

CHANGE REQUEST	
CR-Form-v9.4	
33.402 CR 0030	rev 2 Current version: 8.1.1

For [HELP](#) on using this form look at the pop-up text over the ¶ symbols. Comprehensive instructions on how to use this form can be found at <http://www.3gpp.org/specs/CR.htm>.

Proposed change affects: UICC apps ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	¶ Alignment of TS 33.402 to draft-arkko-eap-aka-kdf and clarification of indication of type of authentication from AAA to HSS
Source to WG:	¶ Ericsson, Nokia Corporation, Nokia Siemens Networks
Source to TSG:	¶ SA3
Work item code:	¶ SAES
Date:	¶ 03/11/2008
Category:	¶ F
Use <u>one</u> of the following categories:	
F (correction)	
A (corresponds to a correction in an earlier release)	
B (addition of feature),	
C (functional modification of feature)	
D (editorial modification)	
Detailed explanations of the above categories can be found in 3GPP TR 21.900 .	
Release:	¶ Rel-8
Use <u>one</u> of the following releases:	
R99 (Release 1999)	
Rel-4 (Release 4)	
Rel-5 (Release 5)	
Rel-6 (Release 6)	
Rel-7 (Release 7)	
Rel-8 (Release 8)	
Rel-9 (Release 9)	

Reason for change:	¶ Alignment with draft-arkko-eap-aka-kdf which defines EAP-AKA'. Current text in clause 6.2, step 6, reads "The 3GPP AAA server includes an indication that the authentication vector is for EPS use...". This is inaccurate as it was agreed at the last SA3 meeting that EPS use of AKA includes both EAP-AKA', as described in clause 6.2 for trusted access over S2a, and ordinary use of EAP-AKA, as described in RFC 4187, for untrusted access and access over S2c.
Summary of change:	¶ Alignment with draft-arkko-eap-aka-kdf which defines EAP-AKA'. More accurate text is proposed for step 6 of clause 6.2. Clarifying references are added to clauses 8.2.1 and 9.2.2.1
Consequences if not approved:	¶ Misalignment with draft-arkko-eap-aka-kdf which defines EAP-AKA'. Risk of HSS delivering the wrong type of authentication vectors.

Clauses affected:	¶ 2, 6.1, 6.2, 6.3, 8.2.1, 7.2.1.4, 9.2.1.2.1 and 9.2.2.1								
Other specs affected:	¶ <table><tr><td>Y</td><td>N</td></tr><tr><td>X</td><td></td></tr></table> Other core specifications ¶ 29.273 <table><tr><td>X</td><td></td></tr><tr><td>X</td><td></td></tr></table> Test specifications O&M Specifications	Y	N	X		X		X	
Y	N								
X									
X									
X									
Other comments:	¶ Reference to TS 24.302 is added in CR 0033, and the reference is used in the present CR.								

Commented [H1]: Document numbers are allocated by the Working Group Secretary. Use the format of document number specified by the [3GPP Working Procedures](#).

Commented [H2]: Enter the specification number in this box. For example, 04.08 or 31.102. Do not prefix the number with anything . i.e. do not use "TS", "GSM" or "3GPP" etc.

Commented [H3]: Enter the CR number here. This number is allocated by the 3GPP support team. It consists of at least four digits, padded with leading zeros if necessary.

Commented [H4]: Enter the revision number of the CR here. If it is the first version, use a "-".

Commented [H5]: Enter the version of the specification here. This number is the version of the specification to which the CR was written and (normally) to which it will be applied if it is approved. Make sure that the latest version of the specification (of the relevant release) is used when creating the CR. If unsure what the latest version is, go to <http://www.3gpp.org/specs/specs.htm>.

Commented [H6]: For help on how to fill out a field, place the mouse pointer over the special symbol closest to the field in question.

***** start first change *****

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] IETF RFC 4877: "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture".
- [3] IETF RFC 4306: "Internet Key Exchange (IKEv2) Protocol".
- [4] draft-ietf-dime-mip6-split-06.txt: "Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction".
- [5] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".
- [6] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".
- [7] IETF RFC 4187 (January 2006): "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".
- [8] 3GPP TS 23.003: "Numbering, addressing and identification".
- [9] 3GPP TS 33.234: "3G: security; Wireless Local Area Network (WLAN) interworking security".
- [10] IETF RFC 4072 (August 2005): "Diameter Extensible Authentication Protocol (EAP) Application".
- [11] 3GPP TS 33.102: "3G security; Security architecture".
- [12] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".
- [13] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".
- [14] 3GPP TS 23.203: "Policy and charging control architecture".
- [15] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN); Overall description; Stage 2".
- [16] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security Architecture".
- [17] IETF RFC 3344: "IP Mobility Support for IPv4".
- [18] IETF RFC 4555: "IKEv2 Mobility and Multihoming Protocol (MOBIKE)".
- [19] IETF Internet-Draft, draft-ietf-hokey-ems-k-hierarchy-07: "Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)", work in Progress
- [20] 3GPP TS 24.303: "Mobility Management based on Dual-Stack Mobile IPv6; Stage 3"

[yy] IETF Internet-Draft, draft-arkko-eap-aka-kdf-09: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", work in Progress

***** start next change *****

6.1 General

Access authentication for non-3GPP access in EPS shall be based on EAP-AKA [7] or on EAP-AKA' [yy]. The EAP server for EAP-AKA and EAP-AKA' shall be the 3GPP AAA server residing in the EPC.

The UE and 3GPP AAA server shall implement both EAP-AKA and EAP-AKA'. It is specified in this specification in which cases EAP-AKA and EAP-AKA' respectively shall be used.

If the terminal supports 3GPP access capabilities, the credentials used with EAP-AKA and EAP-AKA' shall reside on the UICC.

If the terminal does not support 3GPP access capabilities, 3GPP does not specify where the credentials used with EAP-AKA and EAP-AKA' reside.

NOTE: EAP-AKA and EAP-AKA' may use the same credentials.

