressed in 820, too. These aspects in 820 should eventually be merged with 611.

5.12.3.1.1 Key issue details

TR 22.861 has the following requirement in [PR.5.1.3.2-001] for IoT UEs "The 3GPP system shall support a secure mechanism to remotely provision a device that has not been pre-provisioned, with its 3GPP subscription credentials." We understand the text "3GPP subscription credentials" such that it refers to USIM credentials on a UICC as they are currently defined, i.e. they are the credentials required for the AKA protocol. But other requirements point to the potential need for supporting non-AKA authentication methods requiring different credentials, cf. e.g. requirements referring to "alternative authentication methods" in TR 22.862. We therefore distinguish these two cases below.

a) AKA credentials on UICCs

UICCs are likely to continue to play an important role in NextGen security.

Traditionally, provisioning of subscription credentials in UICCs and Authentication Centres for AKA-based authentication have not been subject to 3GPP standardization.

Over the last years, a standard for embedded UICCs has been developed by the GSMA and by ETSI TC SCP. Embedded UICCs allow for remote provisioning of credentials. The conceptual framework for embedded UICCs includes a solution for the problem of gaining initial connectivity to the provisioning server. This initial connectivity can be provided using pre-installed USIM credentials and therefore requires no changes to 3GPP standards.

Lenovo Ex. 1007
Page 431

Editor's Note: The initial connectivity could also be provided through the connectivity of a companion UE or through non 3GPP access (GSMA SGP.21 v 1.0 and SGP.22 v1.0).

Further concepts for remotely manageable UICCs are currently being worked on.

b) Other cases

Editor's Note: These 'other cases' may refer to non-AKA credentials in future versions of UICCs or in other forms of storage on the UE. (Both are ffs). In particular, it is ffs whether the concept of UICC may evolve in NextGen so as to include also the storage of non-AKA credentials.

A requirement may necessitate the support for alternative authentication methods, cf. above.

Editor's Note: It is ffs whether EAP-TLS or EAP-TTLS, or the use of client certificates, are suitable examples of these methods.

It may be desirable to provision such non-AKA-credentials, to the UE.

Editor's Note: Such a provisioning process may use an online process involving a provisioning server. It is ffs whether there would be a need to specify such a process in 3GPP. But even if it is decided not to specify such a non-AKA credential provisioning process in 3GPP it may be desirable to specify some minimal support for such processes in 3GPP, namely for enabling initial connectivity to the provisioning server for the case that initial connectivity cannot be provided using pre-installed USIM credentials.

5.12.3.1.2 Security threats

Unauthenticated access entails the risk of Denial of Service against the NextGen serving network.

Unauthenticated access entails the risk of unauthorized use of NextGen services if traffic from an unauthenticated UE is not strictly limited to communication with a provisioning server predefined in the NextGen core network.

Editor's note: The list of security threats needs to be further completed.

5.12.3.1.3 Potential security requirements

Editor's Note: It is ffs whether optional support by the 3GPP network for access to provisioning servers is needed. This issue is to be distinguished from the credential provisioning procedure between UE and provisioning server. For the latter, it is ffs whether the provisioning procedure is standardized in 3GPP or uses method described in other groups.

5.12.3.2 Key Issue #12.2: Remote credential provisioning for IoT devices

5.12.3.2.1 Key issue details

The next generation system will combine multiple network accesses and new services, such as Internet of Things (IoT). Different network accesses and services have their own characteristics therefore the requirements for security mechanisms are diverse.

Internet of Things (IoT) is one of the five catertories classified for NextGen use cases in [1] (TR 22.891). IoT devices will span a wide range, from small devices (such as sensors, wearable devices) to big devices (such as smart home appliance). Some of them may not be pre-provisioned with 3GPP subscription credentials when they are manufactured, and thus cannot access the 3GPP network directly though they may access the 3GPP network with a companion UE with 3GPP credentials..

5.12.3.2.2 Security threats

An attacker may be able to attack the communication between the 3GPP network and legitimate IoT devices during their remote provisioning procedure in case there is no secure mechanism to protect the confidentiality and integrity. They may misuse these credentials, which may cause a lot of issues, such as charging issue, invasion of privacy.

Lenovo Ex. 1007
Page 432

5.12.3.2.3 Potential security requirements

- The 3GPP System shall support a secure mechanism to remotely provision an IoT device that has not been pre-provisioned, with its 3GPP subscription credentials.

Editor's note: It is ffs whether this provisioning is standardised in 3GPP or uses method described by other groups

5.12.3.y Key issue #12.y: <key issue name>

5.12.3.y.1 Key issue details

5.12.3.y.2 Security threats

5.12.3.y.3 Potential security requirements

5.12.4 Solutions

5.12.4.1 Solution #12.1: Remote credential provisioning – Add Headless IoT device to existing user's MNO subscription

5.12.4. 1.1 Overview

Internet of Things (IoT) is an important use case for next generation networks. It will enable usage scenarios like home automation (including, security, convenience, energy packages), industry automation, smart cities with low power devices (i.e., a battery life of several years), can be easily installed and operated in challenging coverage conditions e.g. indoors and basements. These devices cannot access the 3GPP network without subscription credentials. Deployment of devices cannot be geo-specific and will have challenges to provide geo-specific credentials or provisioning information during the manufacturing time.

The owner of IoT devices, with a high probability, will have a companion UE subscribed to NextGen operator. The Companion UE and IoT device may access each other through a variety of short range communication mean e.g. NFC, Bluetooth, Wi-Fi Direct, lower power Wi-Fi, etc. The Companion UE acts as a bridge between IoT device and 3GPP network to add the IoT device to the user's subscription profile (associated with the companion UE) and provision the IoT device with a subscription profile.

5.12.4.1.2 Solution Details

The following pre-conditions are assumed:

1) IoT device is configured with appropriate Device & Security Configuration by the device manufacturer. Device Information includes Device Model, Serial number, manufacturer ID, etc. Device Security information includes public/private pair burned the manufacturing time and URL to a web site containing the certificate chain for this device.

2) IoT device is equipped with a short range radio such NFC, Bluetooth Low Energy, Low Power Wi-Fi, etc. over which it can establish secure communication with the companion UE.

3) Companion UE already has established a secure connection with Core Network using its 3GPP subscriber credentials.

4) IOT Device is provisioned with certificate of the subscription Manager used for mutual authentication.

Figure 5.12.4.1.2-1 shows the steps for the procedure to provision a subscription profile using a companion UE. Hereafter for clarity, we assume NFC is used as a short range radio for communication between the companion UE and IoT device. The IoT device is assumed to be equipped with read/write passive tag, and the companion UE is equipped with NFC radio capable of reading from and writing to a passive NFC tag. For other short range radio alternatives (e.g., Bluetooth Low Energy), there may be more steps between the companion UE and IoT device to establish the communication.

Lenovo Ex. 1007
Page 433

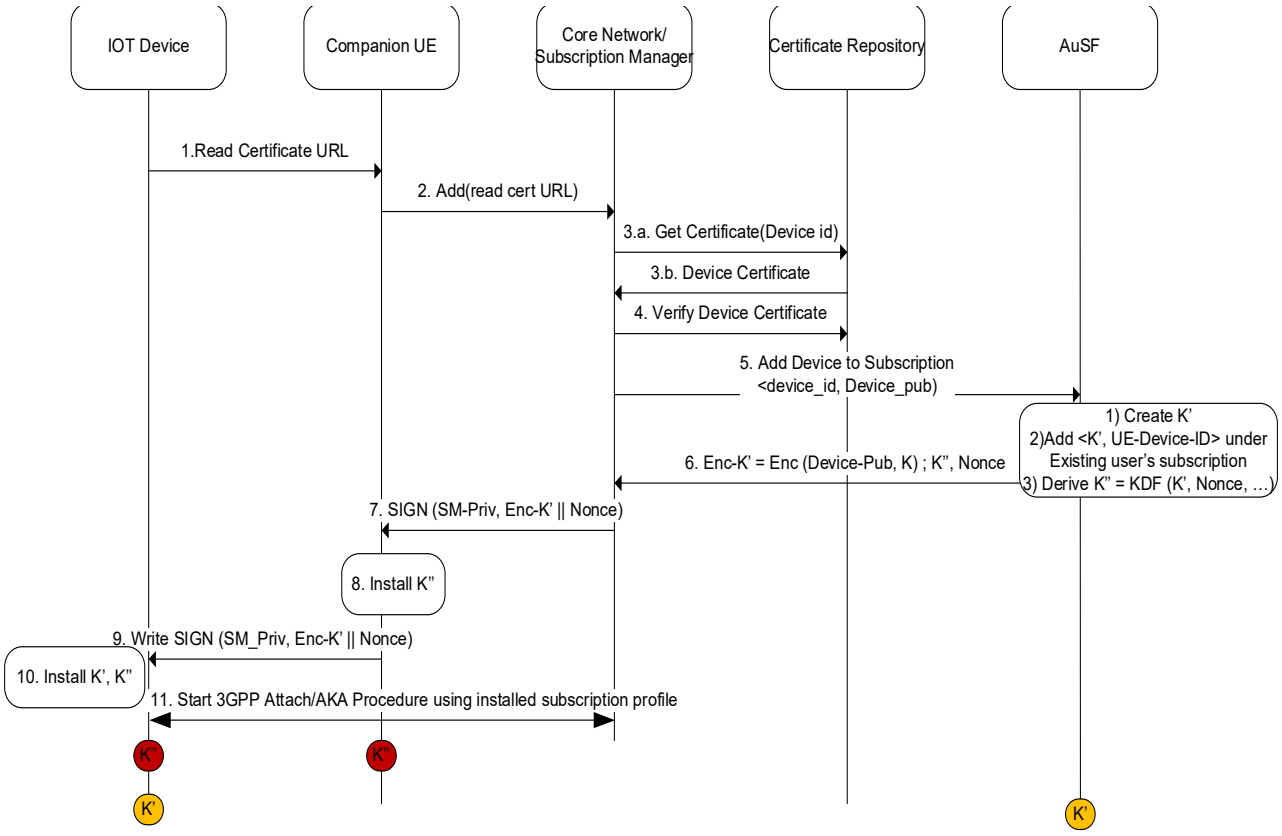


Figure 5.12.4.1.2-1: Credentials provisioning using Companion UE.

1) The user uses the companion UE to read to read URL pointer to the device certification and perhaps other information about device from the passive NFC tag on the IoT device. The URL also includes a unique identifier for this device – e.g., www.NextGenCertAuthority.com/DeviceID=xxxx.

2) The read URL is sent from companion UE to a specified functional component (hereafter, it is referred to as subscription manager) in the Core Network.

3) The subscription manager obtains the device certificate for this certificate URL from the Certification Authority.

4) Subscription manager verifies the certificate. The verification steps include verifying the chain of certificates all the way up to the root, verifying that the root is a trusted CA for this operator and verifying that the certificate is valid, meaning not expired and issued for the purpose for which it is used. The received device certification may also include additional information pertaining to the device such as, device serial number, manufacturer ID, etc.

5) Subscription manager will request the NextGen Authentication Server Function (AuSF) to add this IoT device to the existing companion UE's subscription. The request will includes a unique device identity, device public-key.

   a. Authentication Server Function derives a Master Key (hereafter it is referred to as K') for this IoT device. Then it encrypts the derived key with the device's public key (hereafter it is referred to encrypted K') and sent it to subscription manager in response.

6) Subscription manager derives a key to secure communication between the companion UE and IoT device, by using K', a nonce, IoT device information – hereafter this key is referred to as K''.

7) Subscription Manager creates a subscription profile for this IoT device (including encrypted K', NextGen Network Identity, Network assigned Identity for this device, etc.) and sends the profile, K'', the nonce used to generate K'' to the companion UE. For mutual authentication, Subscription Manager signs the profile, nonce using the private key of the Subscription Manager.

8) Companion UE installs K'' for this IoT device.

Lenovo Ex. 1007
Page 434

9) Companion UE sends the received subscription profile and the nonce (to generate K'') to the IoT device over NFC link.

10) IoT Device verifies the payload received using the public key of Subscription Manager. It also decrypts the subscription profile, nonce for K''. The device generates the K" and installs K', K''.

User resets the IoT device. Upon successful reset, the IoT device installs the profile and attempts to authenticate to the NextGen network.

5.12.4.1.3 Evaluation

Editor's Note: Evaluation content is FFS.

Editor's Note: The proposed solution needs to be evaluated against the existing GSMA solution (as described in GSMA's document "SGP .22: RSP Architecture") using a companion device in order to justify the motivation for having another solution.

Editor's Note: Evaluation of this solution for low power IOT devices is FFS.

5.12.4.2 Solution #12.2: Remote credential provisioning - for headed devices using captive portal technique

5.12.4.2.1 Overview

This proposed solution describes credential provisioning for headed Devices using Device credentials over NextGen Access. The solution uses the same model as used in Wi-Fi captive portal. Upon successful NextGen network discovery and selection, the device performs one-way authentication to the NextGen network in order to obtain a limited connectivity to access the subscription portal to complete sign-up process and download a subscription profile.

5.12.4.2.2 Solution Details.

Following pre-conditions are assumed:

1) Device is provisioned with device credentials at the manufacturing time. For example, public-private key pair and certificate URL that includes a pointer to Certificate Authority and a unique identifier of the device – e.g.., www.NextGenCA.com/DeviceID=xxxx.

Figure 5.12.4.2.2-1 shows high-level steps.

Lenovo Ex. 1007
Page 435

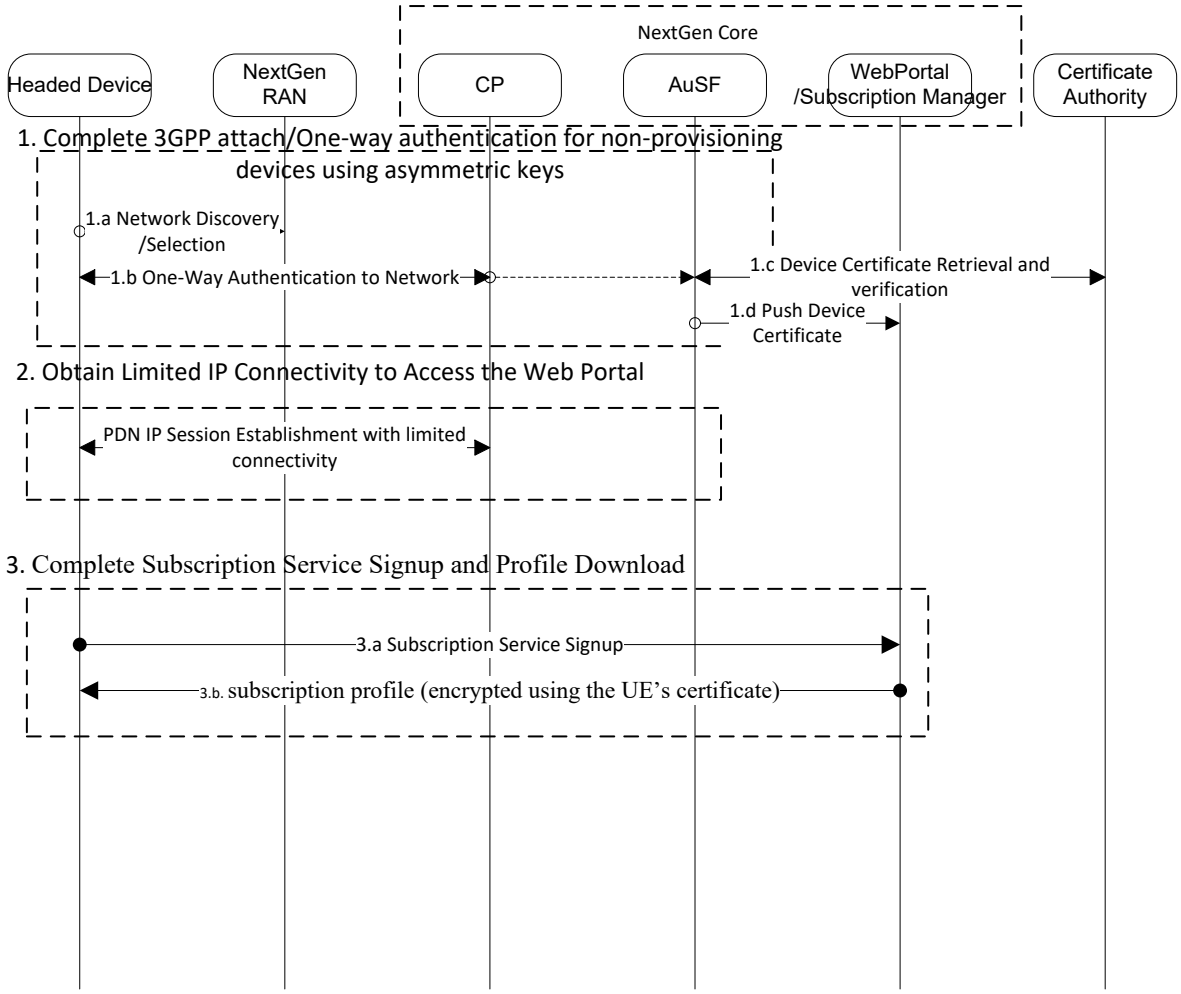


Figure 5.12.4.2.2-1: Credentials provisioning using captive portal technique

1. Device starts 3GPP Attach/One-way Authentication for non-provisioned device

    a. When device is turned on, it performs network discovery to find available NextGen Networks. The device may use a pre-configured policy to select a NextGen network or the selection can be made by the user's intervention.

    b. Device starts 3GPP Attach / one-way authentication procedure to authenticate to the network using asymmetric keys. During this procedures, the device provides the Certificate URL to the NextGen Core Authentication Server Function (AuSF).