The procedure in clause 6.2 shall be performed whenever the procedure in clause 8 of the present document is not performed with the following exception:

- if the security procedure in clause 9.2.2.2 for DS-MIPv6 is performed over a trusted access network and
- if the trusted access network has the properties listed in clause 9.2.2.1

then the procedure in clause 6.2 may be skipped.

However, it is recommended to use the procedure in clause 6.2 unless another strong authentication and key establishment method is used, which is documented in a standard covering the non-3GPP access network.

NOTE: There are cases when the procedure in clause 6.2 cannot be performed due to lack of support for EAP in the access network. DSL-based access networks are examples of such access networks.

In cases where it is difficult to assess whether a given access network has the properties listed in clause 9.2.2.1, it is strongly recommended to use the procedures for untrusted access in clause 8.

The HSS shall send an authentication vector with AMF separation bit = 1 (cf. TS 33.401 [16]) to a 3GPP AAA server as specified for the EAP-AKA' procedures defined in the present document. For authentication vectors with the "separation bit" set to 1, the secret keys CK and IK generated during AKA shall never leave the HSS, and shall not be used in a non-EPS context.

Editor's Note: Shall the credentials used with EAP-AKA reside on the UICC for all cases in non-3GPP accesses ?.

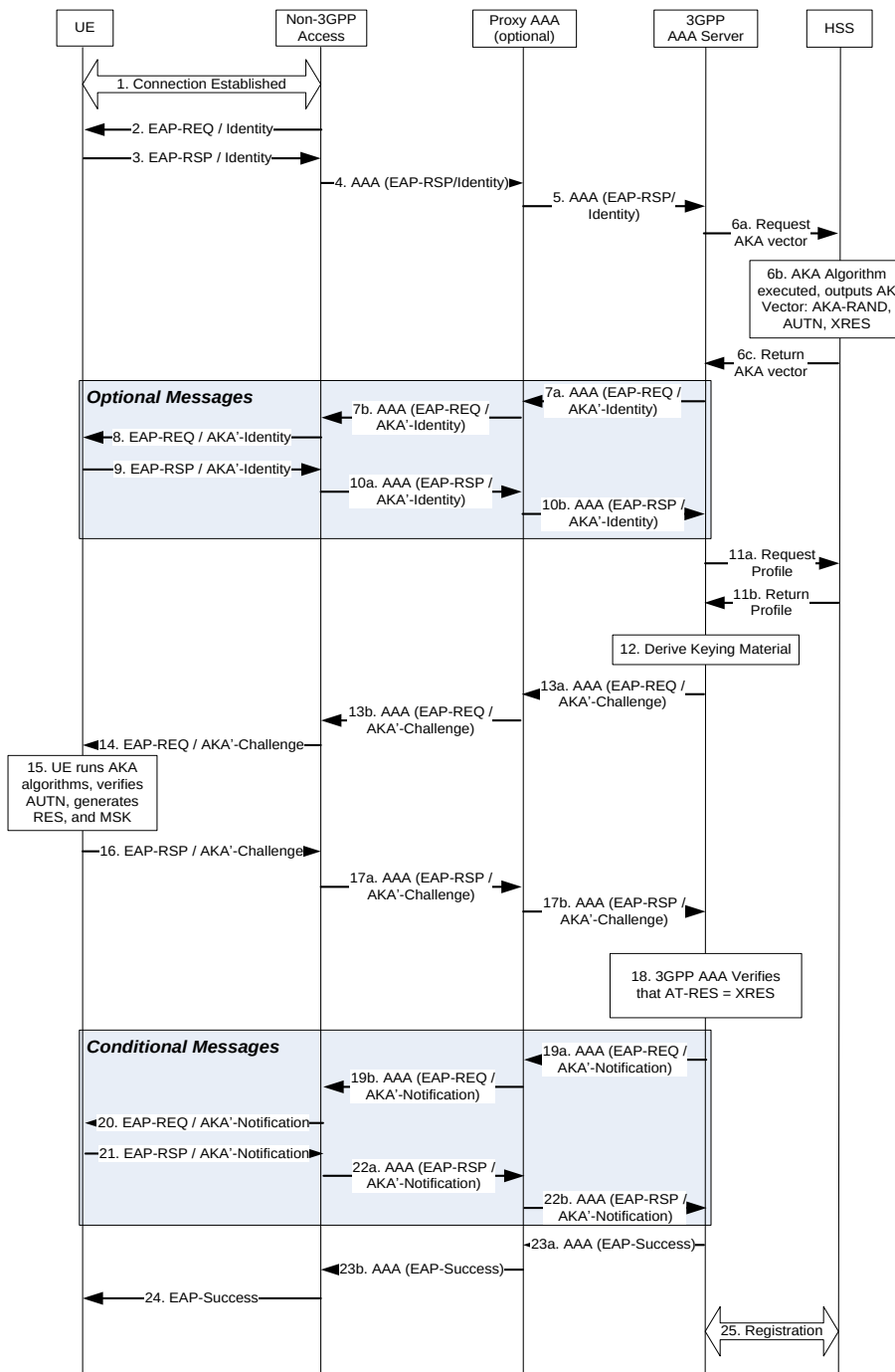
The non-3GPP access networks, which are trusted, can be pre-configured in the UE. The UE can e.g. have a list with non-3GPP access technologies, or access networks, or serving network operators that allow procedures for trusted non-3GPP IP access. Additionally, during 3GPP-based access authentication the UE may receive an indication whether the non-3GPP IP access is trusted or not. If such an indication is sent it shall be sent by the 3GPP AAA server as part of an EAP-AKA or EAP-AKA' request. If no such indication is received by the UE, and there is no pre-configured information in the UE, the UE shall consider the non-3GPP IP access as untrusted. In case of pre-configured information and indication received as part of an EAP-AKA or EAP-AKA' request are in conflict, the received indication shall take precedence.

NOTE: ~~the~~The protection mechanisms of EAP-AKA and EAP-AKA' prevent that an indication sent as part of an EAP-AKA request could be forged.

Formatted: NO

***** start next change *****

6.2 Authentication and key agreement for trusted access



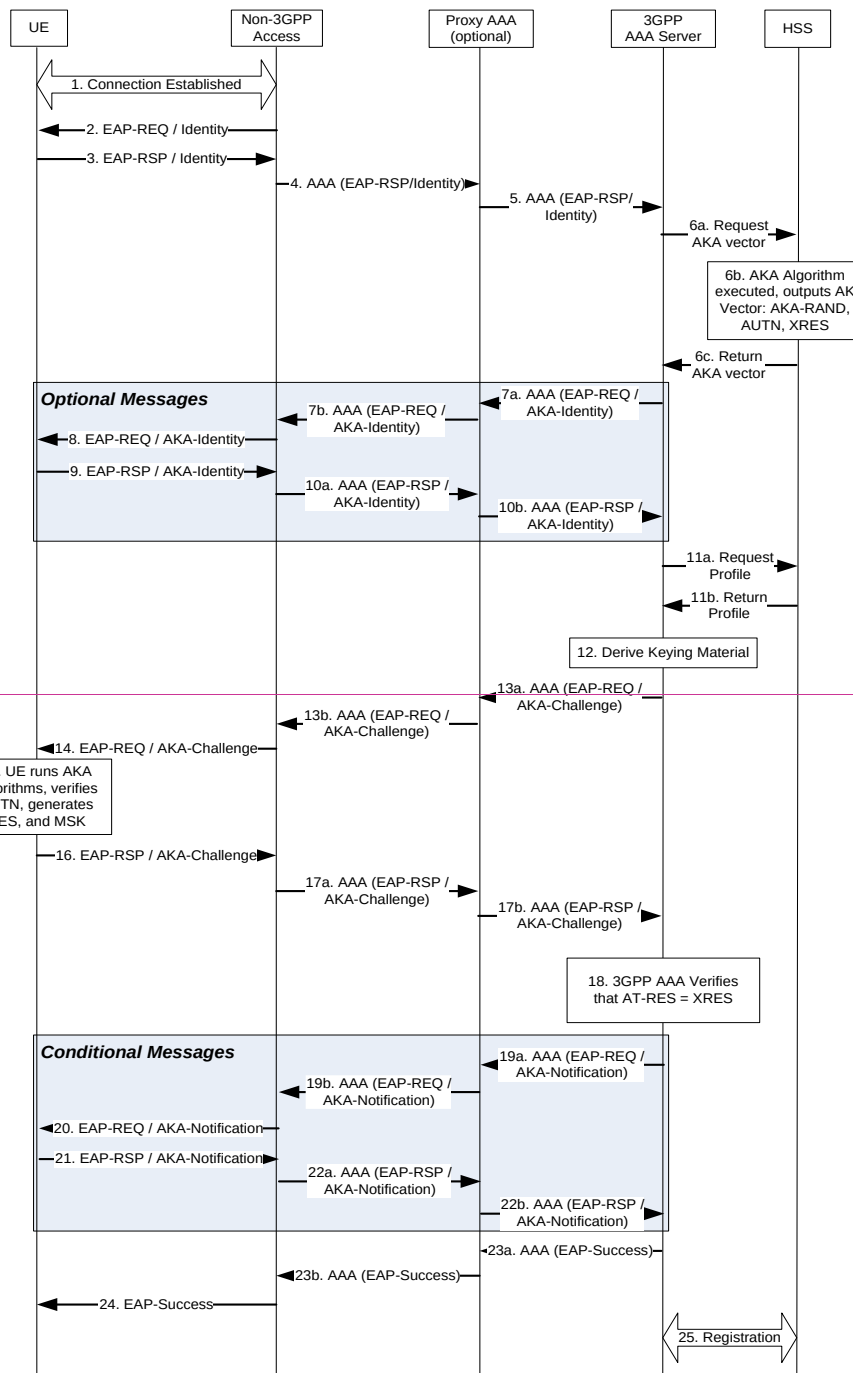


Figure 6.2-1: Non-3GPP Access Authentication

EAP-AKA' as defined in [yy] shall be used for mutual authentication and key agreement.

1. A connection is established between the UE and the trusted non-3GPP access network, using a procedure specific to the non-3GPP access network (which is out of scope for the present document).
2. The authenticator in the trusted non-3GPP access network sends an EAP Request/Identity to the UE.

NOTE 1: EAP packets are transported over this access network using a protocol specific to this access network (which is out of scope for the present document).

3. The UE sends an EAP Response/Identity message. The UE shall send its identity complying with Network Access Identifier (NAI) format specified in TS 23.003 [8]. NAI contains either a pseudonym allocated to the UE in a previous run of the authentication procedure or, in the case of first authentication, the IMSI. In the case of first authentication, the NAI shall indicate EAP-AKA as specified in TS 23.003 [8].
4. The message is routed towards the proper 3GPP AAA Server based on the realm part of the NAI as specified in TS 23.003 [8]. The routing path may include one or several AAA proxies. The access type and the identity of the access network in which the authenticator resides, shall be included by the authenticator in the Diameter message. In the case of roaming, the visited network AAA proxy shall also include the visited network identifier in the same Diameter message.
The access network identity is defined separately for each access network type. For each access network type, the access network identity shall be documented in TS 23.00324.302 [zz8] to ensure that UE and HSS use the same access network identities as input for key derivation.

NOTE 2: Diameter referral can also be applied to find the AAA server.

NOTE 3: The visited network identifier identifies a visited 3GPP network, and is to be distinguished from the access network identifier, which relates to a non-3GPP access network.

5. The 3GPP AAA Server receives the EAP Response/Identity message that contains the subscriber identity and the access type over the Ta*/ Wd* interface. In the case of roaming, the 3GPP AAA server also receives the visited network identifier in the same Diameter message that carried the EAP Response/Identity message.
6. The 3GPP AAA Server checks whether it has an unused authentication vector with AMF separation bit = 1 and the matching access network identifier available for that subscriber. If not, a set of new authentication vectors is retrieved from HSS. The 3GPP AAA server includes an indication that the authentication vector is for EAP-AKA', as defined [yy]EPS use, and the identity of the access network in which the authenticator resides in a message sent to the HSS. A mapping from the temporary identifier (pseudonym in the sense of RFC 4187 EAP-AKA [7]) to the IMSI is required.