NOTE: An optional network to device authentication is possible by the network providing a certificate as well. For the device to be able to check the certificate, the network may have to provide a certificate chain and the device should have a repository of trusted root certificates on board that it can use to check the validity of the chain.

    c. AuSF will retrieve and verify device certificate for this device

    d. Upon successful One-way authentication, the device certificate is made available to the Web Portal Subscription manager.

Editor's Note: Definition and protocol for 3GPP Attach / One-way authentication is FFS

2. Obtain limited IP connectivity to access web portal subscription manager

    a. Device establishes user plane bearer session with limited internet connectivity to access the web portal subscription manager

Editor's Note: User plane Bearer Session establishment for limited connectivity is FFS

Lenovo Ex. 1007
Page 436

3. Complete Subscription Service Signup and Profile Download

    a. Device is redirected to a web portal (provided by the NextGen system) so that the user can sign up for a subscription service.

        i. Also at this stage an additional authenticity check is possible. The web portal could use HTTPS with a certificate of the operator. The device could test the validity of the certificate, provided the network provides the certificate chain and the device trusts the root. Alternatively, the operator could allow access to the device manufacturer site so that the device can check an online repository of trusted root certificates.

    b. Upon successful service subscription sign-up, a subscription profile (encrypted using the device's certificate) is pushed to the device.

5.12.4.2.3 Evaluation

Editor's Note: Evaluation content is FFS

NOTE 1: The liability implications are an agreement between the operator and the provider of the certification authority; it is a business decision and not a security issue. In real life, cross-certification or a business decision to trust a certain CA always goes via lawyers on both sides. It is in those negotiations that the liability issues are dealt with and agreed.

5.12.4.3 Solution #12.3: Secure Mechanism to Achieve Remote Credential Provisioning for IoT devices

5.12.4.3.1 Introduction

This solution addresses key issue #12.2.

For UE (e.g. IoT device) equipped with Embedded UICCs (i.e. eUICC), it can initiate an attach to 3GPP network without its 3GPP subscription credentials using eUICC credentials i.e. eUICC certificate chain including eUICC certificate socalled Cert_eUICC and the eUICC manufacturer (EUM) certificate socalled Cert_EUM. It allows the UE to securely access a 3GPP network only dedicated for the purpose of remote provisioning. The detailed procedure is illustrated in Figure 5.12.4.3.2-1.

5.12.4.3.2 Solution details

Editor's Note: Whether the following procedure terminates in UE or eUICC is FFS.

1. UE sends Attach Request (Attach type, $RAND_{UE}$, Cert_eUICC, UE_Signature1) to CP-AU (i.e. Core Network Authentication function), in which the Attach type indicates UE accesss to the network without its 3GPP subscription credentials, Cert_eUICC is the certificate of the eUICC, and UE_Signature1 is generated by UE based on $RAND_{UE}$ and eUICC_ID.

    NOTE 1: When ME cannot find any 3GPP subscription credentials (e.g. USIM or GSM applications) available, ME sends request to initate eUICC to generate a random number $RAND_{UE}$ and a signature UE_Signature1 across $RAND_{UE}$ and eUICC_ID i.e. EID [49] that is the eUICC identifier. Then, eUICC sends response including $RAND_{UE}$, Cert_eUICC, and UE_Signature1 to ME.

    Editor's Note: How to protect the eUICC_ID is FFS.

    Editor's Note: How to prevent replay of parameters in Step 1 is FFS.

2. Upon receiving the Attach Request, CP-AU verifies the UE_Signature1 using the public key included in Cert_eUICC. If the verifications succeed, CP-AU continues the procedure, otherwise, it is aborted by CP-AU. In term of the received Attach type, CP-AU generates a random number $RAND_{AU}$, a Diffie-Hellman key pair (private key SK_AU and corresponding public key PK_AU), and futher generates its signature AU_Signature across $RAND_{UE}$, $RAND_{AU}$, and PK_AU.

    NOTE 2: CP-AU carries out SignatureUE verification to ensure the integrity of received message. In addition, Elliptic Curve Diffie Hellman would be a suitable key exchange algorithm.

Lenovo Ex. 1007
Page 437

NOTE 3: CP-AU could execute the certification revocation checking e.g. using CRL [51].

3. CP-AU sends User Authentication request (Cert_AU, AU_Signature, PK_AU, $RAND_{AU}$, $RAND_{UE}$) to UE, in which Cert_AU is the certificate of CP-AU.

   NOTE 4: CP-AU applies its certificate Cert_AU from the CA held by the operator it belongs to.

   NOTE 5: UE is assumed to have the public key of the operator.

4. After receiving the User authentication request, UE verifies Cert_AU and AU_Signature. If the verifications succeed, the network is authenticated by UE. Then, UE generates its Diffie-Hellman key pair (private key SK_UE and corresponding public key PK_UE) and uses the received PK_AU and its private key SK_UE to generate the session key $K_{session}$ which is used derive the related keys to protect the NAS and AS confidentiality and integrity. UE further generates UE_Signature2 accorss $RAND_{AU}$ and PK_UE.

   NOTE 6: eUICC in the UE applies the Cert_eUICC from GSMA CI which is different CA between CP-AU belongs to. Therefore, UE and CP-AU shall carry out cross-certification [50] to perform mutual authentication.

5. UE sends User authentication response (Cert_EUM, Cert_eUICC, UE_Signature2, PK_UE, $RAND_{AU}$) to CP-AU.

6. Upon receving User authentication response, CP-AU verifies Cert_EUM, Cert_eUICC and UE_Signature2. If the verifications succeed, UE is authenticated by network. Then CP-AU uses the received PK_UE and its private key SK_AU to generate $K_{session}$ which is used to derive the related keys to protect the CP and UP confidentiality and integrity, e.g. NAS and AS confidentiality and integrity.

7. CP-AU initiates related entities (e.g. UE, AN, and SCM (Security Context Management function)) to establish Security Context, e.g. NAS and AS confidentiality and integrity protection.

8. A PDU session is estabilised following the attach procedure.

9. After the PDU session establish successfully, the UE established HTTPS connection with the subscription preparation server to download the 3GPP subscription credentials of the attached PLMN.

   NOTE 7: UE downloads 3GPP subscription credentials from the subscription preparation server (e.g. Subscription Manager Data Preparation+ (SM-DP+) defined by GSMA), the detailed authentication and profile download and installation procedures refer to GSMA RSP specification [49].

   NOTE 8: The UE attaches to the PLMN network which the 3GPP subscription credentials to be downloaded belongs to. In this case the network should restrict the UE only to download the 3GPP subscription credentials using the connection established by a PDU session (e.g. a special DN name or APN), and the detailed procedure is addressed in SA2.

Lenovo Ex. 1007
Page 438

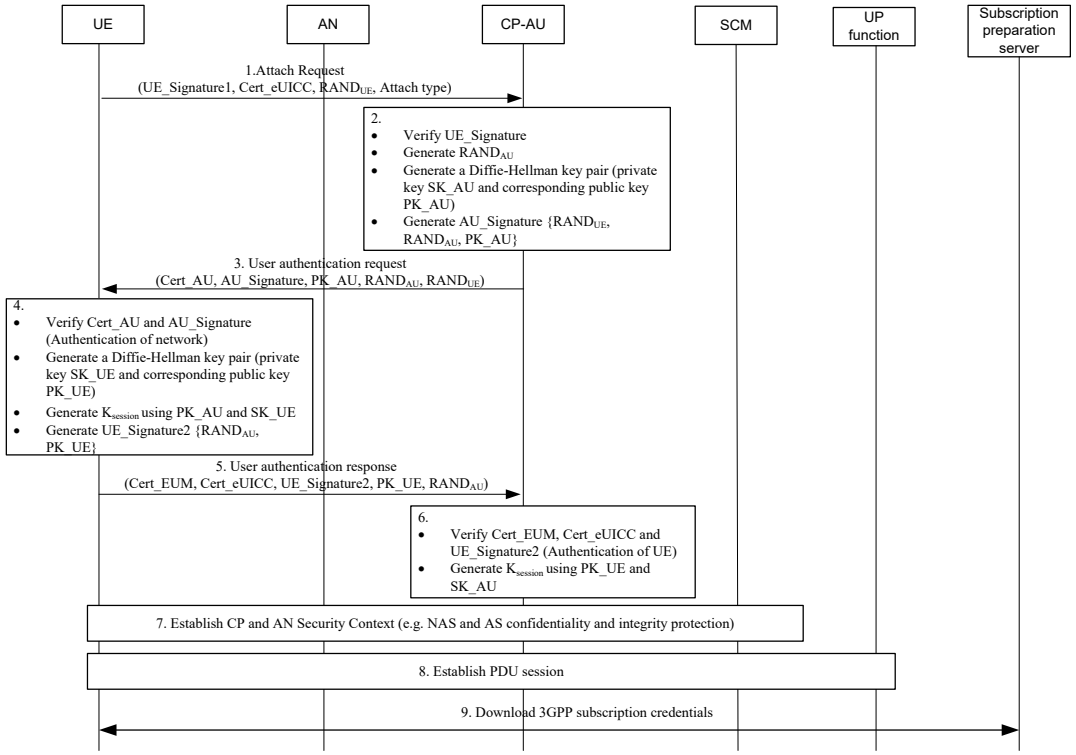


Figure 5.12.4.3.2-1: Secure Mechanism of Remote Credential Provisioning for IoT devices

Editor's Note: Using EAP-TLS as the authentication protocol is FFS.

5.12.4.3.3 Evaluation

FFS.

5.12.4.4 Solution #12.4 Authentication Procedure for credential provisioning

Editor's Note: The content of this whole clause needs to be reworded for clarity.

5.12.4.4.1 Introduction

The normal UE attaches to the network using its own 3GPP subscription credentials. When the UE has no USIM and any 3GPP subscription credentials are not provisioned yet, the LTE UE cannot attach and use the network for usual data network service except emergency services.

However, if the NextGen UE has an embedded UICC (i.e. eUICC) with pre-provisioned credentials which can afford to mutually authenticate with the NextGen Core using the 3rd Party authentication credentials. The NextGen System should supports the attachment of such a NextGen UE to enable the download of 3GPP subscription credentials via 3GPP network as described in this solution.

Lenovo Ex. 1007
Page 439

5.12.4.4.2 Reference Architecture for connectivity for credential provisioning

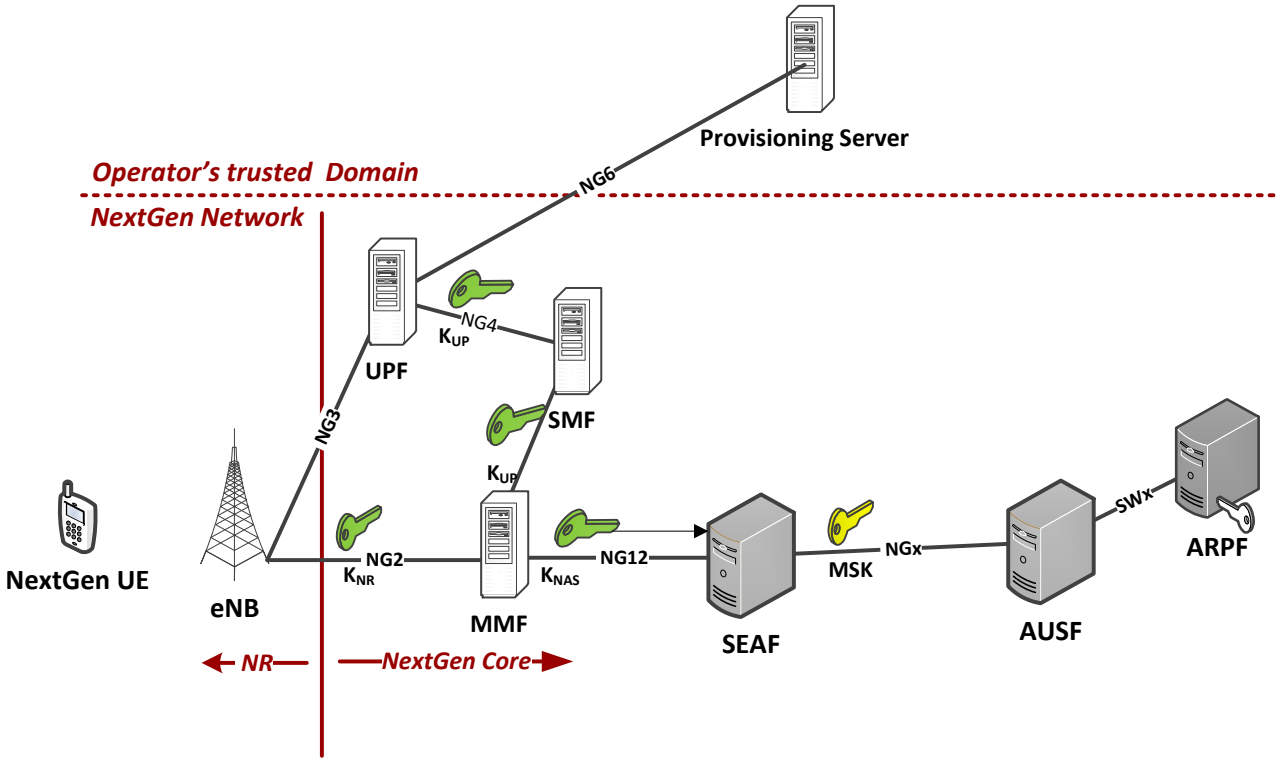


Figure 5.12.4.4.2-1: Reference Architecture for credential provisioning.

The use of 3rd party credentials for mutual authentication can be achieved in several ways, for example, the 3rd party domain may host a AUSF and the SEAF of the operator domain may interface with it, or alternatively, the AUSF of the 3rd party may be contacted via the AUSF proxy in the 3GPP operator domain. The potential candidate considered in this solution is, using direct interface between the AUSF of the 3GPP operator and the ARPF of the 3rd party domain. When such a NextGen UE attaches to the network for the credential provisioning, even if the NextGen UE attaches with the network for limited service successfully, the allowed data network services for the NextGen UE should be restricted only for the credential provisioning. In such a state, the subscriber is not identified from the NextGen CN, so the NextGen CN should manage the NextGen UE differently from the other normal registered NextGen UEs. And, on the successful remote provisioning, the NextGen UE should detach from the network and re-attach with the provisioned 3GPP subscription credentials.

Provisioning server should be placed within the Operator's trusted domain.