NOTE_4: As the UE moves around the access network identifier may change. But an authentication vector stored in the 3GPP AAA server can only be used if it is associated with the access network identifier of the current access network. This may make stored authentication vectors unusable. Furthermore, as the 3GPP AAA server resides in the home network there is no significant performance advantage in fetching batches of authentication vectors. It is therefore recommended that the 3GPP AAA server fetches only one authentication vector at a time.

Upon receiving from the 3GPP AAA server an indication that the authentication vector is for EAP-AKA' as defined in [yy], the HSS generates an authentication vector with AMF separation bit = 1. The HSS then transforms this authentication vector into a new authentication vector by computing (CK', IK') = F(CK, IK, <access network identity>) where F is a key derivation function. The HSS then sends this transformed authentication vector to the 3GPP AAA server.

NOTE 5: The 3GPP AAA server does not notice the transformation and treats this authentication vector like any other authentication vector.

NOTE 6: The HSS and/or 3GPP AAA server need to ensure that the non-3GPP access requesting the authentication data is entitled to use the access network identity used to calculate CK' and IK'. The exact details of how to achieve this are not covered in this specification.

UE and 3GPP AAA server need to know when to apply the new EPS specific processing of EAP-AKA. This can be achieved by several means:

Formatted: Not Highlight

1. Indication about support for EPS security procedures, as defined in this specification, and for I-WLAN security procedures, as defined in 3G TS 33.234, may be exchanged as part of EAP-AKA messages. In this way, a 3GPP AAA server in the EPC capable of supporting both, EPS security procedures and I-WLAN security procedures, can also serve legacy UEs supporting only I-WLAN security procedures. Details of these selection procedures can be found in 3GPP TS 24.302.
2. Indication about the security procedures supported by the UE may also be provided as part of reserved NAI realms, cf. definitions of NAI in TS 23.003. Additionally,
3. Configuration in the UE or in the 3GPP AAA server, e.g. there may be lists with non-3GPP access technologies, or access networks, or serving network operators that allow only procedures for access to the EPC.

In case information received by various of the above means is in conflict, then the following order of precedence shall apply: information in EAP-AKA messages shall take precedence over information received in NAIs, which in turn shall take precedence over pre-configured information.

Editor's Note: The second bullet in the preceding paragraph is ffs in stage 3 work by CT1 and CT4. There is ongoing work at the IETF regarding the first bullet in the preceding paragraph. If this work is not finalized by the end of Rel-8, this bullet will be deleted. If this work is finalized by the end of Rel-8 then UE and 3GPP AAA server shall comply with the provisions of the corresponding new RFC. —

Editor's Note: It is ffs whether and how legacy UEs (which do not support EPS procedures) are served by the EPC as this may have an impact on network entities serving both EPS and legacy UEs, in particular in the context of EAP-AKA procedures.

The HSS shall check if there is a 3GPP AAA Server already registered to serve for this subscriber. In case the HSS detects that another 3GPP AAA Server has already registered for this subscriber, it shall provide the current 3GPP AAA Server with the previously registered 3GPP AAA Server address. The authentication signalling is then routed to the previously registered 3GPP AAA Server with Diameter-specific mechanisms, e.g., the current 3GPP AAA Server transfers the previously registered 3GPP AAA Server address to the 3GPP AAA proxy or the AAA entity in the trusted non-3GPP access network, or the current 3GPP AAA Server acts as a AAA proxy and forwards the authentication message to the previously registered 3GPP AAA Server.

7. The 3GPP AAA Server requests again the user identity, using the EAP Request/AKA Identity message. This identity request is performed as the intermediate nodes may have changed or replaced the user identity received in the EAP Response Identity message, as specified in [draft-arkko-eap-aka-kdf RFC 4187 EAP-AKA-\[7yy\]](#). However, in order to avoid this new request of the user identity, the home operator should ensure that the Authenticator and all AAA entities between the EAP peer and EAP server process the EAP-Response/Identity message inline with EAP-AKA' as specified in the present document and TS 23.003. Consequently, if the EAP server knows that the EAP-Response/Identity message was processed accordingly, the EAP server shall use the user identity which was received in the EAP-Response/Identity message in step 5 and skip this EAP Request/AKA' Identity request in steps 7 through 10.
8. The authenticator in the access network forwards the EAP Request/AKA' Identity message to the UE.
9. The UE responds with the same identity it used in the previous EAP Response Identity message.
10. The authenticator in the access network forwards the EAP Response/AKA' Identity to the 3GPP AAA Server. The identity received in this message will be used by the 3GPP AAA Server in the rest of the authentication process. If an inconsistency is found between the identities received in the two messages (EAP Response Identity and EAP Response/AKA' Identity) so that the user profile and authentication vectors previously retrieved from HSS are not valid, these data shall be requested again to HSS (step 6 shall be repeated before continuing with step 11).

NOTE 7: In order to optimise performance, the identity re-request process (the latter four steps) should be performed before user profile and authentication vectors retrieval.

11. 3GPP AAA Server checks that it has the EPS access profile of the subscriber available. If not, the profile is retrieved from HSS. 3GPP AAA Server verifies that the subscriber is authorized to use the EPS.

NOTE 8: This step could be performed at some other point, after step 5 and before step 14.

12. New keying material MSK is derived from CK' and IK' according to [draft-arkko-eap-aka-kdf RFC 4187 EAP-AKA-\[7yy\]](#).

A new pseudonym and/or re-authentication ID may be chosen and if chosen they shall be protected (i.e. encrypted and integrity protected) using keying material generated from EAP-AKA.

13. The 3GPP AAA Server sends RAND, AUTN, a message authentication code (MAC) and two user identities (if they are generated), protected pseudonym and/or protected re-authentication id, to the authenticator in the access network in EAP Request/AKA'-Challenge message. The 3GPP AAA Server ~~may-shall~~ also include the access network identity in this message. ~~Alternatively, the access network identity may be provided by link layer means. Depending on the definition of the access network identity for a particular access technology, the access network identity may also be configured into the UE and the 3GPP AAA server. The access network identity is defined in TS 23.00324.302 [zz]. Information in an EAP message shall take precedence over the information over information provided by the link layer, which in turn shall take precedence over pre-configured information.~~ The sending of the re-authentication id depends on 3GPP operator's policies on whether to allow fast re-authentication processes or not. It implies that, at any time, the 3GPP AAA Server decides (based on policies set by the operator) to include the re-authentication id or not, thus allowing or disallowing the triggering of the fast re-authentication process.

~~Editor's note: There is ongoing work at the IETF regarding the transport of the access network identity in EAP-AKA. If this work is not finalized by the end of Rel-8, the corresponding sentence will be deleted.~~

The 3GPP AAA Server may send as well a result indication to the authenticator in the access network, in order to indicate that it wishes to protect the success result message at the end of the process (if the outcome is successful). The protection of result messages depends on home operator's policies.

14. The authenticator in the access network sends the EAP Request/AKA'-Challenge message to the UE.
15. The UE first checks whether the AMF separation bit is set to 1. If this is not the case the UE shall reject the authentication. Otherwise, the UE runs AKA algorithms on the USIM application on UICC. The USIM application verifies that AUTN is correct and hereby authenticates the network. If AUTN is incorrect, the terminal rejects the authentication (not shown in this example). If the sequence number is out of synch, terminal initiates a synchronization procedure, c.f. [draft-arkko-eap-aka-kdf RFC 4187 \[7yy\]](#). If AUTN is correct, the USIM application computes RES, IK and CK.

The UE then computes (CK', IK') = F(CK, IK, <access network identity>) in the same way as the HSS. The UE derives required additional new keying material, including the key MSK, according to [draft-arkko-eap-aka-kdf RFC 4187 EAP-AKA \[7yy\]](#) from the new computed CK', IK' and checks the received MAC with the new derived keying material.

If a protected pseudonym and/or re-authentication identity were received, then the UE stores the temporary identity(s) for future authentications.

~~NOTE 9: the text following NOTE 5 in step 6 applies also here.~~

~~The access network identity, which is input to key derivation to obtain CK', IK', may-shall be pre-configured into the UE, or obtained by link layer means, or sent by the 3GPP AAA server in the EAP-request / AKA'-Challenge message as defined in draft-arkko-eap-aka-kdf [yy]. Depending on the definition of the access network identity for a particular access technology, the access network identity may also be configured into the UE and the 3GPP AAA server. Information in an EAP message shall take precedence over the information over information provided by the link layer, which in turn shall take precedence over pre-configured information.~~

~~Editor's Note: There is ongoing work at the IETF regarding the transport of the access network identity in EAP-AKA. If this work is not finalized by the end of Rel-8, the corresponding part of the above paragraph will be deleted.~~

Draft-arkko-eap-aka-kdf [yy] specifies a possibility for the UE to compare the access network identity received from the 3GPP AAA server with the access network identity received locally, e.g. from the link layer. It is defined in 3GPP TS 24.302 [zz] for which access networks the comparison is done, how the UE shall determine the locally received network name and what the UE shall do if the check fails. If the comparison is done for a specific access network, it shall be done according to the rules specified in draft-arkko-eap-aka-kdf [yy]. The UE - or the human user - may use the network name as a basis for an authorization decision. E.g. the UE may compare the network name against a list of preferred or barred network names.

16. The UE calculates a new MAC value covering the EAP message with the new keying material. UE sends EAP Response/AKA'-Challenge containing calculated RES and the new calculated MAC value to the authenticator in the access network.

The UE shall include in this message the result indication if it received the same indication from the 3GPP AAA Server. Otherwise, the UE shall omit this indication.

17. The authenticator in the access network sends the EAP Response/AKA'-Challenge packet to 3GPP AAA Server.

18. The 3GPP AAA Server checks the received MAC and compares XRES to the received RES.

19. If all checks in step 18 are successful, the 3GPP AAA Server shall send the message EAP Request/AKA'-Notification, previous to the EAP Success message, if the 3GPP AAA Server and the UE have indicated the use of protected successful result indications as in [RFC 4187](#)[draft-arkko-eap-aka-kdf](#) [7yy]. This message is MAC protected.

NOTE 10: Steps 19 to 22 are conditional based on the EAP Server and the UE having indicated the use of protected successful result indications.

20. The authenticator in the access network forwards the message to the UE.

21. The UE sends the EAP Response/AKA'-Notification.

22. The authenticator in the access network forwards the EAP Response/AKA'-Notification message to the 3GPP AAA Server. The 3GPP AAA Server shall ignore the contents of this message

23. The 3GPP AAA Server sends the EAP Success message to the authenticator in the access network (perhaps preceded by an EAP Notification, as explained in step 20). The 3GPP AAA Server also includes the key MSK, [draft-arkko-eap-aka-kdf](#)[RFC 4187](#) [4yy], in the underlying AAA protocol message (i.e. not at the EAP level). The authenticator in the access network stores the keying material to be used in communication with the authenticated UE as required by the access network.

24. The authenticator in the access network informs the UE about the successful authentication with the EAP Success message. Now the EAP-AKA' exchange has been successfully completed, and the UE and the authenticator in the access network share keying material derived during that exchange.

25. The 3GPP AAA Server shall initiate the registration to the HSS. The 3GPP AAA Server shall keep access session information related to the subscriber including the access network identity. The 3GPP AAA Server shall implement a policy to limit the number of active access sessions.

NOTE 11: It may happen in handover situations that, due to pre-registration, a subscriber is authenticated in a target access network while still being attached to the source access network.