Lenovo Ex. 1007
Page 440

5.12.4.4.3 Authentication procedure for credential provisioning

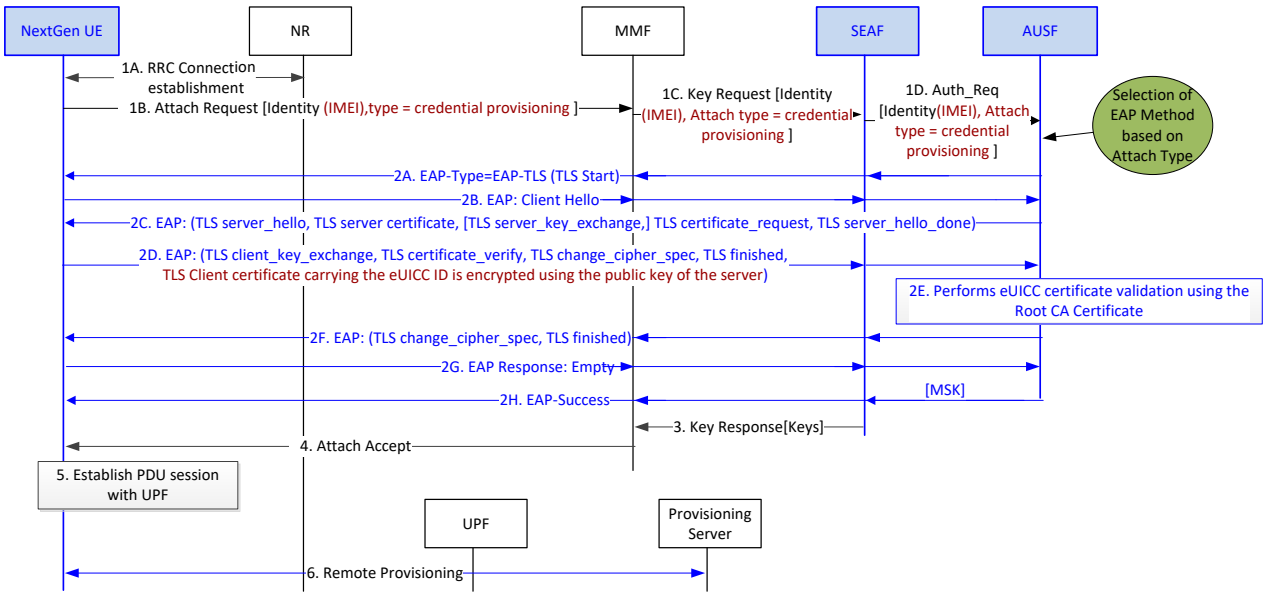


Figure 5.12.4.4.3-1: Attach procedure for UE without 3GPP subscription credentials

1. The NextGen UE sends the attach request message with a new attach type indicating that it is for remote SIM provisioning of the NextGen UE which has not been provisioned with any 3GPP subscription credentials. The NextGen UE identifier is set by the identifier of ME (e.g. IMEI) instead of IMSI. The IMEI check to the EIR may be performed. If the IMEI is blocked, operator policies determine whether the Attach procedure continues or is stopped. The MM function then triggers the authentication procedure through the SEAF. The AUSF initiates the EAP-TLS authentication procedure with the UE (i.e. eUICC in the UE).

2. The NextGen UE (i.e. eUICC in the UE) performs the mutual authentication with the AUSF. The 3rd Party ARPF- (for example, device manufacturer) and the eUICC in the UE, are pre-configured with the necessary credentials to perform EAP-TLS authentication. One option is to use the pre-provisioned eUICC credentials (e.g. eUICC certificate and its private key) defined in GSMA RSP specification SGP.02[49]. In order to verify the eUICC certificate, the AUSF is provisioned with the certificate of the root CA who issued the eUICC certificate, and to verify the server certificate, the eUICC is provisioned with the certificate of the root CA who issued the server certificate. One example of the Root CA for this purpose is the GSMA CI which is defined in SGP.02 [49].

   The TLS client certificate carrying the eUICC ID is encrypted by the public key of the AUSF before transmitting to the AUSF (step 2D). Alternatively, if asymmetric computation is a significant overhead for the NextGen UE, then the TLS client certificate carrying the eUICC ID is encrypted by the random key generated by the UE and the UE encrypts the random key using the public key of the AUSF. The UE transmits both encrypted TLS certificate carrying the eUICC ID and the encrypted random key to the AUSF.

Editor's Note: Impact on TLS Handshake is FFS

3. If the authentication succeeds, then the AUSF provides the MSK key to the SEAF. The SEAF derives further keys and provides the respective keys to the NR, UPF and MMF. The UE also derives the necessary keys. Then the NextGen UE and the NextGen core network and NR share the security contexts derived from the authentication results. From this point, CP and UP messages are confidentiality and/or integrity protected.

4. The MMF creates the session and sends the Attach accept message to the NextGen UE if it accepts the NextGen UE to connect to the network for credential provisioning. This message may include some information such as the operator's SIM provisioning server address, to be used by the NextGen UE to perform the step 6.

5. The PDU session is established, where the PDU session is restricted to allow the NextGen UE to only access the SIM provisioning-related servers (e.g. DNS server, SIM provisioning server such as SM-DP+ and SM-DS, or the operator's subscription portal, and so on.). During this step, the information obtained by the MMF (e.g. operator's SIM provisioning server address) in the step 4 may be used to configure the restriction rule of the PDU session.

Lenovo Ex. 1007
Page 441

Editor's Note: It's FFS how to restrict the UE traffic over the PDU session. It will depend on the design of SM procedures defined by SA2.

6. After the PDU session is established successfully, the NextGen UE connects to the SIM provisioning server and downloads the 3GPP subscription credentials (e.g. based on GSMA RSP specification SGP.02 [49]).

   NOTE: This step and provisioning of AKA credentials to the ARPF of the operator's network are out of the scope of 3GPP specification.

After the 3GPP subscription credentials are downloaded successfully, NextGen UE detaches from the network.

The 3GPP subscription credentials are activated and the NextGen UE attaches to the NG network as the normal attach (AUSF fetch the subscriber credentials for authentication from the ARPF of the operator's network).

5.12.4.4.4 Evaluation

5.12.4.5 Solution #12.5: Network access for credentials provisioning

5.12.4.5.1 Introduction

This solution addresses Key Issue #12.2 Remote credential provisioning for IoT devices.

The solution proposes a general framework for network access for credentials provisioning. The actual provisioning process is out of scope for this solution.

5.12.4.5.2 Solution details

5.12.4.5.2.1 Credentials and identifiers used for network access for credentials provisioning

In this solution, it is assumed that the UE is not pre-provisioned with any 3GPP subscription credentials. Furthermore, it is assumed that the network access for credentials provisioning is authenticated. In order for the UE to authenticate itself towards the network, the UE needs to have some sort of credentials. In this solution, we use the name "provisioning credentials" for the credentials used for authentication for network access for credentials provisioning. As the UE is not pre-provisioned with 3GPP subscription credentials, the provisioning credentials cannot be related to a subscription. As an example, the provisioning credentials could include certificates, and instead of being related to a subscription, they could be related to a business agreement to accept this kind of certificate for network access for credentials provisioning.

NOTE: It is in the scope of the security areas #5 'Security within NG-UE' to decide which function stores the provisioning credentials.

It is expected that some kind of identifier is needed for access to a NG network. Because the provisioning credentials are not related to a subscription, they will probably not include a 3GPP subscription identifier (e.g., IMSI). Hence, the UE needs to have a provisioning identifier as well. This provisioning identifier could, but need not, be identical to the equipment identifier (e.g., IMEI).

There are other solutions in this Security area that use provisioning credentials and provisioning identifiers for network access for credentials provisioning. Solution #12.2 uses a public-private key pair and certificate URL that includes a pointer to Certificate Authority and a unique identifier of the UE. Solution #12.3 uses the eUICC-certificate and eUICC-ID. Solution #12.4 uses the equipment identifier and pre-configured credentials. The term "provisioning credentials" introduced in this solution is a more general term that includes the credentials and identifiers used in solutions #12.2, #12.3 and #12.4, but possibly also other types of credentials and identifiers, as long as they are not related to a subscription.

The goal of the credentials provisioning process is to provision the UE with 3GPP subscription credentials that it can use for general network access. The 3GPP subscription credentials could be AKA-credentials, as for the GMSA remote provisioning specification (e.g. SGP.02 [49]), but also other types of 3GPP subscription credentials.

5.12.4.5.2.2 Network access for credentials provisioning

Editor's Note: More detail should be added to this solution to describe how it mitigates the threats detailed in security area 12.

Lenovo Ex. 1007
Page 442

This solution proposes to use EAP-methods for authentication, because they provide a general and well-studied framework for authentication. Examples for EAP-methods that can be used are EAP-TLS, EAP-TTLS and PEAP.

In Figure 5.12.4.5.2.2-1, high-level flows are provided for network access for credentials provisioning.

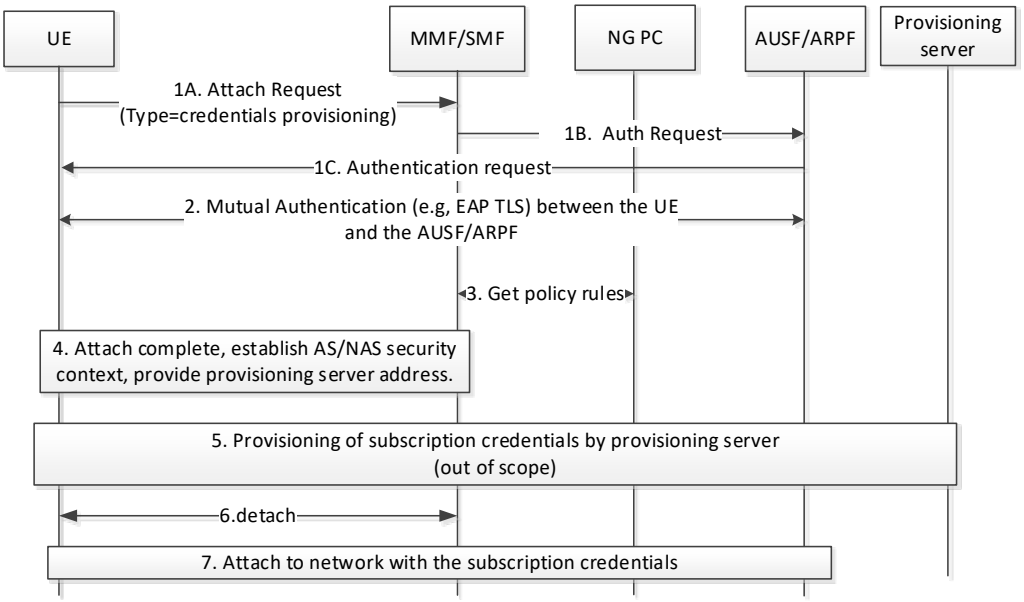


Figure 5.12.4.5.2.2-1: Network attach procedure for credentials provisioning

1. The UE sends the attach request message, with attach type credentials provisioning. The UE uses the provisioning identifier instead of the subscription identifier. The MM function triggers the authentication procedure with the AUSF/ARPF, which initiates the authentication procedure with the UE.

2. The AUSF/ARPF authenticates the UE using the provisioning credentials and an EAP method, e.g., EAP-TLS, EAP-TTLS or PEAP. The authentication process may also involve communication of the AUSF/ARPF with an external entity, e.g., a certificate authority or a 3rd party authentication server.

   The authentication process includes an authorization check whether the provided provisioning credentials may be used for network access for credentials provisioning for that UE.3. The SMF requests from the NG PC policy rules (i.e. QoS rules) related to the traffic flows the UE will be authorized to establish for remote provisioning of credentials. The SMF installs the received rules at the NG User Plane Function (NG-UPF not depicted). This ensures that the UE only uses the connection for the purpose of the remote provisioning of subscription credentials. The NG-UPF then enforces the policy rules.4. The MMF completes the attach request and establishes the security contexts. The MMF/SMF may provide information to the UE e.g. the address of the provisioning server that the UE is allowed to connect to according to the policy rules.

5. The actual provisioning process between the UE and the provisioning server takes place over User Plane signalling and is out of scope for this solution. The provisioning server may be outside the operator domain.

6. After the successful provisioning of the 3GPP subscription credentials, the UE detaches from the network. The detach may also be enforced by the network due to the policy rules, e.g., after a certain time.

7. The UE now uses its 3GPP subscription credentials to attach to the network for general access.

5.12.4.5.3 Evaluation

5.12.4.z Solution #12.z: <solution name>

5.12.4.z.1 Introduction

Editor's note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the security area.

5.12.4.z.2 Solution details

5.12.4.z.3 Evaluation

5.12.5 Conclusions

Editor's note: This clause will contain the evaluation between the solutions, and the conclusions made by SA3.

5.13 Security area #13: Security for Interworking and Migration

5.13.1 Introduction

This security area focuses on security aspects of migration and interworking scenarios.

Example interworking scenarios to consider are from EPC to NextGen core.

In addition, typical roaming scenarios between operators are studied in TR 23.799. For example the need for NextGen core of an operator to support roaming with partners that have not yet migrated to the NextGen core. Typically an MNO will not deploy a standalone Next Generation System right from the beginning, but rather deploy it in parts of his PLMN area in addition to an existing legacy 3GPP RAN.

Further NextGen core of an operator will need to support roaming with partners that have not yet migrated to the NextGen core. Thus migration strategies and interworking is required to maintain service for UEs changing between NextGen Radio (NR) and legacy 3GPP RAN. This key issue focuses on security aspects of migration and interworking scenarios based on the findings TR 23.799.

Several options of interworking and migration between radio technologies and possible core network concepts have been identified.

- Radio technologies to be considered are eLTE (Rel-15) and NR.
- Core Network concepts to be considered are EPC and Next Generation Core (NGCN).

This key issue should in particular address security aspects of

- handover mobility and
- idle mode mobility

when a NextGen system interworks with LTE/eLTE and vice versa, or other systems (e.g. WiFi). In the latter trusted and untrusted access needs to be considered.

Editor's Note: Mobility during inactive state may also have to be considered, depending on SA2 decisions.

Based on the identified migration and roaming scenarios the need for security in interworking solutions between the NextGen core network and EPC will be determined and related solutions will be discussed.

Possible deployment options (Option 3, 4, 5 and 7) for interworking between LTE/EPC and the NextGen System are collected in Annex J in TR 23.799 [2].

Interim agreements on EPC-NextGen Core interworking are collected in clause 8.11.1 of TR 23.799 [2]:

- The standard defined for mobility procedures from NG Core to EPC shall be able to support "single radio/single attach" UEs and achieve minimal service disruption.
- Support for these procedures in the network is optional and is based on network capabilities.
- Common UP anchor is required for IP address preservation.
- A common subscriber database (similar to HSS) is used between EPC and NG Core.
- The standard shall support a source to target CN interface to transfer certain context between MME and CP Function of NG Core.

Lenovo Ex. 1007
Page 444

5.13.2 Security assumptions

Editor's Note: This clause will document security assumptions related to each security area.

Assumption: no SRVCC in NextGen, no interworking with GSM/GPRS, UMTS.

Furthermore, it is assumed that mobility scenarios can be considered separately for core network and radio access network.

Editor's Note: It is ffs whether this assumption is warranted. It is to be verified e.g. whether we will use the same key derivation scheme as for (e)LTE with the vertical and horizontal handovers.

5.13.3 Key issues

5.13.3.1 Key issue #13.1: Security for Handovers

5.13.3.1.1 Key issue details

NOTE: (e)LTE access networks can be attached to NextGen Core.

Security for the various handover scenarios needs to be considered:

Core network:

- UE moves inside NextGen Core (while changing radio access technology)
- UE moves between EPC and NextGen Core

Radio access:

- UE moves between NR and (e)LTE
- UE moves between NR and non-3GPP access
- UE moves between (e)LTE and non-3GPP access

Editor's Note: the above list needs to be checked for completeness. This may also depend on decisions in SA2.

5.13.3.1.2 Security threats

5.13.3.1.3 Potential security requirements

5.13.3.2 Key issue #13.2: Security for Idle Mode Mobility

5.13.3.2.1 Key issue details

NOTE: (e)LTE access networks can be attached to NextGen Core.

Security for the various idle mode mobility scenarios needs to be considered:

Core network:

- UE moves inside NextGen Core (while changing radio access technology)
- UE moves between EPC and NextGen Core

Radio access:

- UE moves between NR and (e)LTE
- UE moves between NR and non-3GPP access
- UE moves between (e)LTE and non-3GPP access

Lenovo Ex. 1007
Page 445

Editor's Note: the above list needs to be checked for completeness. This may also depend on decisions in SA2.

5.13.3.2.2 Security threats

5.13.3.2.3 Potential security requirements

5.13.3.3 Key issue #13.3: Security aspects of migration

5.13.3.3.1 Key issue details

Typical roaming scenarios between operators are studied in TR 23.799. For example the need for NextGen core of an operator to support roaming with partners that have not yet migrated to the NextGen core.

This key issue is introduced to study any security issues that may arise due to migration.

Interim agreements on option 3 to NG Core migration are collected in clause 8.11.2 of TR 23.799 [2]:

- Solution 18.3 for migration from E-UTRAN/EPC including option 3 to NG Core options has been selected
- RAN related aspects of migration e.g. related to RRC or user plane will be addressed by RAN WGs

Solution 18.3 in TR 23.799 [2] is a solution for migration from E-UTRAN/EPC including Option 3 to Option 2,4,5, or 7.

For the deployment options, see Annex J in TR 23.799 [2].

5.13.3.3.2 Security threats

5.13.3.3.3 Potential security requirements

5.13.3.4 Key issue #13.4: Bidding down to an older 3GPP generation or a non-3GPP access technology

5.13.3.4.1 Key issue details

NextGen systems will be operated alone or in interworking scenarios with other systems, which also include earlier 3GPP generations and non-3GPP access. Nonetheless, 5G is expected to provide enhanced security features compared to earlier generations, e.g. enhanced user identity confidentiality.

An attacker may impersonate a base station to attract UEs with weaker security. Such bidding down attacks have been a problem in earlier generations of 3GPP systems. For example, an LTE-capable phone was tricked into attaching to a false GSM base station and, in this way, accepted weak GSM security. 5G systems should specifically pay attention to mitigate such attacks.