NOTE 12: More detailed provisions may be required for particular access networks, similar to those in bullet 25 in TS 33.234 [9], subclause 6.1.1.1 for WLAN access networks.

The authentication process may fail at any moment, for example because of unsuccessful checking of MACs or no response from the UE after a network request. In that case, the EAP AKA process will be terminated as specified in [draft-arkko-eap-aka-kdf](#) [RFC 4187](#) [7yy] and an indication shall be sent to HSS.

***** start next change *****

6.3 Fast re-authentication procedure for trusted access

Fast re-authentication for EAP-AKA' is specified in [draft-arkko-eap-aka-kdf](#) [RFC 4187](#) [yy7]. Fast re-authentication re-uses keys derived on the previous full authentication. Fast re-authentication does not involve the HSS nor the USIM application, and does not involve the handling of AKA authentication vectors, which makes the procedure faster and reduces the load on the HSS and, in particular, the Authentication Centre.

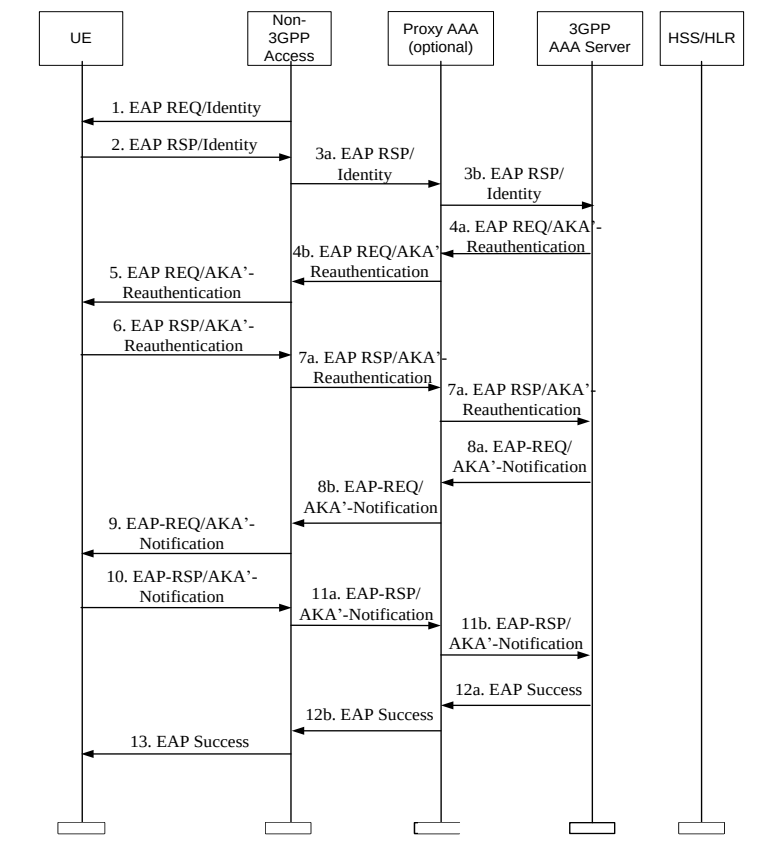
UE and 3GPP AAA server shall implement fast re-authentication for EAP-AKA'. Its use is optional and depends on operator policy. If fast re-authentication for EAP-AKA' is used the 3GPP AAA server shall indicate this to the UE by means of sending the re-authentication identity to the UE as in step 13 of subclause 6.2.

The security level of fast re-authentication for EAP-AKA' is lower as it does not prove the presence of the USIM application on the user side. The operator should take this into account when defining the policy on fast re-authentication.

Fast re-authentications for EAP-AKA' generates new keys MSK, which may be used for renewing session key used for protection in the non-3GPP access network.

The access network identity shall not change when going from the full to the fast re-authentication process. If this happens, the re-authentication process shall be terminated as defined in draft-arkko-eap-aka-kdf [yy].

In this section it is described how the process works for trusted non-3GPP access to EPS.



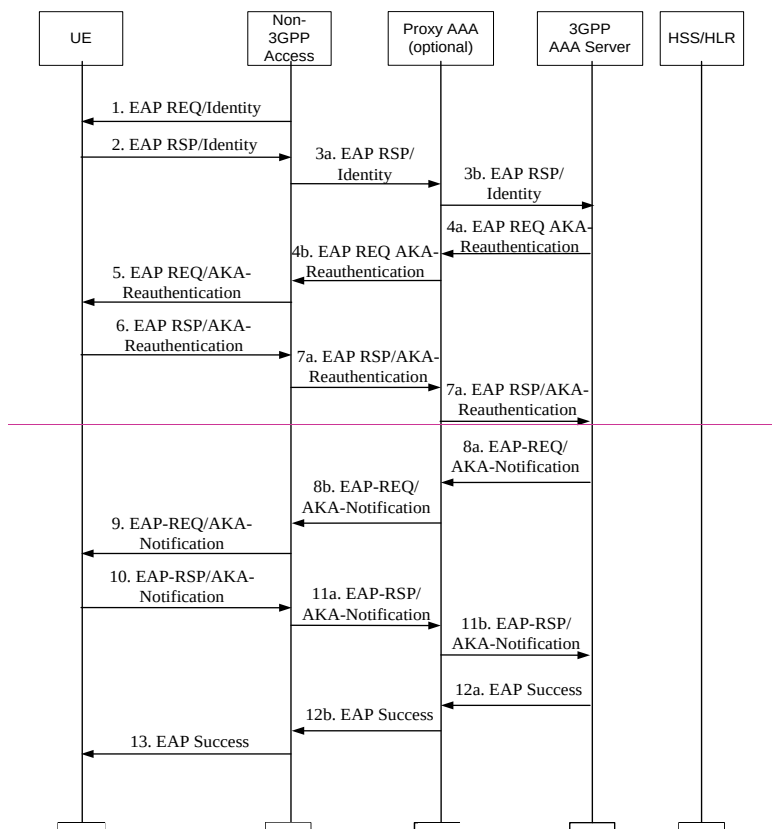


Figure 6.3-1: Non-3GPP Fast Re-authentication

1. Non-3GPP Access Network sends an EAP Request/Identity to the UE.
2. UE replies with an EAP Response/Identity containing a re-authentication identity (this identity was previously delivered by AAA server in a full authentication procedure).
3. The Non-3GPP Access Network forwards the EAP Response/Identity to the AAA server. Intermediate Proxy AAA's may perform routing and forwarding functions.
4. The AAA server initiates the Counter (which was initialized to one in the full authentication process) and sends it in the EAP Request message, together with the NONCE, the MAC (calculated over the NONCE) and a protected re-authentication ID for a next fast re-authentication. If the AAA server is not able to deliver a re-authentication identity, next time the UE shall force a full-authentication (to avoid the use of the re-authentication identity more than once).