5.13.3.4.2 Security threats

An attacker masquerades as false network and forces NG UEs to use no security or weak security, by making the UE believe that there was no 5G coverage. Thus NG UEs are tempted to connect to a false network offering an older 3GPP generation or a non-3GPP access technology. Using weaker security makes it easy to further attack the NG UE, e.g. to eavesdrop, intercept or modify the communication data.

Thus, even in spite of enhanced 5G security features as envisioned in 5G, bidding down attacks, e.g. IMSI catching, could still be successful and would harm NG UEs.

5.13.3.4.3 Potential security requirements

It shall be possible for a NG UE to limit its system selection to only systems with 5G security capabilities

Lenovo Ex. 1007
Page 446

5.13.4 Solutions

5.13.4.1 Solution #13.1:

5.13.4.1.1 Introduction

This solution is related to key issue 13.4.

5.13.4.1.2 Solution details

To limit NG-UE's system selection to only systems with 5G security capabilities, the NG-UE could be set manually by the user or by a policy configured in the UE.

NOTE: Such settings were possible in earlier phone generations, e.g. in new UMTS phones, but they seem to have disappeared from present-day phones.

5.13.4.1.3 Evaluation

5.13.4.z Solution #13.z: <solution name>

Editor's Note: Solutions within the security area are not in any particular order but they are added incrementally (z = 1, 2, 3…) when new solution is identified. 'x' refers to the security area.

5.13.4.z.1 Introduction

Editor's note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the security area.

5.13.4.z.2 Solution details

5.13.4.z.3 Evaluation

5.13.5 Conclusions

Editor's note: This clause will contain the evaluation between the solutions, and the conclusions made by SA3.

5.14 Security area #14: Security aspects of small data

5.14.1 Introduction

To address massive number of IoT UEs that usually send small amounts of data sporadically and also moves around, different solutions have been proposed in TR 23.799. In all the proposals UE sends data to the NextGen Core via a user plane path without requiring more signalling to set up and tear down dedicated bearers. No additional signalling to the network (RAN and Core) is expected than the amount of user data to be transferred on this interface, which is referred here as small data interface. Some of the solutions envision occasional signalling for setup and management of the small data interface.

Once the PDU session for the UE has been set-up, in order for the UE to be able to send or receive data on the small data interface, no dedicated connection for the UE needs to be setup on the RAN-Core interfaces NG2 or NG3.

In some scenarios, PDU session setup may not be necessary.

5.14.2 Security Assumptions

The UE gets authenticated and Attaches to the network. Based on the service required, UE sets up PDU sessions, the session set up may or may not involve set up of special context sending small data. Following are the general security assumptions for the small data feature

Lenovo Ex. 1007
Page 447

- UE has a session and security context established, control plane context in the Controller and user plane context in User Plane Gateway.
- UE may or may not have AS context established in the RAN, the AS context is not used to small data packets
- There is no dedicated signalling exchange specific to the UE between the RAN and the Core, there is no UE specific security in the RAN. The security and header decompression of the user plane packets are handled in the NextGen Core (in the UPGW part of the NextGen Core). Security algorithms, Compression algorithms etc are negotiated between the UE and the CN during the PDU Session set up. Security keys are derived are also derived at the UE and CN during the session set up.
- The MM procedures (e.g. ATTACH, authentication, Tracking Area Update ,etc) are independent from whether the UE has a small data transmission mode .
- When the UE is already attached to the network and has established a PDU session, to send UL data.
- There is no NG2 signalling exchange dedicated to the UE between the RAN and the Core.
- There is no NG3 data plane connection dedicated to the UE between the RAN and the Core

In some scenarios, the setup of a PDU session before UE sends a small data packet is optional. In those scenarios the network can validate the data packet based on the information in that packet.5.x.3 Key Issues

5.14.4 Solutions

5.14.5 Key issues

5.14.3.1 Key Issue #14.1: Access security for small data session

5.14.3.1.1 Key issue details

Since there are no specific signaling needed to access the small data bearer, eNB Access Stratum radio bearers for the small data access need to be secured or restricted. Since the service is for sporadic bursts of small data, UEs should be prevented from accessing the interface for other services.

5.14.3.1.2 Security threats

If the eNB access is not secured, there could be attacks on the NextGen network in general and the small data access interface in particular. Hacking in to NextGen network using small data access is potential threat to be avoided.

5.14.3.1.3 Potential security requirements

eNB access for sending data on the small data interface needs to be protected to prevent un authorized UEs accessing small data interface or hacking in to network.

5.14.3.2 Key Issue #14.2: Security for data over the small data interface.

5.14.3.2.1 Key issue details

Data sent over the small data interface need be protected for privacy and integrity. It should be possible to encrypt the data and prevent any manipulation of data.

5.14.3.2.2 Security threats

Without security, data sent over the small data interface may have no privacy.

Without security data sent over the small data interface could be manipulated.

Lenovo Ex. 1007
Page 448

5.14.3.2.3 Potential security requirements

It should be possible to encrypt and or integrity protect the data sent over the small data interface, with minimum overhead.

5.14.3.3 Key Issue #14.3: Restricting small data resource utilization

5.14.3.3.1 Key issue details

Since the small data interface is for transmitting small data packets in frequently, and there is no dedicated signaling to setup radio bearers, UEs may repeatedly access the small data interface and keep sending data hogging the resources and creating DOS attacks.

5.14.3.3.2 Security threats

UEs constantly sending data packets over the small data interface may cause DOS attacks.

5.14.3.3.3 Potential security requirements

UEs accessing small data interface need to be restricted for their frequency of access as well as amount of data (packet size) send on the interface. UEs sending data more than the size of allowed packet size need to be signaled to be in the regular connected mode. UEs sending data more frequently than allowed frequency of transmission need to signaled to be in connected mode.

5.14.3.4 Key Issue #14.4: Small data context retention

5.14.3.4.1 Key issue details

Since the small data interface is for transmitting small data packets in frequently, the UEs may stay in Idle/power saving mode for a long time without any activity. Authenticating UEs at every transmission occasion may consume power and drain the battery, hence this need to be avoided too. Hence solutions which doesn't need a specific context to be retained either in the UE or in the network are also to be studied.

5.14.3.4.2 Security threats

UE and the UPGW need to keep the small data security context for a long time. If security context is leaked, the session could be hijacked.

5.14.3.4.3 Potential security requirements

UE and UPGW need to keep the security context active for a long duration of time securely. The duration of context retention may be known to both UE and the UPGW or may not be known to both UE and the UPGW

It should be possible for the network to challenge and verify the UE periodically and re-authenticate the UE for the small data service.

5.14.4 Solutions

5.14.4.z Solution #14.z: <solution name>

Editor's Note: Solutions within the security area are not in any particular order but they are added incrementally (z = 1, 2, 3…) when new solution is identified. 'x' refers to the security area.

5.14.4.z.1 Introduction

Editor's note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the security area.

Lenovo Ex. 1007
Page 449

5.14.4.z.2 Solution details

5.14.4.z.3 Evaluation

5.14.5 Conclusions

Editor's note: This clause will contain the evaluation between the solutions, and the conclusions made by SA3.

5.15 Security area #15: Broadcast/Multicast Security

5.15.1 Introduction

NextGen System will provide broadcast services (TR 23.799, clause 4). Broadcast/Multicast will be used in verticals, for example MCPTT, Critical Communication, V2X, and massive MTC. Specific solutions proposed in TR 23.799 such as1:many and 1:all communication, group handling, group communication need to be analysed with respect to security.

This security area will study functionality needed to satisfy security for current and emerging 3GPP broadcast/multicast requirements and application architecture requirements (e.g. MCPTT, MCVideo, MCData, CriC, and massive MTC).

This security area is addressing "MBMS security" and will cover aspects such as Broadcast/Multicast capabilities has been defined in TR 23.799, clause 5.13.

Editor's Note: It should be noted that SA2 have put the key issue on Broadcast/Multicast to phase 2 in their meeting in July 2016.

5.15.2 Security assumptions

Editor's Note: This clause will document security assumptions related to each security area.

5.15.3 Key issues

5.15.3.1 Key issue #15.1: Broadcast/Multicast capabilities

5.15.3.1.1 Key issue details

LTE/eLTE features, e.g. GCSE/MCPTT or V2X, already use or will use multicast / broadast capabilities. This key issue should study, whether additional security considerations are needed within the NextGen architecture concept.

5.15.3.1.2 Security threats

5.15.3.1.3 Potential security requirements

5.15.3.2 Key issue #15.2: Usage of MBMS security

5.15.3.2.1 Key issue details

MBMS security is specified in 3GPP TS 33.246 [18]. This key issue should study its application to NextGen architecture and whether additional functional implications result from it.

Lenovo Ex. 1007
Page 450

5.15.3.2.2 Security threats

5.15.3.2.3 Potential security requirements

5.15.4 Solutions

5.15.4.z Solution #15.z: <solution name>

Editor's Note: Solutions within the security area are not in any particular order but they are added incrementally (z = 1, 2, 3…) when new solution is identified. 'x' refers to the security area.

5.15.4.z.1 Introduction

Editor's note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the security area.

5.15.4.z.2 Solution details

5.15.4.z.3 Evaluation

5.15.5 Conclusions

Editor's note: This clause will contain the evaluation between the solutions, and the conclusions made by SA3.

5.16 Security area #16 Management security

Editor's Note: A more appropriate name of this security area is FFS.5.16.1 Introduction

Security of network management and deployment is always one of the key security topics. Some of the existing concerns in traditional networks, e.g. in LTE system are carried over, even in next generation networks. In TS 33.401, the management security is discussed in Section 5.3, Chapter 12 and 13. The deployment is also discussed in Section 5.3 and also in TS 33.310.

In the next generation network, several changes can introduce difficulties into network management and deployment:

- The network architecture evolution.
- The introduction of network virtualization.
- The deployment location of network functions.
- The open of management interfaces.

The impacts brought by those changes are discussed in the key issue sections.

5.16.2 Security assumptions

Editor's Note: This clause will document security assumptions related to each security area.

Lenovo Ex. 1007
Page 451

5.16.3 Key issues

5.16.3.1 Key issue # 16.1: management plane communication protection

5.16.3.1.1 Key issue details

Protecting the communication between the manager and the managed network elements or network functions are the basic feature of the management security. Chapter 13 of TS 33.401 gives the protections for management plane over S1 interface. In next generation, should consider two more scenarios:

- The AN and CN function could be deployed in unsecure domain.
- The communication between NE and Manager could pass virtualized network. The infrastructure might be not owned by network operator.

Both scenarios show the management plane communication can be subject to external attacks. Especially in the virtualized environments, it is hard to know whether communication is internal or external. Therefore, the protections on S1 interface should be deployed in all management communications.

Editor's Note: Whether management plane security needs to be taken account for Next Gen is FFS.

5.16.3.1.2 Security threats

All threats to management functions, i.e. the FCAPS functions. The attackers could

- Disclosing or tampering the software, configuration in NEs, and thereafter attacking the network functions or attacking other NEs via the compromised NEs.
- Attacking the OM center from compromised NEs.
- Spoofing or interrupting services or privacy of UEs.

5.16.3.1.3 Potential security requirements

The security requirements are:

- Network management entities shall be mutually authenticated and authoirized before establishing management plane communication.
- Management plane communication shall be confidentiality- and integrity-protected.

5.16.3.2 Key issue #16.2: network element deployment security

5.16.3.2.1 Key issue details

NEs could be deployed and commissioned by local or remote configuration, or the combination of local and remote operation. The automatical deployments are studied in LTE and the corresponding security protections are discussed in TS 33.310.

In next generation, low cost and quick deployment is required. The requirements should suit both the "ultra dense" and the "virtualized infrastructure" characrastics. Both are required to minimize manual operations and rely on automated operations as much as possible. The automated operations should be protected and, the provisioning of security related credentials, trust roots and policy configurations should be done in a secure way.

5.16.3.2.2 Security threats

Attackers could

- Faking NEs connecting to OM center or connecting to network.
- Faking OM center to disclose or tampe the software, configuration in NEs, and thereafter attacking the network functions or attacking other NEs via the compromised NEs.

Lenovo Ex. 1007
Page 452

- Attacking the OM center from compromised NEs.
- Steal credentials of NEs.
- Spoofing or interrupting services or privacy of UEs.

5.16.3.2.3 Potential security requirements

- NE and OM center shall be mutually authenticated, e.g. during remote or local provisioning.
- NE and OM center shall be authorized to communicate with each other, e.g. during remote or local provisioning.
- NE credentials and NE trust list, verification materials shall be securely provisioned..
- Communication between NE and OM center shall be confidentiality- and integrity-protected during provisioning.

5.16.3.3 Key issue #16.3: Network slice life-cycle security

5.16.3.3.1 Key issue details

In TR 28.801 a network slice life-cycle is described to have thesephases:

- Preparation phase
- Instantiation, Configuration and Activation phase
- Run-time phase
- Decommissioning phase

Securing the life-cycle of a network slice should cover all phases to avoid ending up with vulnerabilities in any of the phases that can compromise the security of the network slice. A vulnerability can be introduced in one phase and be exploited in another phase (e.g a poorly designed network slice blueprint could have vulnerabilities that are exploited in the run-time phase).

Some security aspects of network slices are being handled by other key issues and solutions in this document. The purpose of this key issue is to act as an overview to make sure all security aspects of the network slice life-cycle phases are covered.

- In the **Preparation phase** topics such as creation and verification of network slice blueprints are handled.
- In the **Instantiation, Configuration and Activation phase** the network slice is configured, instantiated and eventually activated
- In the **Run-time phase** the network slice is used, supervised, upgraded and reconfigured.
- During the **decommissioning phase** the network slice is deactivated. This includes removing dedicated resources and configurations. If there is information (e.g auditing information) that needs to saved, this happens during this phase. After this phase, the network slice is no longer in existence.

5.16.3.3.2 Security threats

A general comment regarding security threats is that if security aspects are not analysed on the entire life-cycle of a network slice, vulnerabilities may be overlooked or introduced in one phase and be exploited in other phases.

- Preparation phase
  - If an attacker (insider or outsider) is able to compromise a network slice blueprint a vulnerability (e.g inserting some kind of malware such as a Trojan or an Advanced Persistent Threat (APT)) can be introduced that can affect all network slices based on the blueprint.
  - Lack of hardening (Hardening entails removing unnecessary functionality from for instance an OS, e.g removing unnecessary software and closing unnecessary ports) of network slice blueprints can introduce

Lenovo Ex. 1007
Page 453

vulnerabilities (e.g if software that is considered untrusted such as telnet is not removed from an OS it can be used by an attacker to gain control of for instance a network element) that can affect all network slices based on the blueprint.

- Security design flaws in network slice blueprints can introduce vulnerabilities (e.g not establishing a password policy that requires strong passwords or two factor authentication) that can affect all network slices based on the blueprint.
- Failing to incorporate security patches (e.g using unpatched virtual machine templates) can result in vulnerabilities (an example from 2014 of this kind of vulnerability is "Heartbleed") that can affect all network slices based on the blueprint.

- Instantiation, configuration and activation phase
  - APIs exposed to instantiate, configure and activate network slices could be compromised.

Editor's note: Further clarification on API is needed.

- Run-time phase
  - A network slice in use may be attacked due to lack of security controls such as the ones described in security area #8.
  - APIs exposed to tenants used for supervision and management could be compromised.
  - Failing to incorporate security patches may over time degrade the security level if known vulnerabilities (a well-known source of information regarding reported vulnerabilities is CVE (Common Vulnerabilities and Exposures) in for instance hypervisors or virtual machines are left unpatched.
- Decommissioning phase
  - If not all resources and configurations are removed when deactivating the network slice instance, attackers may be able to use the resources left behind to perform attacks.
  - When deactivating the network slice there may be information (e.g auditing information) that needs to be saved for bookkeeping or for legal reasons. If this information is not handled in a secure way (e.g encrypting stored data) it may be used by an attacker to get valuable information about the network slice tenant and users.

Editor's note: These security threats should not be considered as an exhaustive list. Further security threats are FFS.

5.16.3.3.3 Potential security requirements

Editor's note: Solutions addressing this key issue will be considered in Phase 2.

5.16.3.y Key issue #16.y: <key issue name>

5.16.3.y.1 Key issue details

5.16.3.y.2 Security threats

5.16.3.y.3 Potential security requirements

5.16.4 Solutions

5.16.4.z Solution #16.z: <solution name>

5.16.4.z.1 Introduction

Editor's note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the security area.

Lenovo Ex. 1007
Page 454

5.16.4.z.2 Solution details

5.16.4.z.3 Evaluation

5.16.5 Conclusions

Editor's note: This clause will contain the evaluation between the solutions, and the conclusions made by SA3.

5.17 Security area #17: Cryptographic algorithms

5.17.1 Introduction

This clause deals with cryptographic algorithms for Next Generation System.