The 3GPP AAA Server may send a result indication to the UE, in order to indicate that the success result message at the end of the process shall be protected (if the outcome is successful). The protection of result messages depends on home operator's policies.

The 3GPP AAA server may fail to recognize the identity as it may have been altered by proxies. In this case, the 3GPP AAA server may, as in the case of a full authentication, instead perform an EAP AKA' method specific identity request; i.e. "EAP-Request/AKA' identity [Any identity]" in order to obtain a more reliable

identity, in analogy of step 7 of the full EAP AKA' authentication. This should however only be used in case the server fails to recognize the identity, as otherwise the purpose of fast re-authentication is defeated.

5. The Non-3GPP Access Network forwards the EAP Request message to the UE.
6. The UE verifies that the Counter value is fresh and the MAC is correct, and it sends the EAP Response message with the same Counter value (it is up to the AAA server to step it up) and a calculated MAC.

The UE shall include in this message the result indication if it received the same indication from the 3GPP AAA. Otherwise, the UE shall omit this indication.
7. The Non-3GPP Access Network forwards the response toward the AAA server.
8. The AAA server verifies that the Counter value is the same as it sent, and the MAC is correct, and sends the message EAP Request/AKA'-Notification, previous to the EAP Success message, if the 3GPP AAA Server requested previously to use protected success result indications. The message EAP Request/AKA'-Notification is MAC protected, and includes an encrypted copy the Counter used in the present re-authentication process.
9. The Non-3GPP Access Network forwards the EAP Request/AKA'-Notification message to the UE.
10. The UE sends the EAP Response/AKA'-Notification.
11. The Non-3GPP Access Network forwards the EAP Response/AKA'-Notification message toward the 3GPP AAA server. The 3GPP AAA Server shall ignore the contents of this message.
12. The AAA server sends an EAP Success message. If some extra keying material was generated for Access Network specific confidentiality and/or integrity protection, then the 3GPP AAA Server includes this derived keying material in the underlying AAA protocol message. (i.e., not at EAP level). The Non-3GPP Access Network stores the keying material which may be used in communication with the authenticated UE.
13. The EAP Success message is forwarded to the UE.

The re-authentication process may fail at any moment, for example because of unsuccessful checking of MACs or no response from the UE after a network request. In that case, the EAP AKA process will be terminated as specified in [draft-arkko-eap-aka-kdf RFC 4187 \[yy7\]](#) and an indication shall be sent to HSS/HLR.

***** start next change *****

7.2.1.4 Security of the initial access to EPS via HRPD

EAP-AKA' access authentication shall be used according to section 6. As a result of EAP-AKA', the two keys, MSK and EMSK, are generated, cf. [draft-arkko-eap-aka-kdf RFC 4187 \[yy7\]](#).

In addition, according to subclause 6.2 of the present document, the 3GPP AAA Server sends the key MSK to the authenticator in the access network. The 3GPP AAA server shall retain the EMSK either until the subsequent EAP-AKA' authentication, or until it receives an indication that the current authenticated session is finished.

The security contexts in the HRPD access network may be based on keys derived from MSK. The HRPD access network is required to ensure that the identity of a user with whom a security context is established is securely tied to the identity of a user authenticated by EAP-AKA'.

The further details of the establishment of security contexts in the HRPD access network are outside the scope of the present document.

NOTE 1: Initial access to the EPS via HRPD is described in the TS 23.402 [5].

NOTE 2: TS 23.402 [5] requires access authentication for trusted non-3GPP systems to be based on EAP-AKA'.

***** start next change *****

8.2.1 General

- The UE and the ePDG shall use IKEv2, as specified in RFC 4306 [3], in order to establish IPsec security associations.
- Public key signature based authentication with certificates, as specified in RFC 4306 [3], shall be used to authenticate the ePDG. The ePDG shall authenticate itself to the UE with an identity. This identity shall be the same as the FQDN of the ePDG determined by the ePDG selection procedures defined in TS 23.402 [5]. This identity shall be contained in the IKEv2 ID_FQDN payload and shall match a dNSName SubjectAltName component in the ePDG's certificate.
- EAP-AKA, as specified in RFC 4187 [7], within IKEv2, as specified in RFC 4306 [3], shall be used to authenticate UEs.
- For profile for IKEv2, IPsec ESP and certificate contents and processing refer to subclause 8.2.4.

***** start next change *****

9.2.1.2.1 Procedures

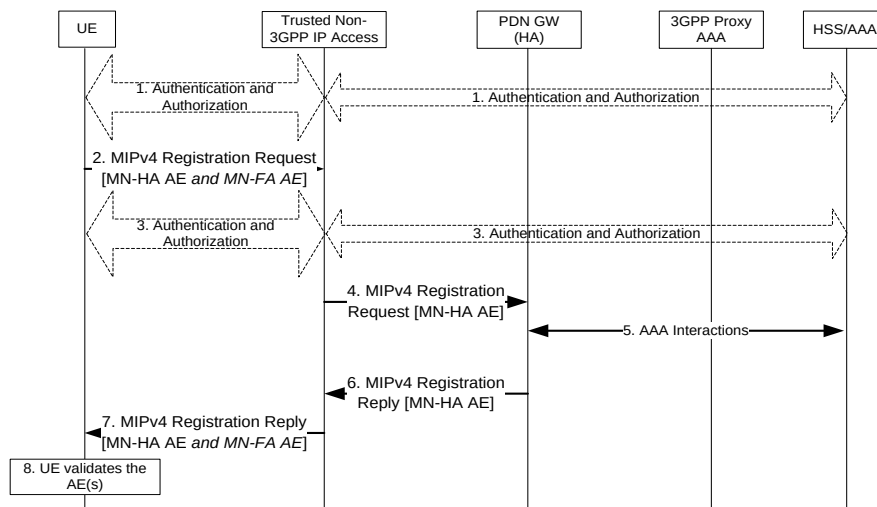


Figure 9.2.1.2.1-1: MIPv4 bootstrapping

The event that triggers Authentication and Authorization in step 1 or in step 3 between the Trusted Non-3GPP IP Access and the EAP Server cfr.TS 23.402 [5].