5.17.2 Security assumptions

Security mechanisms and protocols rely on the use of cryptographic algorithms.

5.17.3 Key issues

5.17.3.1 Key issue #17.1: Cryptographic algorithms for backward compatibility

5.17.3.1.1 Key issue details

Next Generation System is expected to be backward compatible with SAE/LTE. SAE/LTE security relies on a list of cryptographic algorithms optional or mandatory to support.

5.17.3.1.2 Security threats

The use of unsecure or deprecated cryptographic algorithms according to today state of the art in cryptography results in compromising security mechanisms (e.g confidentiality or integrity of transmitted data), or in compromising security protocols (e.g. TLS).

5.17.3.1.3 Potential security requirements

Next Generation System shall support a list of cryptographic algorithms enabling the backward compatibility with SAE/LTE security. This list of algorithms shall reflect the today state of the art in cryptography (confer [52], [53]).

5.17.3.2 Key issue #17.2: Quantum safe cryptography

5.17.3.2.1 Key issue details

Current asymmetric cryptographic algorithms in use nowadays, and largely deployed, will be considerably impacted by the arrival of large-scale quantum computers. Even if the date of arrival of quantum computing era with large-scale quantum computers for code-breaking is an open question, Next Generation System will probably be on the field when quantum computers become a reality.

Several reports on Quantum Safe Cryptography exist; confer [54] and [55].

Shor's algorithm will practically break all currently standardized public-key algorithms, including RSA, Elliptic-Curve Cryptography (ECC), Diffie-Hellman, and pairing-based crypto. With Shor's algorithm, today's public-key algorithms lose almost all security, and increasing the key length does not help much.

Quantum computers would also have a theoretical impact on symmetric cryptography. Grover's algorithm can invert any function using only $\mathcal{O}(\sqrt{N})$ evaluations, where N is the number of possible inputs, e.g. cryptographic keys. But Grover's algorithm cannot be effectively parallelized, and together with the higher cost and lower clock rates, this

Lenovo Ex. 1007
Page 455

means that a cluster of classical computers will likely remain the most cost-efficient way to break symmetrical crypto. It is unknown if Grover's algorithm will ever be relevant for practical cryptanalysis.

3GPP should wait until publicly evaluated PQC algorithms have been standardized. Introducing algorithms that has not been publicly evaluated for many years introduces more risks than it eliminates. 3GPP should mandate implementation of post-quantum cryptography as soon as public evaluated algorithms have been standardized. Actions should be aligned with IETF standardization of TLS, IKEv2, and X.509. 3GPP should aim to deprecate non-quantum safe algorithms before large enough quantum computers emerge. Timely introduction of post-quantum cryptography enables this.

Editor's Note: UE capabilities needed for quantum resistant cryptography are ffs.

5.17.3.2.2 Security threats

At the arrival of large-scale quantum computers for code-breaking, the currently used algorithms based on asymmetric cryptography will be broken.

Some examples of asymmetric algoritms that will be no longer secure:

- RSA, DSA or ECDSA for digital signatures
- DH, ECDH for key exchange.

AES is considered as quantum safe since the cipher can adapt to resist quantum computing attacks by increasing the length of keys.

Editor's Note: Selection of appropriate key lengths used for symmetric key algorithms, hash functions, and the associated message authentication codes generated, to be quantum-safe is FFS.

Editor's Note: It is FFS whether AES-128 and SHA-256 are quantum secure as well.

New quantum-safe asymmetric cryptography is needed (to replace RSA, ECDSA…); some alternatives, based on coding theory, lattices, hash functions, multivariate equations, and supersingular elliptic curves, are under being studied but need more time for scrutinization by the crypto community.

Quantum-resistant cryptographic algorithms that have not been sufficiently publicly evaluated may have weaknesses that would have been discovered in the public evaluation.

5.17.3.2.3 Potential security requirements

Next Generation System shall be able to support cryptographic algorithms that can resist quantum computing attacks.

Next Generation System shall enable transition to quantum safe cryptography.

The use of quantum cryptographic algorithms known to be resistant against quantum computer attacks shall be considered in priority when designing new security mechanisms and protocols.

The quantum-resistant cryptographic algorithms supported by the Next Generation system shall be standardized and have been publicly evaluated for many years.

Lenovo Ex. 1007
Page 456

5.17.3.y Key issue #17.y: <key issue name>

5.17.3.y.1 Key issue details

5.17.3.y.2 Security threats

5.17.3.y.3 Potential security requirements

5.17.4 Solutions

5.17.4.1 Solution #17.1: Incorporate a quantum safe algorithm from day one

5.17.4.1.1 Introduction

This solution addresses key issue #17.2.

5.17.4.1.2 Solution details

We anticipate that a set of public key algorithms will be specified as mandatory to support (by various entities, potentially including UICC, UE, serving network nodes and home network nodes) in the NextGen security specification.

When the NextGen security specification is created, at least one "best known in class" quantum safe algorithm is included in this set of mandatory to support algorithms. By "best known in class" we mean the algorithm deemed best by SA3 (taking suitable advice from other sources) in terms of

- being believed safe against cryptanalysis by quantum computers;
- efficiency (computing time, signature size etc).

We deliberately avoid selecting such an algorithm in this TR. The selection of the algorithm(s) should be left as late as is reasonably possible, to allow for new results in the very active, not yet mature field of quantum safe cryptography.

5.17.4.1.3 Evaluation

The clear advantage of this solution is that the quantum safe algorithm is there from day one, and any NextGen entity can confidently assume that the other party with which it is communicating will also support this algorithm.

The clear disadvantage is that quantum safe cryptography is an immature field of study. Quantum computers may not become a real threat for many years, and in that time there may very well be big advances in the field, such as:

- new quantum safe algorithms that are much more efficient than those known today;
- new algorithms giving much better assurance of quantum safety;
- algorithms currently believed to be quantum safe turning out not to be.

A (supposedly) quantum safe algorithm in the initial NextGen specifications may therefore turn out to be very sub-optimal.

5.17.4.2 Solution #17.2: Message flexibility

5.17.4.2.1 Introduction

This solution addresses key issue #17.2.

Lenovo Ex. 1007
Page 457

5.17.4.2.2 Solution details

All standardised messages that carry public key signatures are specified in such a way that the signature size is flexible enough to include much larger signatures in future. Likewise, all standardised messages that carry public keys (either raw or in certificates) are specified in such a way that much larger public keys can be accommodated in future.

5.17.4.2.3 Evaluation

Algorithms currently believed quantum safe typically involve much larger keys and much larger signatures than classical public key algorithms. This solution makes allowance for such algorithms to be introduced in future.

The solution is specified only at a very high level; further detailed study will be required to apply it in practice.

5.17.4.3 Solution #17.3: Updating algorithms to be used by home network and UE

5.17.4.3.1 Introduction

This solution addresses key issue #17.2, for algorithms used to protect messages sent in either direction between individual subscribers and home network nodes.

5.17.4.3.2 Solution details

A home network can deliver an entire new algorithm to a UE (including UICC), using any OTA mechanism at its disposal. This could be new code that the UE (possibly the UICC) can compile, or can run in an interpreter.

A new home network public key (raw or certificate) can be delivered to the UE using the same mechanism, if required.

If the UE needs its own key pair for use with the new algorithm, then the home network will deliver the corresponding key generation algorithm along with the public key algorithm. This key generation can make use of a random number generator API on the UE. The UE uses the key generation algorithm to generate its own key pair.

After successful delivery of a new (e.g. quantum safe) algorithm, and confirmed delivery / creation of necessary keys, the home network can require that the UE always uses this new algorithm, and reject attempts to use older algorithms. The extent to which the home network can be confident in a particular subscriber's ability to use a new algorithm will depend on:

- whether the new algorithm has been delivered to run in the UICC, or elsewhere in the device;
- whether the UICC is fixed or removable.

Similarly the UE can require that the home network always uses this new algorithm, and reject attempts to use older algorithms.

5.17.4.3.3 Evaluation

Supporting the ability to deliver whole new algorithms in this way means that a new (e.g. quantum safe) algorithm can be phased in, in such a way that the home network can be confident that it happens, and is not reliant on whether a device manufacturer delivers patches, or whether the user chooses to accept such patches. Phasing in of a new algorithm can be done, for instance, if and when the risk from non-quantum-safe algorithms is deemed high enough, and when the study of quantum safe algorithms is deemed mature enough for an algorithm to be selected.

Risks / challenges with this approach include:

- the fact that entire new algorithms may be significantly larger than OTA mechanisms typically handle today;
- it may be hard for a newly delivered algorithm to run as efficiently, and with as much resistance to side channel attacks such as differential power analysis, as could be true of a native algorithm implementation.

Lenovo Ex. 1007
Page 458

5.17.4.4 Solution #17.4: Secure negotiation of algorithms to be used by home network and UE

5.17.4.4.1 Introduction

This solution addresses key issue #17.2. It is an alternative to solution #17.3.

We assume that, if a new algorithm is specified for use between UE and home network in the NextGen system, then for some years to come:

- some newly manufactured UEs will support the new algorithm, and some will not;
- some existing UEs will be patched to support the new algorithm, and some will not;
- some home networks will support the new algorithm, and some will not.

5.17.4.4.2 Solution details

Using any OTA mechanism at its disposal – or directly, in the creation of new USIMs (or their NextGen equivalent) – the home network can cause a flag to be set in the UE (e.g. on the UICC). A UE that has been created or patched to support the new algorithm will recognise that this flag means that the home network supports the new public key algorithm.

A new home network public key (raw or certificate) can be delivered to the UE using any secure OTA mechanism, if required.

When a UE supporting the new algorithm first observes this indicator flag to be set, it communicates to the home network that it (the UE) also supports this algorithm (including confirmation that the UE has generated a key pair for the new algorithm, if it needs one). This could be done in an OTA message, or it could be included as a parameter in a message to the home network such as the Initial Authentication Request defined in solution #2.12. Receipt of this message needs to be acknowledged by the home network.

After confirmation that both the UE and the home serving network support a new (e.g. quantum safe) algorithm, then this solution means that they can agree only to use this new algorithm, and can each reject attempts to use older algorithms.

Editor's note: The above solution is described only at a high level – more details are needed.

5.17.4.4.3 Evaluation

This solution allows the UE and home network to enforce use of a superior (e.g. quantum safe) algorithm when both parties support it. It allows device manufacturers to patch in new algorithms in the best way they can, rather than delivering them in a "device agnostic" way as in solution 17.3; allowing the manufacturer to implement the algorithm is likely to lead to more efficient implementations and/or better resistance to side channel attacks such as differential power analysis. It allows new algorithms to be phased in gradually, in such a way that there is value in doing so.

However, it does not give the home network any way to push out support for a new algorithm to existing devices: patching in a new algorithm is entirely down to the standard device update process, with all its failings.

5.17.4.5 Solution #17.5: Secure negotiation of algorithms to be used by serving network and UE

5.17.4.5.1 Introduction

This solution addresses key issue #17.2, for algorithms used to protect messages sent in either direction between individual subscribers and serving network nodes (not broadcast messages from the serving network).

We assume that, if a new algorithm is specified for use between UE and serving network in the NextGen system, then for some years to come:

- some newly manufactured UEs will support the new algorithm, and some will not;

Lenovo Ex. 1007
Page 459

- some existing UEs will be patched to support the new algorithm, and some will not;
- some serving networks will support the new algorithm, and some will not.

5.17.4.5.2 Solution details

In the initial authentication exchange when a UE connects to a serving network, the UE communicates its public key algorithm capabilities to the serving network (either directly or via the home network), in a way that is integrity protected based on the long term subscriber secret key. See solution #2.12 for an example of how this can be done via the home network.

Also as part of the initial authentication exchange, the serving network communicates a set of permitted algorithms to the UE, in a way that is integrity protected based on the long term subscriber secret key. This set of permitted algorithms will be a subset of the algorithms that the UE supports. The indication may optionally go into finer detail, specifying different sets of algorithms for use in different circumstances (this may be helpful, for instance. if only some serving network nodes support a particular algorithm).

If both the UE and the serving network support a new (e.g. quantum safe) algorithm, then this solution means that they can agree only to use this new algorithm, and can each reject attempts to use older algorithms.

5.17.4.5.3 Evaluation

This solution allows communicating parties to enforce use of a superior (e.g. quantum safe) algorithm when both parties support it, and prevent the type of attack in which the attacker pretends to be one party but claims only to support algorithms that it can in fact break. It allows new algorithms to be phased in gradually, in such a way that there is value in doing so.

It does not, however, address the challenge of introducing new (e.g. quantum safe) algorithms for use in "connectionless" messages such as signed broadcasts from the serving network to multiple devices, or encrypted uplink messages sent before authentication.

5.17.4.z Solution #x.z: <solution name>

5.17.4.z.1 Introduction

Editor's note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the security area.

5.17.4.z.2 Solution details

5.17.4.z.3 Evaluation

5.17.5 Conclusions

Editor's note: This clause will contain the evaluation between the solutions, and the conclusions made by SA3.

5.x Security area #x: <security area name>

Editor's Note: The study is expected to be divided into several security areas which all have their own key issues and solutions. Security areas are not in any particular order but they are added incrementally (x = 1, 2, 3…) when new area is identified.

5.x.1 Introduction

Editor's Note: This clause gives background information on the security area.

Lenovo Ex. 1007
Page 460

5.x.2 Security assumptions

Editor's Note: This clause will document security assumptions related to each security area.

5.x.3 Key issues

Editor's note: This clause will contain the key issues that need to be addressed by SA3 on each security area. The exact contents are FFS.

5.x.3.y Key issue #x.y: <key issue name>

Editor's Note: Key issues within the security area are not in any particular order but they are added incrementally (y = 1, 2, 3…) when new key issue is identified. 'x' refers to the security area.

5.x.3.y.1 Key issue details

5.x.3.y.2 Security threats

5.x.3.y.3 Potential security requirements

5.x.4 Solutions

5.x.4.z Solution #x.z: <solution name>

Editor's Note: Solutions within the security area are not in any particular order but they are added incrementally (z = 1, 2, 3…) when new solution is identified. 'x' refers to the security area.

5.x.4.z.1 Introduction

Editor's note: Each solution should list the key issues that it addresses. There may be references to the key issues outside the security area.

5.x.4.z.2 Solution details

5.x.4.z.3 Evaluation

5.x.5 Conclusions

Editor's note: This clause will contain the evaluation between the solutions, and the conclusions made by SA3.

6 Conclusions

Editor's note: This clause will contain the overall conclusions made by SA3.

Lenovo Ex. 1007
Page 461

Annex A:
Focus areas, and rationales behind them

Editor's note: It is proposed that this Annex would include a list of security topics that are expected to help identifying areas of preferred contributions.

Lenovo Ex. 1007
Page 462

Annex B:
Guiding principles

Editor's note: It is proposed that this Annex would include a list of guiding principles.

B.1 Introduction

Editor's note: A placeholder clause for an introduction

B.2 Guiding principles

B.2.1 Usage of the wording 'security level' for a system:

B.2.1.1 Issue details

The issue with the notion of 'security level' is that it assumes that there is a one-dimensional representation that indicates a 'level' of security of a complex system. In the Next Generation system, however, there will be building blocks for multiple security aspects that allow for different degrees of protection that are fit for varying business cases. For that reason, the notion of 'security level' should be avoided or its meaning should be explained within the context of the potential solution or key issue clauses whenever it is used.

B.2.1.2 Recommendations

Ideally, the termininology 'security level' should be avoided. If it is used, its meaning should be explained within the context of the potential solution or key issue clauses.

B.2.2 Comparison of 'security levels' between building blocks or slices

B.2.2.1 Issue details

The issue with comparing 'security levels' for different building blocks is that it prevents the proper selection of security measures fit for the use cases under consideration. In Next Generation the concept of 'network slicing' was introduced and so operators can choose to use slices in their networks and apply security mechanisms fit for the purpose of each slice.

It is also noted that Next Generation systems will have different building blocks that include selection of security endpoints, type of protection (e.g. confidentiality and integrity) and perhaps choice of algorithms. Therefore, it makes sense to compare the different features of the different building blocks within their context, e.g. use case or deployment location. For example: even if a HNodeB with a TrE may be seen as more secure than a macro NodeB, this does not mean that a macro NodeB network is less secure overall.

B.2.2.2 Recommendation

Comparisons between 'security levels' of systems is to be avoided, rather the security features of the security building blocks are to be compared with respect to their respective context, e.g. use case or deployment location. If 'security level' is used for comparisons then the recommendation in B.2.1.2 is applicable.

NOTE: This recommendation does not mean that unacceptably weak security algorithms, protocols or features are acceptable for standardization as weak security building blocks may weaken the security of the system as a whole.

Lenovo Ex. 1007
Page 463

B.2.3 Threats - functional requirements - security requirements

B.2.3.1 Issue details

Various considerations may lead to security requirements. Security threats are a main source of information to derive security requirements. But it is also possible to define security requirements that do not counter a threat, because they are derived from functional requirements on security features.

B.2.3.2 Recommendation

Description of key issue details should clearly show the validity of threats, which together with functional requirements derived from use cases lead to security requirements.

B.2.4 Solutions and Evaluations

B.2.4.1 Solution Location

In general, solutions should be placed in the security area that contains the key issues that are addressed by the solution.

Solutions may be relevant to several key issues in several security areas. In this case, the solution should be put in the most relevant area.

B.2.4.1 Solution Presentation

Solutions should have at least:

- an "Introduction" clause – This should detail at least the scope of the solution, the key issues addressed by the solution and high level overview of the solution.
- a "Solution Details" clause – This should describe the solution in as much detail as possible and include diagrams and message flows, where appropriate.
- an "Evaluation" clause – This clause:
  - should evaluate the solution against the proposed requirements for the key issues being addressed,
  - may evaluate the solution against the threats identified for the key issues being addressed,
  - where appropriate, may evaluate against other solutions that address the same key issue(s).

Where the solution is not a "complete" solution for a key issue, this should be stated. Any other consequences of the solution that do not directly relate to the Key issue requirements may also be stated.

Lenovo Ex. 1007
Page 464

Annex C:
Trust model study for network slicing

C.1 Introduction

In this study we build on the trust model of LTE in order to identify where new mitigations or security mechanisms, if any, are required.

C.2 Trust model

The trust model in LTE systems consists of a trusted core network, a set of trusted eNodeBs and the exposed interfaces in between that are susceptible to attacks (see Figure C.2-1). Based on this model, security mechanisms have been defined in TS 33.401 [34] in order to protect the exposed interfaces. In addition to the 3GPP-access, LTE systems support non-3GPP-acesses in two variants: trusted and untrusted. Similarly, mechanisms have been provided in TS 33.402 [35] in order to secure the communication with the non-3GPP trusted access or across the non-trusted access.

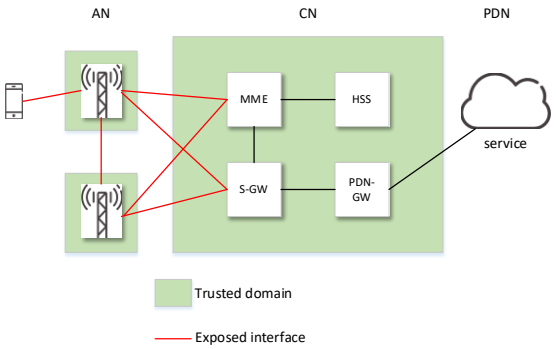


Figure C.2-1: Trust model in LTE Systems

By analogy to LTE, a network slice is in fact a self-contained instance of a core network configured specifically to provide a certain service. Therefore, it is reasonable to aim at defining a trust model where each single Network Slice is a trusted domain (see Figure C.2-2). As a consequence, similar mechanisms to the ones in TS 33.401 [34] and TS 33.402 [35] can be reused in order to protect the exposed interfaces. The question now is how to establish such trust dynamically for example upon the creation or the deployment of the network functions and how to maintain it. In the remainder of this clause, a high level justification is proposed in support of the proposed trust model.

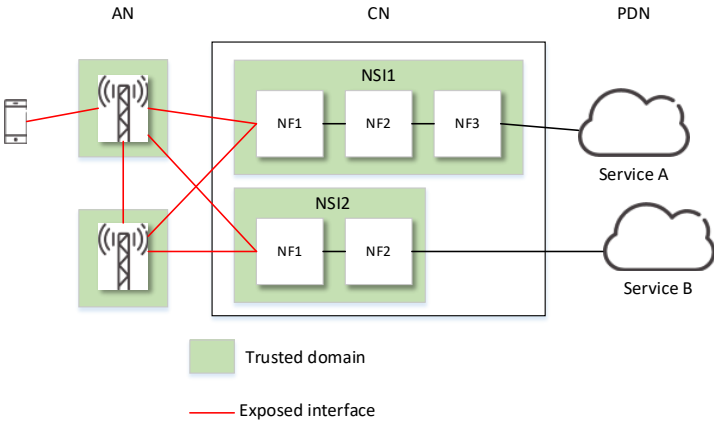


Figure C.2-2: Trust model in Next Generation systems

Lenovo Ex. 1007
Page 465

C.3 Trust establishment

C.3.1 Analysis

In the context of virtualization, trust needs to be established on several layers:

- The infrastructure layer
- The virtualization layer
- The network function layer

C.3.2 The infrastructure layer

This is the hardware/physical resource layer on which the network slice is running. For trust in this layer to be assumed, it could be expected that the hardware platforms have support for secure boot mechanisms. In combination with some type of credentials (for example the vendor), the hardware platform is then established as the root of trust and therefrom, a trust chain can be established to all other software components in the layer above.

C.3.3 The virtualization layer

This is the hypervisor layer which provides the abstraction of the physical resources towards the application layer. Integrity verification of all the software components in this layer can be then performed using possibly other credentials (for example the operator).

C.3.4 The network function layer

This is the network slice layer where the network functions are deployed. The trust chain anchored at the hardware can extend to this layer via secure boot mechanisms. Integrity verifications of the software components of the network function can be then performed in a similar manner using possibly other credentials (for example the slice owner). Furthermore, the network functions need to be mutually authenticated for example using similar credentials specific to for example the slice owner.

It should be noted that it is FFS if aspects related to virtualization in those layers are in the scope of 3GPP and how SA3 should take the ongoing work of ETSI NFV ISG on those topics into account

C.4 Trust maintenance

C.4.1 Analysis

Maintaining the trust towards a network slice requires security measures in place in order to, for example, prevent unauthorized access, impersonation of the network functions, impersonation of UE's or even impersonation the access network, disclosure of sensitive information compromising the end-user privacy or the system security, etc.

C.4.2 The Accesses

Proper authorization mechanisms could be required for any type of access, whether for the service by end-users or for maintenance by admins, so that unauthorized users are not granted access and authorized ones are not able to misuse their access rights. Therefore, only authenticated agents must be granted access for example based on subscription information or access rights. Furthermore, any data traffic reaching the slice must be replay and integrity protected in order to prevent impersonation and packet injection attacks.

Lenovo Ex. 1007
Page 466

C.4.3 The Data flows

The protection keys for the data flows could be cryptographically separated so that user plane traffic is protected by keys bound to the intended network slice. For example, this can be achieved by using slice specific information (unique identifiers) in the derivation of access keys like the K_{ASME} in LTE. The separation requirement applies as well to the backhaul and can be achieved for example by using dedicated IPsec tunnels or dedicated child security associations within the same tunnel.

C.4.4 The network slices

The 3GPP security requirements such as the ones in TS 33.117 [36] and TS 33.310 [37] would still be applicable. In the context of virtualization, the work in progress such as in [38, 40, 39, 41, 42] could be taken into account to isolate the virtualized components. It is possible that a risk assessment could be always conducted on case to case basis. The deployment configuration of the network functions could then be based on an agreement with the service provider.

Lenovo Ex. 1007
Page 467

Annex D:
Prioritization of key issues

Below table concludes the key issue prioritization of the present TR. "Yes" (or phase 1) means that key issue needs to be decided in phase 1. "Yes" (or phase 1) does not mean that assumption made in key issue description is recognized as valid.

	Phase 1/rel-14 study? (Yes or Phase 2)	**Comments**
Security area #1: Architectural aspects of Next Generation security	Yes	
Key issue #1.1: Overview of NextGen security architecture	Yes	
Key issue #1.2: Need for security anchor in NextGen network	Yes	
Key Issue #1.3: User plane integrity between UE and network	Yes	
Key Issue #1.4: User plane confidentiality between UE and network	Yes	
Key Issue #1.5 Integrity protection for the control plane between UE and network	Yes	
Key Issue #1.6 Confidentiality for the control plane between UE and network	Yes	
Key issue #1.7: Key hierarchy	Yes	
Key Issue #1.8: UEs with Asymmetric Keys	Yes	Depends on selection of solutions from other key issues
Key issue #1.9: Security features for AN-CN Control Plane	Yes	
Key issue #1.10: Security features for AN-CN User Plane	Yes	
Key issue #1.11: Security features for CN-CN Control Plane	Yes	
Key issue #1.12: Security features for CN-CN User Plane	Yes	
Key Issue #1.13: Security Implications to Achieve Low Latency	Phase 2	If it is for specific use cases in phase 1, then phase 1. (check with RAN WG)
Key issue #1.14: Security for serving functions in a less secure location	Yes	Decision should be made in Phase 1
Key issue #1.15: Termination point of UP security	Yes	

Lenovo Ex. 1007
Page 468

Key issue #1.16: User plane protection granularity	Yes	
Key issue #1.17: On-demand security policy	Yes	Need to figure out differences between 1.17 and 1.18
Key issue #1.18: Flexible security policies negotiation in control plane	Yes	Need to figure out differences between 1.17 and 1.18
Key issue #1.19: Untrusted non-3GPP access	Yes	
Key issue #1.20: Trusted non-3GPP access	Phase 2	
Security area #2: Authentication		
Key Issue #2.1 Authentication framework	Yes	
Key Issue #2.2: Reducing the impact of secret key leakage	Yes (low priority)	Leakage of Permanent key. Check potential bidding down attack possibility. May need further prioritization later.
Key issue #2.3: Authentication identifiers and credentials	Yes	
Key issue #2.4: Equipment identifier authentication	Yes (low priority)	Check potential bidding down attack possibility. May need further prioritization later. (There was input from MMF)
Key issue #2.5: Non-AKA-based authentication	Yes	Need to make a decision in phase 1
Key Issue #2.6: Efficient in energy consuming and reduced signalling for resource constraint environment	Phase 2	RAN decision (massive IoT)
Key Issue #2.7: Reduced signalling overload for massive number of UEs activating at the same time	Phase 2	Decision at SA3#85
Key Issue #2.8: Authentication of the user	Phase 2	
Key issue #2.9: Security for service provider connection	No decision	Further clarification required for the scope, based on SA2 docs. If there is modification/impact on key hierarchy from the solution, then move to phase 1. (relevant part only, not protocol)
Key issue #2.10: Secondary authentication for network slice access by 3rd party service	Yes	
Key issue #2.11: Increasing home control in roaming situations	Yes	
Security area #3: Security context and key management		

Lenovo Ex. 1007
Page 469

Key Issue #3.1: Interception of radio interface keys sent between operator entities	Yes	
Key Issue #3.2: Refreshing keys	Yes	
Key issue #3.3: Principles of security negotiation	Yes	
Key Issue #3.4: Security context sharing	Yes	Need to check if this key issue is covered by KI #2.1
Key issue #3.5: Unnecessary dependence of keys between security layers	Yes	
Key issue #3.6: Top-level key for access-network-specific keys	Yes	
Key issue #3.7: The storage of security context	Yes	Need to check if this key issue is covered by security area #5
Key issue #3.8: Security context for small data mode	Phase 2	
Key issue #3.9: void		See #1.19
Key issue #3.10: void		See #1.20
Key issue #3.11: 5G security key and context identification	Yes	
Security area #4: RAN security		
Key Issue #4.1: AS security during RRC idle mode	Yes	DoS attack on MT service only (not small data, D2D)
Key issue #4.2: Security requirements on gNB	Yes	
Key issue #4.3: Security aspects of dual connectivity	Yes	
Key issue #4.4: Security aspects of intra-NR mobility	Yes	
Key issue #4.5: Security aspects of RAN-WLAN aggregation/integration	Phase 2	RAN decision on non-3GPP access
Key issue #4.6: User plane DoS attacks	Phase 2	Massive IoT devices
Key issue #4.7: Key handling in RRC inactive state to RRC active state transition	Yes	
Key issue #4.8: void	Yes	Merged with #4.3
Security area #5: Security within NG-UE		
Key issue #5.1: Secure storage and processing of credentials and identities	Yes	

Lenovo Ex. 1007
Page 470

Key issue #5.2: Secure storage and processing of equipment identifier and credentials	Yes (low priority)	Secure storage is Phase 1. Check potential bidding down attack possibility. May need further prioritization later. (There was input from MMF)
Key issue #5.3: NG UE supporting different use cases	Phase 2	
Security area #6: Authorization		
Key issue #6.1: UE authorization	Yes	Improvements for phase 2 may be required
Key issue #6.2: Network authorization	Yes	Improvements for phase 2 may be required
Key issue #6.3: Authorization decoupled from authentication	Phase 2	Check potential bidding down attack possibility. Phase one solution needs to be extendable.
Security area #7: Subscription privacy		
Key Issue #7.1: Refreshing of temporary subscription identifier	Yes	
Key issue #7.2: Concealing permanent or long-term subscription identifier	Yes	
Key issue #7.3: Concealing permanent or long-term equipment identifier	Yes	Procedure (like in LTE) needs to be provided in Phase 1, we may not need an enhanced procedure in phase 1
Key issue #7.4: Using effective temporary or short-term subscription identifiers	Yes	Related to 7.1
Key issue #7.5: Transmitting permanent identifiers in secure interface	Yes	Procedure (like in LTE) needs to be provided in Phase 1, we may not need an enhanced procedure in phase 1
Key issue #7.6: Transmitting permanent subscription identifiers only when needed	Yes	
Key issue #7.7: Using effective temporary or short-term equipment identifiers	Phase 2	
Key issue #7.8: Privacy protection of network slice identifier	Yes	Identifier format from SA2 needs to be analyzed for privacy impacts
Key issue #7.9: Need to protect entire Permanent Identifier	Yes	
Security area #8: Network slicing security		
Key Issue #8.1: Security isolation of network slices	Yes	

Lenovo Ex. 1007
Page 471

Key Issue #8.2: Security mechanism differentiation for network slices	Phase 2	Security framework in phase 1 shall allow for adding such differentiation in phase 2. This doesn't mean the solutions need to be worked on in phase 1.
Key Issue #8.3: Security on UEs' access to slices	Yes	
Key Issue #8.4: Security on sensitive network elements	Yes	Needs to be studied further, is this SCAS type of work?
Key Issue #8.5: Security on management of slicing	Phase 2	Understanding of what other groups (including outside 3GPP) are doing
Key Issue #8.6: Security on interacting with third party	Depends on SA2 whether this relates to SCEF	
Key Issue #8.7: Security of inter slice communications	Phase 2	Based on our current understanding, depends on SA2 model, whether inter-slice communication exists
Key Issue #8.8: Virtualization security	Yes	Needs to be studied further, is this SCAS type of work? Understanding of what other groups (including outside 3GPP) are doing
Security area #9: Relay security	Phase 2	Based on SA2 decision
Key Issue #9.1: Mutual authentication of remote UE and network over a relay	Phase 2	Based on SA2 decision
Key Issue #9.2: Integrity and confidentiality protection of remote UEs	Phase 2	Based on SA2 decision
Key Issue #9.3: Remote UE session continuity	Phase 2	Based on SA2 decision
Security area #10: Network domain security		
Key Issue #10.1: Network and NE communication security	Yes	
Key issue #10.2: Interconnection Security	Yes	
Security area #11: Security visibility and configurability		
Key Issue #11.1: Service-dependent security requirements	Yes	
Key Issue #11.2: User awareness of security	Yes	
Key Issue #11.3: User control of security	Yes	Shouldn't fall back behind what we already have, e.g. in EGPRS
Key Issue #11.4: On demand security framework	Yes	Shouldn't fall back behind what we already have, e.g. in EGPRS

Lenovo Ex. 1007
Page 472

Security area #12: Credential provisioning	Phase 2	Credential provisioning will be discussed in phase 2.
Key issue #12.1: Credential provisioning	Phase 2	Credential provisioning will be discussed in phase 2.
Key Issue #12.2: Remote credential provisioning for IoT devices	Phase 2	Credential provisioning will be discussed in phase 2.
Security area #13: Security for Interworking and Migration		
Key issue #13.1: : Security for Handovers	Yes	
Key issue #13.2: Security for Idle Mode Mobility	Yes	
Key issue #13.3: Security aspects of migration	Yes	
Key issue #13.4: Bidding down to an older 3GPP generation or a non-3GPP access technology	Yes	
Security area #14: Security aspects of small data	Phase 2	Based on SA2 decision
Key Issue #14.1: Access security for small data session	Phase 2	Based on SA2 decision
Key Issue #14.2: Security for data over the small data interface.	Phase 2	Based on SA2 decision
Key Issue #14.3: Restricting small data resource utilization	Phase 2	Based on SA2 decision
Key Issue #14.4: Small data context retention	Phase 2	Based on SA2 decision
Security area #15: Broadcast/Multicast Security	Phase 2	Based on SA2 decision
Key issue #15.1: Broadcast/Multicast capabilities	Phase 2	Based on SA2 decision
Key issue #15.2: Usage of MBMS security	Phase 2	Based on SA2 decision
Security area #16 Management security		
Key issue # 16.1: management plane communication protection	Not in phase 1	More of a SCAS type of issue? Adaptation of SCAS catalogue to 5G equipment required
Key issue #16.2: network element deployment security	Yes	Shouldn't fall back behind what we already have, e.g. automatic enrollment of certificates in 33.310.
Key issue #16.3: Network slice life-cycle security	Depending on e.g. SA5 definition of network slice lifecycle	

Lenovo Ex. 1007
Page 473

Security area #17: Cryptographic algorithms		
Key issue #17.1: Cryptographic algorithms for backward compatibility	Yes	
Key issue #17.2: Quantum safe cryptography	Yes	Decision is required in phase 1, but algorithms may come later.