- 1) The Non-3GPP access specific authentication procedure based on EAP-AKA' is performed as specified in clause 6.2. Depending on the type of non-3GPP access system, the PDN GW address (HA address) may be determined at this point. The details of this procedure and IPMM protocol selection procedure are specified in TS 23.402 [5]. If the network selects mobility management protocol as MIPv4 FACoA for the UE, then the UE and the EPC derive the keys required for MIPv4 bootstrapping.

The key EMSK that result from the EAP-AKA' authentication procedure is used to derive MIPv4 bootstrapping keys. Section 9.2.1.2.2 shows the derivation of MIPv4 bootstrapping keys in the UE and in the 3GPP AAA server and the key distribution from the 3GPP AAA server to the mobility agents. The trusted non-3GPP network receives a set of mobility keys and other keys in the Access-Accept message as a result of successful authentication.

- 2) The UE sends a Registration Request (RRQ) message to the FA as specified in TS 23.402 [5]. The UE includes the MN-HA Authentication Extension (AE) and optionally the MN-FA Authentication Extension (AE) as specified in RFC 3344 [17].
- 3) In some non-3GPP access networks, the RRQ triggers the access authentication procedure TS 23.402 [5]. The Non-3GPP access specific authentication procedure based on EAP-AKA' is performed, if an authentication procedure is not preformed in step 1.

Editor's Note: MIPv4 key derivation and distribution for this scenario is FFS.

- 4) The FA processes the message according to RFC 3344 [17] and validates the MN-FA Authentication extension if present. The FA then forwards the RRQ message to the PDN GW. The RRQ message shall be protected between the FA and the PDN GW according to TS 33.210 [6].
- 5) The selected PDN GW obtains Authentication and Authorization information from the AAA/HSS.
- 6) The PDN GW validates the MN-HA authentication extension. After successful authentication extension validation, the PDN GW sends a Registration Reply (RRP) to the UE through the FA. The RRP message shall be protected between the PDN GW and the FA according to TS 33.210 [6].
- 7) The FA processes the RRP according to RFC 3344 [17]. The FA then forwards the RRP message to the UE. The FA includes the MN-FA authentication extension, if the FA received MN-FA authentication extension in the RRQ message.
- 8) The UE validates the MN-HA authentication extension and MN-FA authentication extension, if present.

***** start next change *****

9.2.2.1 General

The DS-MIPv6 security is based on IPsec as defined in RFC4877 [2]. The IPsec security association is established between the UE and the node acting as HA (i.e. PDN GW).

The following principles apply:

- The UE and the HA use IKEv2, as specified in RFC4306, in order to establish IPsec security associations.
- Public key signature based authentication with certificates, as specified in RFC 4306 [3], is used to authenticate the HA. The HA shall authenticate itself to the UE with an identity. This identity shall be the same as the FQDN of the HA if the HA is found via DNS cfr. TS 23.402 [5].
- EAP-AKA, [as specified in RFC 4187 \[7\]](#), within IKEv2, as specified in RFC4877 [2] and RFC 4306 [3], is used to authenticate UEs, which contain a USIM.

The following properties are needed to provide secure S2c over a Trusted Non-3GPP Access:

- The Trusted Access will authenticate the UE and provide a secure link for the data to be transferred from the UE to the Trusted Access.
- The Trusted Access protects against source IP address spoofing.
- The Trusted Access and PDN GW will have a secure link between them to transfer the user's data across.
- The Trusted Access and EPC need to co-ordinate when the UE detaches from the Trusted Access in order to ensure that the IP address that was assigned to the UE is not be used by another UE without EPC being aware of the change (i.e. enable the PDN GW to remove the CoA address binding for the old UE).

These properties ensure that the traffic the PDN GW is receiving has originated at the UE while UE is attached to the Trusted Access.

NOTE 1: If Trusted Access and EPC do not co-ordinate regarding UE detachment then the UE that was re-assigned the IP address would be capable of impersonating traffic until the binding in PDN GW timed out

NOTE 2: Procedures internal to the Trusted Access are outside the scope of the present document.

The allocation of IP addresses in the access network may provide the last property listed above. If the IP address is not re-allocated until after the MIP Binding has expired or IKE Dead Peer Detection has been run. This means that the PDN GW will no longer associate the old UE to the IP address once the new UE gets the IP address and hence there is no risk of impersonation attacks.

PCC may also be used to provide the last property listed above in access networks that support it. In the case that PCC is used, a GW control session is established between the Trusted Access and the PCRF. This GW control session is identified by the UE ID and the IP address allocated to the UE (i.e. CoA if DSMIPv6 is used). Using the GW control session, the UE is restricted to limited access; in particular, the Trusted Access restricts the forwarding of the packets only to IKEv2 and BU messages until the binding at the PDN GW is established. The Trusted Access knows when the binding is established at the PDN GW because it receives an update of the GW control session. The flows for this control of policy are given in section(s) 6.3 and 6.6.2 of TS 23.402. This prevents a UE that attaches to the Trusted Access from sending non-signalling traffic to the PDN GW until it has completed a BU with the PDN GW and prevents an impersonation attack.

***** end changes *****