Lenovo Ex. 1007
Page 474

Annex E:
Questions and Interim Agreements

E.1 Questions and Interim Agreements for security area #1

E.1.1 Questions and Interim Agreements for Key Issue #1.1

E.1.2 Questions and Interim Agreements for Key Issue #1.2

E.1.2.1 Need for a security anchor

E.1.2.1.1 Description of Question

Is there a need for a security anchor used for all kinds of access networks?

E.1.2.1.2 Interim Agreement

Yes, there is a need for a single security anchor per PLMN used for all kinds of access networks. The security anchor is the SEAF as defined in clause 5.2.1.2. It is, by definition, the network entity that hosts the anchor key as described in the interim agreement E.2.1.4.

E.1.2.2 Separation of security anchor from other entities

E.1.2.2.1 Description of Question

Should the security anchor be separate from the mobility management and session management?

E.1.2.2.2 Interim Agreement

In 5G phase 1, the SEAF and the AMF are co-located. The SMF is a separate entity, as defined in TS 23.501. The key hierarchy is done in phase 1 such that AMF and SEAF can be separated in later 5G phases.

E.1.3 Questions and Interim Agreements for Key Issue #1.3

E.1.3.0 Questions in other clauses affecting this key issue

Questions with respect to the selection of a UP security termination point are addressed in the questions on key issue 1.15.

E.1.3.1 Support of User plane integrity between UE and network

E.1.3.1.1 Description of Question

This question addresses whether it should be mandatory for the UE and the Network to support user plane integrity protection between the UE and the Network. "*Shall UP integrity be mandatory to support / use by 5G UEs, 5G networks?"*

E.1.3.1.2 Interim Agreement

UP integrity is mandatory to support and optional to use by 5G UEs and 5G networks in 5G phase 1, with the exception of 5G UEs that can only access the EPC.

Lenovo Ex. 1007
Page 475

E.1.3.2 How should use of the feature be negotiated between UE and network

E.1.3.2.1 Description of Question

This question addresses how use of the feature is negotiated between UE and network "*How should use of the feature be negotiated between UE and network*?"

E.1.3.2.2 Interim Agreement

It shall be possible to negotiate the use of UP integrity between 5G UEs and 5G networks in 5G phase 1. Its use shall be determined by the network.

E.1.4 Questions and Interim Agreements for Key Issue #1.4

E.1.4.0 Questions in other clauses affecting this key issue

The questions with respect to the selection of a UP security termination point is addressed in the questions on key issue 1.15. Questions related to how the UP confidentiality is displayed to the user (i.e. the ciphering indicator) are addressed in the questions relating to key issues 11.1-11.4.

E.1.4.1 Support of UP confidentiality protection in the UE and the Network

E.1.4.1.1 Description of Question

This question addresses whether it should be mandatory for the UE and the Network to support UP confidentiality protection between the UE and the Network. It should also address how the system deals with a situation when an encryption algorithm has been shown to have insufficient strength. The answer should also take into account whether or not the UP confidentiality protection may be negotiated between the UE and the Network in a way that avoids bidding down attacks.

E.1.4.1.2 Interim Agreement

Solution #1.3 is taken as a base for normative work, in accordance with the agreement for KI #1.15 – UP security termination point and in accordance with stage 2 architecture specifications.

E.1.5 Questions and Interim Agreements for Key Issue #1.5

E.1.5.0 Questions in other clauses affecting this key issue

TBD

E.1.5.1 Shall CP integrity be mandatory to support / use by 5G UEs, 5G networks?

E.1.5.1.1 Description of Question

The question intends to address the following points:

1. Shall the CP integrity be mandatory to support by 5G UEs?
2. Shall the CP integrity be mandatory to support by 5G network?
3. Shall the CP integrity be mandatory to use by 5G UEs?
4. Shall the CP integrity be mandatory to use by 5G network?

Lenovo Ex. 1007
Page 476

E.1.5.1.2 Interim Agreement

CP integrity is mandatory to support by 5G UEs and 5G network.

CP integrity is mandatory to use except for except for a well-defined list of exceptions in certain procedures (e.g. unauthenticated emergency call).

E.1.5.2 Shall integrity for all NAS messages terminate in a single point?

E.1.5.2.1 Description of Question

NAS messages between UE and network are MM messages between UE and AMF or SM messages between UE and SMF. SA2 has already decided that all NAS messages for one UE are routed via a single AMF. SA2 has also assigned security functionality for NAS messages to the AMF, but not to the SMF, cf. TS 23.501 v030, clauses 6.2.1 and 6.2.2. An Editor's Note in these clauses leaves the possibility open for SA3 decisions to override this assignment.

The question to be answered by SA3 (in the context of key issue 1.5) is whether there shall be a single termination point for integrity protection for all NAS messages, including MM and SM messages.

E.1.5.2.2 Interim Agreement

There shall be a single termination point for integrity protection for all NAS messages, including MM and SM messages. This point shall be the AMF.

E.1.6 Questions and Interim Agreements for Key Issue #1.6

E.1.6.0 Questions in other clauses affecting this key issue

TBD

E.1.6.1 Shall CP confidentiality be mandatory to support / use by 5G UEs, 5G networks?

E.1.6.1.1 Description of Question

The question intends to address the following points:

1. Shall the CP confidentiality be mandatory to support by 5G UEs?
2. Shall the CP confidentiality be mandatory to support by 5G network?
3. Shall the CP confidentiality be mandatory to use by 5G UEs?
4. Shall the CP confidentiality be mandatory to use by 5G network?

E.1.6.1.2 Interim Agreement

The answer to questions 1 and 2 above is yes. The answer to questions 3 and 4 is that CP confidentiality should always be used where regulations permit, except for a well-defined list of exceptions in certain procedures..

E.1.6.2 Shall confidentiality for all NAS messages terminate in a single point?

E.1.6.2.1 Description of Question

For the background see E.1.5.2.1.

The question to be answered by SA3 (in the context of key issue 1.6) is whether there shall be a single termination point for confidentiality protection for all NAS messages, including MM and SM messages.

NOTE: it is obvious that the questions in E.1.5.2.1. and the present question need to be answered in the same way.

Lenovo Ex. 1007
Page 477

E.1.6.2.2 Interim Agreement

There shall be a single termination point for confidentiality protection for all NAS messages, including MM and SM messages. This point shall be the AMF.

E.1.7 Questions and Interim Agreements for Key Issue #1.7

E.1.8 Questions and Interim Agreements for Key Issue #1.8

E.1.8.0 Questions in other clauses affecting this key issue

Questions affected the questions on Equipment identifier authentication (Key Issue #2.4), Non-AKA-based authentication (Key Issue #2.5), Remote credential provisioning for IoT devices (Key Issue #12.2), as well as AS security during RRC idle mode (Key Issue #4.1) and Key issue #7.1 Subscription identifier privacy

E.1.8.1 Private keys in the UE

E.1.8.1.1 Description of Question

This question addresses whether a UE should contain one or multiple private keys to be used with an associated public key.

E.1.8.1.2 Interim Agreement

E.1.8.2 Public network keys

E.1.8.2.1 Description of Question

This question addresses whether a UE should contain one or multiple public keys to be used with an associated network private key.

E.1.8.2.2 Interim Agreement

E.1.9 Questions and Interim Agreements for Key Issue #1.9

E.1.9.0 Questions in other clauses affecting this key issue

tba

E.1.9.1 Security features for the AN-CN control plane

E.1.9.1.1 Description of Question

Question: What security features are mandatory to support / use on the N2 interface?

E.1.9.1.2 Interim Agreement

Confidentiality and integrity are mandatory to support on N2. The use of confidentiality and integrity is mandatory unless N2 is secured by physical means. If confidentiality and integrity are used the solution shall follow the principles of TS 33.210 (NDS/IP).

Support by the gNB for the certificate enrolment procedure as specified in TS 33.310 [37] is mandatory.

Lenovo Ex. 1007
Page 478

E.1.10 Questions and Interim Agreements for Key Issue #1.10

E.1.10.0 Questions in other clauses affecting this key issue

tba

E.1.10.1 Security features for the AN-CN user plane

E.1.10.1.1 Description of Question

Question: What security features are mandatory to support / use on the N3 interface?

E.1.10.1.2 Interim Agreement

Confidentiality and integrity are mandatory to support on N3. For deployments where UP security does not terminate in a secure location and the N3 interface is not secured by physical means the use of confidentiality and integrity is mandatory on N3.

E.1.11 Questions and Interim Agreements for Key Issue #1.11

E.1.11.0 Questions in other clauses affecting this key issue

The questions in security area #10 may affect this clause.

E.1.11.1 Security features for the CN-CN control plane

E.1.11.1.1 Description of Question

Question: What security features are mandatory to support / use on the CN-CN control plane?

E.1.11.1.2 Interim Agreement

The principles of Network Domain Security, as described in 3GPP TS 33.210, shall apply. Further agreements in security area #10, if any, shall apply and may supersede the statement in the previous sentence.

E.1.12 Questions and Interim Agreements for Key Issue #1.12

E.1.12.0 Questions in other clauses affecting this key issue

The questions in security area #10 may affect this clause.

E.1.12.1 Security features for the CN-CN user plane

E.1.12.1.1 Description of Question

Question: What security features are mandatory to support / use on the CN-CN user plane?

E.1.12.1.2 Interim Agreement

No cryptographic protection is standardized for the CN-CN user plane (same as in EPS). Further agreements in security area #10, if any, shall apply and may supersede the statement in the previous sentence.

Lenovo Ex. 1007
Page 479

E.1.13 Questions and Interim Agreements for Key Issue #1.13

E.1.13.0 Questions in other clauses affecting this key issue

none.

E.1.13.1 Security Implications to Achieve Low Latency

E.1.13.1.1 Description of Question

Question: Is there a need to introduce or modify security features and procedures in 5G phase 1 that are dedicated specifically to achieve lower latency?

E.1.13.1.2 Interim Agreement

No security features or procedures need to be introduced or modified in 5G phase 1 that are dedicated specifically to achieve lower latency because no phase 1 use cases have been identified that would require lower latency.

E.1.14 Questions and Interim Agreements for Key Issue #1.14

E.1.14.0 Questions in other clauses affecting this key issue

E.1.2.2 Separation of security anchor from other entities.

E.1.14.1 Security for serving core network functions in a less secure location

E.1.14.1.1 Description of Question

Question: Is there a need in 5G phase 1 to take care of serving core network functions in a less secure location? (A function in a secure location is, in the context of this question, an implementation of the function in a physically inaccessible location.)

The question should be addressed separately for the control plane and the user plane.

E.1.14.1.2 Interim Agreement

No, it is assumed that all serving core network control plane functions based on technology available for phase 1 reside in a secure location.

The agreement for user plane functions is tbd.

E.1.15 Questions and Interim Agreements for Key Issue #1.15

E.1.15.0 Questions in other clauses affecting this key issue

The questions with respect to the selection of a UP confidentiality / integrity protection are affected by this clause as well, the questions on KI1.9 and KI1.10 .

E.1.15.1 Location of UP security termination point

E.1.15.1.1 Description of Question

This question addresses where the UP security should be terminated, i.e. whether it should be in the RAN, in the CN, on the border between the two or anywhere else.

Lenovo Ex. 1007
Page 480

E.1.15.1.2 Interim Agreement

The UP security termination point is in the RAN and located in the PDCP layer, as described in solution 1.22. Whether additional measures are needed in phase 1 depends on the possibility of having a gNB split such that the PDCP layer resides in an operator's data centre in a physically secure location.

The agreement should not preclude introducing a UP security termination point in the 5G core in phase 2.

E.1.15.2 Flexibility of UP security termination points

E.1.15.2.1 Description of Question

This question addresses whether it should be possible to flexibly select one or more UP security termination points, depending on e.g. service requirements.

E.1.15.2.2 Interim Agreement

Not applicable in phase 1 for the selection between UP security termination points in RAN and CN, as solution 1.22 foresees only UP security termination points in the RAN.

E.1.19 Questions and Interim Agreements for Key Issue #1.19

E.1.19.0 Questions in other clauses affecting this key issue

none.

E.1.19.1 Untrusted non-3GPP access

E.1.19.1.1 Description of Question

Which solution shall be selected for untrusted non-3GPP access?.

E.1.19.1.2 Interim Agreement

In 5G phase 1, a solution shall be specified that is based on the contributions S3-170663, 664, 665, 682, 835.

Editor's Note: The above contributions are assumed to be merged for SA3#87.

E.1.20 Questions and Interim Agreements for Key Issue #1.20

E.1.20.0 Questions in other clauses affecting this key issue

none.

E.1.20.1 Trusted non-3GPP access

E.1.20.1.1 Description of Question

Which solution shall be selected for trusted non-3GPP access?.

E.1.20.1.2 Interim Agreement

This question is not applicable to 5G phase 1.

Lenovo Ex. 1007
Page 481

E.2 Questions and Interim Agreements for security area #2

E.2.0 Questions and Interim Agreements for Authentication-related functions

E.2.0.1 Need for a SEAF in the HPLMN

E.2.0.1.1 Description of Question

Question: Are there scenarios to be supported that require a SEAF in the home network (in addition to the SEAF that is agreed to be in the visited network)?

E.2.0.1.2 Interim Agreement

There shall be no SEAF in the home network in roaming scenarios in 5G phase 1. Any functionality related to home network-based re-authentication shall be assumed by the AUSF.

The agreement should not preclude introducing a SEAF in the home network in 5G phase 2.

The system shall support the ability to store a key in the home network after an authentication. For this role, the H-SEAF is not needed.

E.2.1 Questions and Agreements for Key Issue #2.1 Authentication Framework

E.2.1.0 Questions in other clauses affecting this key issue

tba

E.2.1.1 Support for AKA and its variants for primary authentication

E.2.1.1.1 Description of Question

Question: shall the 5G UE and 5G network support a variant of the AKA authentication protocol for primary authentication? If so, which variant or variants shall be supported? Variants of the AKA protocol under discussion include EPS AKA, EPS AKA*, EAP-AKA, EAP-AKA', EAP-AKA*, MASA.

In answering this question, the aspects of serving network authentication, efficiency, and increased home control shall be explicitly taken into account.

E.2.1.1.2 Interim Agreement

The 5G UE and 5G serving network shall support EAP-AKA' for primary authentication, for both 3GPP access and untrusted non-3GPP access in 5G phase 1.

The 5G UE and the 5G serving network shall support EPS AKA* for primary authentication for 3GPP access in 5G phase 1.

NOTE1: EPS AKA* is identical to EPS AKA from a UE point of view.

NOTE2: The above is not meant to preclude enhanced IMSI privacy.

NOTE3: EAP-AKA' and EPS AKA* provide increased home control.

Lenovo Ex. 1007
Page 482

E.2.1.2 Support for EAP framework for primary authentication

E.2.1.2.1 Description of Question

Several solutions propose support for the EAP framework for primary authentication. This implies that the access network can carry EAP messages.

Question:

Shall the 5G UE and 5G network support the EAP framework for primary authentication in the above sense?

If so, shall other authentication methods than EAP methods be allowed? The answer should be given separately for 3GPP and non-3GPP accesses.

E.2.1.2.2 Interim Agreement

The 5G UE and 5G serving network shall support the EAP framework for primary authentication in 5G phase 1, for both 3GPP and non-3GPP accesses.EPS AKA* over 3GPP access is the only supported authentication method in 5G phase 1 that is not an EAP method.

E.2.1.3 The choice of EAP methods

E.2.1.3.1 Description of Question

Several solutions propose support for various EAP methods, e.g. EAP AKA, EAP AKA', EAP TLS, EAP TTLS, and EAP PSK.

Question:

Exactly which EAP methods shall be standardized for NextGen access in 3GPP?

E.2.1.3.2 Interim Agreement

The following EAP method shall be standardized in phase 1:

- EAP AKA'

An additional EAP method is described in an informative annex as an example on how the NextGen authentication framework for primary authentication can be applied to other EAP methods than EAP AKA'. The specific additional EAP method is decided in the normative phase. The additional EAP methods are assumed to be used in special use cases, such as in private networks or with IoT devices as specified in TS 22.261.

E.2.1.4 Creating an anchor key through primary authentication

E.2.1.4.1 Description of Question

Question: Shall all methods in the authentication framework used for primary authentication be able to create a unified anchor key that can be used by the UE and the serving network to protect the subsequent communication? Is this anchor key unique to each access or common for all accesses?

NOTE: This question does not affect secondary authentication. The latter may or may not use methods with key establishment.

E.2.1.4.2 Interim Agreement

Primary authentication shall create a unified anchor key that can be used by the UE and the serving network to protect the subsequent communication. This anchor key is common for all accesses.

Lenovo Ex. 1007
Page 483

NOTE: When a UE uses 3GPP access to a visited network and non-3GPP access to the home network then there will be two anchor keys, and the home network will be the serving network for the latter case.

E.2.1.5 Support for secondary authentication

E.2.1.5.1 Description of Question

Question: Which methods shall be supported for secondary authentication? In particular, shall support for general EAP methods for secondary authentication be provided in a way completely transparent to the 3GPP network?

NOTE: Earlier generations of mobile networks provided support only for CHAP or PAP.

E.2.1.5.2 Interim Agreement

Support for general EAP methods for secondary authentication between a UE and an external data network shall be provided such that the authentication method is completely transparent to the 3GPP network. The restrictions from E.2.1.3.2 on the authentication methods do not apply to secondary authentication. The normative work will be based on the solution in #2.30.

E.2.2 Questions and Agreements for Key Issue #2.2 reducing the impact of secret key leakage

E 2.2.0 Questions in other clauses affecting this key issue

E.2.2.1 Support to reduce the impact of secret key leakage.

E.2.2.1.1 Description of Question

Question: Shall there be procedures between the 5G UE and the 5G serving network to reduce the impact of the a leakage of the long term security key?

E.2.2.1.2 Interim Agreement

tba.

E.4 Questions and Interim Agreements for security area #4

E.4.1 Questions and Interim Agreements for Key Issue #4.1

E.4.1.1 Prevention of false base station attack during RRC idle mode

E.4.1.1.1 Description of question

Should prevention of false base station attack during RRC idle mode be addressed in Phase I?

E.4.1.1.2 Interim agreement

TBD.

E.4.1.2 Detection of false base station attack during RRC idle mode

E.4.1.2.1 Description of question

Should detection of false base station attack during RRC idle mode be addressed in Phase I?

Lenovo Ex. 1007
Page 484

E.4.1.2.2 Interim agreement

TBD

E.4.2 Questions and Interim Agreements for Key Issue #4.2

E.4.3 Questions and Interim Agreements for Key Issue #4.3

E.4.3.1 The inputs to the security algorithms for Option 3

E.4.3.1.1 Description of Question

What are in the inputs to the integrity and ciphering algorithm at the gNB for Option 3?

E.4.3.1.2 Interim Agreement

Solution #4.13 describes the agreed inputs for the integrity and ciphering algorithms at the gNB for Option 3.

E.4.4 Questions and Interim Agreements for Key Issue #4.4

E.4.5 Questions and Interim Agreements for Key Issue #4.5

E.4.6 Questions and Interim Agreements for Key Issue #4.6

E.4.7 Questions and Interim Agreements for Key Issue #4.7

E.4.8 Questions and Interim Agreements for Key Issue #4.8

E.4.9 Questions and Interim Agreements for Key Issue #4.9

E.4.10 Questions and interim agreements for key issue #4.10

E.4.10.1 Security of sidehaul (Xn and Xx) interfaces

E.4.10.1.1 Description of question

How should the Xn and Xx interfaces in the Next Generation systems be protected?

E.4.10.1.2 Interim agreement

It is agreed that protection of the Xn and Xx interfaces is done using same principles as in TS 33.401and according to NDS/IP as specified in TS 33.210.

E.4.11 Questions and interim agreements for key issue #4.11

E.4.11.1 Flexibility of retaining or changing AS security keys during HO

E.4.11.1.1 Description of question

Should flexibility of retaining or changing AS security keys during HO be addressed in Phase I?

Lenovo Ex. 1007
Page 485

E.4.11.1.2 Interim agreement

Yes.

E.4.12 Questions and interim agreements for key issue #4.12

E.4.13 Questions and interim agreements for key issue #4.13

E.4.13.1 Prevention of radio jamming attack

E.4.13.1.1 Description of question

Should prevention of low power jamming attack be addressed in Phase I?

E.4.13.1.2 Interim agreement

No.

E.4.13.2 Detection of radio jamming attack

E.4.13.2.1 Description of question

Should detection of low power jamming attack be addressed in Phase I?

E.4.13.2.2 Interim agreement

No.

E.4.14 Questions and interim agreements for key issue #4.14

E.4.14.1 Addressing privacy of RAN level temporary identifiers

E.4.14.1.1 Description of question

Is there a need of NextGen specific privacy solution for RAN level temporary identifiers?

E.4.14.1.2 Interim agreement

It is agreed that this is not to be addressed in Phase 1.

E.5 Questions and Interim Agreements for security area #5

E.5.1 Questions and Interim Agreements for Key Issue #5.1

E.5.1.0 Questions in other clauses affecting this key issue

E.5.1.1 Storage of Credentials

E.5.1.1.1 Description of Question

What are the requirements that shall apply to secure the storage and processing of credentials within the NG UE used for the authentication with the 5G network?

Lenovo Ex. 1007
Page 486

What solution shall be used for storage and processing of credentials within the NG UE used for the authentication with the 5G network?

E.5.1.1.2 Interim Agreement

Requirements in clause 5.5.3.1.3 are the agreed requirements for storage and processing of subscription credentials in the normative work for Phase 1.

The solutions for credentials storage and processing in Phase 1 shall be the UICC and the new SSP (Smart Secure Platform) under discussion in ETSI SCP (with the caveats that the SSP is defined within the Rel 15 timeframe and if it complies with the requirements in 5.5.3.1.3).

NOTE 1: If the SSP is not available in Rel 15 then the related part of the interim agreement has to be revisited.

NOTE 2: Additional solutions can be considered in the normative phase if they comply with the requirements in clause 5.5.3.1.3.

NOTE 3: 3GPP CT6 is in charge of specifying the NextGen USIM and additional non security requirements to the tamper resistant secure hardware component.

E.17 Questions and Interim Agreements for security area #17

E.17.1 Questions and Interim Agreements for cryptographic algorithms

E.17.1.1 Choice for cryptographic algorithms

E.17.1.1.1 Description of Question

Question: Which cryptographic algorithms are to be supported in Phase 1?

E.17.1.1.2 Interim Agreement

The only non-NULL algorithms to be supported in Phase 1 are the following:

EEA1, EEA2 and EEA3 specified in TS 33.401 [31] with the rules for being mandatory/optional the same as in LTE

EIA1, EIA2 and EIA3 specified in TS 33.401 [31] with the rules for being mandatory/optional the same as in LTE.

NOTE: the algorithms will probably be given 5G specific names

E.17.1.2 5G signalling supporting to carry 256-bit keys

E.17.1.2.1 Description of Question

Question: Shall the 5G signalling be designed to carry 256 -bit keys?

E.17.1.2.2 Interim Agreement

Yes

Lenovo Ex. 1007
Page 487

Annex F:
Comparison on non 3GPP access solutions

The non3GPP access solutions are compared below based on different impact areas. All the solutions are expected to support a unified authentication scheme by the NG core. For different procedures the functionality expected at N3IWF and other nodes are captured below.

Impact area	**Solution 5.1.4.26 Untrusted non-3GPP access**	**Solution 5.14.27 AKA procedure for untrusted non 3GPP access**	**Solution 5.1.4.28 AKA procedure for next gen standalone non-3GPP access**	**Solution 5.2.4.25 #2.25** Authentication Procedure for un-trusted non-3GPP access
Untrusted access discovery and attach to N3IWF	No change to untrusted access discovery connection to N3IWF	No change to untrusted access discovery, but changes to N3IWF set up.	No change to untrusted access discovery, but changes to N3IWF set up.	No change to untrusted access discovery, but changes to N3IWF set up.
IKEv2 procedure	No change to IKEv2	No IKEv2 modification	IKEv2 needs modification to carry additional EPS AKA parameters	IKEv2 carries Attach parameters
'Initial Attach Request' to NG Core (EPS AKA)	N3IWF makes the 'Initial Attach Request' on behalf of the UE.	N3IWF makes the 'Initial Attach Request' on behalf of the UE.	UE makes the Initial Attach Request, but this needs changes in EAP messages. 1.EAP-RSP needs to carry entire 'Attach Request'	Attach Request is carried in 3GPP specific IKEv2
NG-PDG Functions	1)NG PDG forms Initial Attach Request on behalf of UE and sends to AMF. 2) NG PDG maintains N2 to AMF and N3 to UPF. 3) Maintains IPSec between UE and NG-PDG. 4) Maintains child SAs for each QoS flows	1)N3IWF is similar to ePDG, transparently forwards the NAS messages via N2' 2) NG2 is different from N2 to gNB? 3)NG PDG sends data packets to UPF (N3).	1)N3IWF is similar to ePDG, transparently forwards the NAS messages via N2' 2) N2' is different from N2 to gNB? 3)NG PDG sends data packets to UPF (N3). 4) Maintains child SAs for each QoS flows	1) User plane data is carried in IPSec child SAs.

Lenovo Ex. 1007
Page 488

Annex G:
Change history

Lenovo Ex. 1007
Page 489

Change history							
date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2016-05	SA3#83	S3-160436				Initial version	0.1.0
2016-05	SA3#83	S3-160815				Version after SA3#83 incorporating changes from S3-160814, S3-160838, S3-160844, S3-160504, S3-160840, S3-160841, S3-160842, S3-160830, S3-160839, S3-160837, S3-160843, S3-160836, S3-160835, S3-160828, S3-160813, S3-160826, S3-160852, S3-160846, S3-160847, S3-160848, S3-160849 S3-160845, S3-160825, S3-160855, S3-160854, S3-160853 S3-160850, S3-160851, S3-160856, S3-160659, S3-160817	0.2.0
2016-07	SA3#83					Implementation of S3-160603 approved in SAS3#83	0.3.0
2016-08	SA3#84	S3-161290				Version after SA3#84 incorporating changes from S3-161184, S3-161185, S3-161186, S3-161188, S3-161189, S3-161192, S3-161259, S3-161067, S3-161069, S3-161070, S3-161194, S3-161197, S3-161191, S3-160945, S3-161198, S3-161074, S3-161201, S3-161202, S3-161199, S3-161260, S3-161203, S3-161204, S3-161200, S3-161043, S3-161076, S3-161205, S3-161206, S3-161207, S3-161208, S3-161082, S3-161210, S3-161209, S3-161211, S3-161267, S3-161268, S3-161269, S3-161270, S3-161271, S3-161273, S3-160979, S3-161272, S3-161274, S3-161275, S3-161276, S3-161277, S3-161278, S3-161279, S3-161279, S3-161280, S3-161281, S3-161282, S3-161257, S3-161090, S3-160957, S3-161285, S3-160959, S3-160960, S3-160961, S3-160962, S3-160963, S3-160976, S3-161287, S3-161288, S3-161289, S3-161212, S3-161214, S3-161213, S3-161215, S3-161258, S3-161262, S3-161261, S3-161264, S3-161265, S3-161266, S3-161190, S3-161183, S3-161187, S3-161263, S3-161193	0.4.0
2016-08						Clean version removing revision marks (MCC)	0.4.1
2016-10	SA3# 84bis					Version after SA3#NextGen (84bis) incorporating changes from S3-161395, S3-161524, S3-161525, S3-161526, S3-161467, S3-161420, S3-161462, S3-161481, S3-161482, S3-161483, S3-161484, S3-161485, S3-161486, S3-161487, S3-161488, S3-161489, S3-161490, S3-161375, S3-161491, S3-161508, S3-161492, S3-161493, S3-161494, S3-161409, S3-161495, S3-161397, S3-161496, S3-161440, S3-161498, S3-161499, S3-161500, S3-161501, S3-161502, S3-161503, S3-161504, S3-161505, S3-161506, S3-161507, S3-161510, S3-161530, S3-161531, S3-161532, S3-161343, S3-161344, S3-161512, S3-161497, S3-161374, S3-161317, S3-161529, S3-161528, S3-161513, S3-161514, S3-161423, S3-161515, S3-161516, S3-161517, S3-161303, S3-161429, S3-161518, S3-161519, S3-161520, S3-161521, S3-161522, S3-161523	0.5.0
2016-11	SA3#85	S3-162138				Version after SA3#85 incorporating changes from S3-161675, S3-161971, S3-161972, S3-161973, S3-161747, S3-161974, S3-161750, S3-161975, S3-161976, S3-162140, S3-161978, S3-161977, S3-161978, S3-161979, S3-162141, S3-161981, S3-161674, S3-161982, S3-161983, S3-161984, S3-161987, S3-162124, S3-161886, S3-161991, S3-161988, S3-161877, S3-161989, S3-161990, S3-161992, S3-162025, S3-161890, S3-161993, S3-161994, S3-161688, S3-162022, S3-162023, S3-162024, S3-162026, S3-162027, S3-162028, S3-161755, S3-161770, S3-162029, S3-161797, S3-161800, S3-161889, S3-161899, S3-162031, S3-161730, S3-162033, S3-162034, S3-162035, S3-162036, S3-162037, S3-162038, S3-162080, S3-162039, S3-161894, S3-161668, S3-161723, S3-162040, S3-162041, S3-161662, S3-161864, S3-162042, S3-162043, S3-162032, S3-162044, S3-162083, S3-161660, S3-162130, S3-162079, S3-162048, S3-162096, S3-162097, S3-162098, S3-162099, S3-162100, S3-162101, S3-161793, S3-161842, S3-161732, S3-161836, S3-162102, S3-161620, S3-162105, S3-162106, S3-162103, S3-161837, S3-161838, S3-161839, S3-161858, S3-161681, S3-161759, S3-162107, S3-161853, S3-162108, S3-161856, S3-162109, S3-161788, S3-162114, S3-162110, S3-162111, S3-162112, S3-162113, S3-161903, S3-161949, S3-162115, S3-162116, S3-162117, S3-162118, S3-161802, S3-162119, S3-162120, S3-162121, S3-162131, S3-162132, S3-162133, S3-161234, S3-161235, S3-161893, S3-162136	0.6.0
2017-02	SA3#86	S3-170503				Version after SA3#86 incorporating changes from S3-170488, S3-170215, S3-170361, S3-170362, S3-170363, S3-170339, S3-170233, S3-170269, S3-170389, S3-170388, S3-170296, S3-170428, S3-170377, S3-170378, S3-170158, S3-170379, S3-170380, S3-170119, S3-170381, S3-170382, S3-170383, S3-170384, S3-170385, S3-170386, S3-170387, S3-170274,	0.7.0

Lenovo Ex. 1007
Page 490

						S3-170391, S3-170393, S3-170395, S3-170292, S3-170396, S3-170397, S3-170398, S3-170399, S3-170400, S3-170401, S3-170128, S3-170403, S3-170268, S3-170426, S3-170405, S3-170406, S3-170078, S3-170257, S3-170123, S3-170407, S3-170303, S3-170410, S3-170042, S3-170043, S3-170430, S3-170431, S3-170047, S3-170432, S3-170049, S3-170050, S3-170435, S3-170433, S3-170412, S3-170436, S3-170438, S3-170439, S3-170440, S3-170441, S3-170442, S3-170466, S3-170443, S3-170445, S3-170229, S3-170234, S3-170446, S3-170221, S3-170222, S3-170447, S3-170448, S3-170449, S3-170450, S3-170451, S3-170228, S3-170231, S3-170305, S3-170461, S3-170462, S3-170219, S3-170463, S3-170230, S3-170300, S3-170444, S3-170367, S3-170059, S3-170500, S3-170501, S3-170502, S3-161702 (figure 5.1.4.9.2.2-1), S3-161705 (figure 5.2.4.13.2-1)	
2017-03	SA#75	SP-170096				Presented for information	1.0.0
2017-03	SA3#86 bis	S3-170962				Version after SA3#86 incorporating changes from S3-170905, S3-170906, S3-170907, S3-170908, S3-170910, S3-170911, S3-170639, S3-170922, S3-170641, S3-170923, S3-170924, S3-170943, S3-170942,S3-170785, S3-170945, S3-170947, S3-170948, S3-170891, S3-170909, S3-170921, S3-170745, S3-170949, S3-170954, S3-170885, S3-170950, S3-170952, S3-170733, S3-170958, S3-170957, S3-170959, S3-170960, S3-170882, S3-170883, S3-170886, S3-170955	1.1.0

Lenovo Ex. 1007
Page 491