

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Samsung Electronics America, Inc.
Samsung Electronics Co., Ltd.
Petitioners

v.

Koninklijke KPN N.V.
Patent Owner

IPR2025-00512
Patent 8,881,235

PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	MANDATORY DISCLOSURES	2
A.	Standing.....	2
B.	Real Party in Interest.....	2
C.	Related Matters.....	2
D.	Lead and Back-Up Counsel (37 C.F.R. § 42.8(b)(3)) and Service Information (37 C.F.R. § 42.8(b)(3)-(4)).....	3
E.	Payment of Fees (37 C.F.R. § 42.15(a)).....	4
III.	FOUNDATIONS.....	4
IV.	LEVEL OF ORDINARY SKILL IN THE ART	6
V.	TECHNOLOGY OVERVIEW (EX1003, ¶¶48-53)	6
VI.	THE '235 PATENT	8
A.	Overview	8
B.	Prosecution History.....	8
VII.	CLAIM CONSTRUCTION	10
A.	“service code” / “expected service code”	11
B.	“communication channel”	11
C.	“authentication data request”	12
D.	“service interface module”	12
E.	“identity module”.....	14
VIII.	OVERVIEW OF THE PRIOR ART	15
A.	TS-33.402 (EX1006).....	15

1.	TS-33.402 Qualifies as Prior Art.....	15
2.	Arkko (EX1008) Qualifies as Prior Art.....	17
B.	Naslund (EX1005).....	18
IX.	GROUND 1: TS-33.402 Alone Or In View of Arkko RENDERS OBVIOUS CLAIMS 1, 3-7, and 11-13.....	19
A.	Claim 1	19
1.	1[pre]: Method for service-based authentication of a terminal to a network, the terminal comprising one or more communications interfaces for setting-up a communication channel with the network, the method comprising:.....	19
2.	1[a]: the terminal sending a service request for access to a network service;	20
3.	1[b]: the terminal receiving in response to the service request an authentication request from the network;	21
4.	1[c]: the terminal identifying the communication channel through which the authentication request was received;	22
5.	1[d]: the terminal determining a service code associated with the identified communication channel; and	26
6.	1[e]: the terminal sending an authentication response to the network, wherein the authentication response depends on the identified communication channel in that the response is calculated on the basis of the information in the authentication request and the determined service code, thereby securely including information regarding the identified communication channel through which the authentication request was received into the response.	27
B.	Claim 3	29
1.	3[pre]: Method according to claim 1, wherein the authentication request comprises authentication	

	information[,] the method further comprising the steps of:	29
2.	3[a]: the terminal modifying the authentication information on the basis of the identified communications channel; and the terminal generating the authentication response on the basis of the modified authentication information.	29
C.	Claim 4	31
1.	4[pre]: Method according to claim 1, wherein the authentication request comprises authentication information, the method further comprising:.....	31
2.	4[a]: the terminal generating the authentication response;.....	31
3.	4[b]: the terminal modifying the authentication response on the basis of the identified communications channel.....	31
D.	Claim 5	32
1.	5[pre]/5[a]: Method according to claim 1, the method further comprising: the terminal sending a service request via a predetermined communications channel to the network;.....	32
2.	5[b]: the network generating an expected service code on the basis of the type of communications channel the service request was sent to the network; and 5[c]: determining on the basis of the expected service code an expected response.	32
E.	Claim 6	34
1.	6[pre]/6[a]: Method according to claim 5, the method further comprising: comparing the expected response with the authentication response sent by the terminal to the network; and	34
2.	6[b]: determining the terminal to be in an un-trusted state if the authentication response is not equal to the expected response.....	34

F.	Claim 7: Method according to claim 1, wherein the terminal comprises a 2G or 3G type radio interface, a Bluetooth radio interface, a WLAN interface, a digital enhanced cordless (DECT) radio interface or an Ethernet data interface.	35
G.	Claim 11	35
1.	11[pre]: A network node for service-based authentication of a terminal to a network, the network node comprising:.....	35
2.	11[a]: a receiver configured to receive an authentication data request;.....	36
3.	11[b]: a first generator configured to determine an expected service code associated with the type of communication channel via which the authentication data request was received by the network; and	36
4.	11[c]: a second generator configured to generate in response to the receipt of an authentication data request a modified expected response, wherein the modification of the expected response depends on the determined expected service code.	37
H.	Claim 12	37
1.	12[pre]: A system for service based authentication to a network, comprising:	37
2.	12[a]: a terminal configured to receive an authentication request from the network, to determine a service code associated with the type of communication channel via which the authentication request was received by the terminal, and to send in response to the authentication request a modified response to the network, wherein the modification depends on the determined service code;.....	37
3.	12[b]: a network node configured to receive an authentication data request and determine an expected service code associated with the type of communication channel via which the authentication data request was received by the network and configured to generate in	

	response to the receipt of the authentication data request a modified expected response wherein the expected response depends on the determined expected service code and configured to compare the modified response with the modified expected response.....	38
I.	Claim 13: A computer program product comprising software code portions configured for, when run in the memory of a terminal, executing the method according to claim 1.	38
X.	GROUND 2: TS-33.402 (With or Without Arkko) In View Of ALDERA RENDER OBVIOUS CLAIMS 2, 8-10, and 13.....	38
A.	Motivation to Combine	39
B.	Claim 8	42
1.	8[pre]: Service interface module for use in a terminal, the service interface module comprising:.....	42
2.	8[a]: a receiver configured to receive an authentication signal from the network via one of the communications interfaces of the terminal;	45
3.	8[b]: a channel identifier configured to identify the communication channel through which the authentication signal was received and provide a service code associated with the identified communication channel;.....	46
4.	8[c]: a channel interface configured to establish a secure communication channel between the module and an identity module of the terminal; and.....	47
5.	8[d]: a modifier configured to modify an authentication response of the identity module on the basis of the service code associated with the identified communication channel.	48
C.	Claim 9: An identity module for establishing a safe communication channel with a service interface module as claimed in claim 8, the identity module comprising: a calculator for calculating a response upon receipt of an authentication	

	request; and a modifier for modifying the response on the basis of a predetermined mathematical function using a service code associated with the identified communication channel.....	49
D.	Claim 10	50
1.	10[pre]: A terminal for accessing network services, the terminal comprising (i) an operating system having memory configured to store program instructions and (ii) a service interface module configured to identify a communication channel through which an authentication request is received, wherein the program instructions are executable by the terminal to:	50
2.	10[a]: receive an authentication request from the network;.....	52
3.	10[b]: determine the communication channel through which the authentication request is received;	52
4.	10[c]: determine a service code associated with the identified communication channel via which the authentication request was received by the terminal; and	52
5.	10[d]: send in response to an authentication request a modified response to the network wherein the modification depends on the determined service code.....	52
E.	Claim 13: A computer program product comprising software code portions configured for, when run in the memory of a terminal, executing the method according to claim 1.	52
F.	Claim 2: Method according to claim 1, wherein the terminal comprises an identity module and a service interface (SI) module configured to securely communicate with the identity module and to identify the communications channel through which the authentication request was received.	52
XI.	GROUND 3: NASLUND RENDERS OBVIOUS CLAIMS 1-7.....	53
A.	Claim 1	53

1.	1[pre]: Method for service-based authentication of a terminal to a network, the terminal comprising one or more communications interfaces for setting-up a communication channel with the network, the method comprising:.....	53
2.	1[a]: the terminal sending a service request for access to a network service;	54
3.	1[b]: the terminal receiving in response to the service request an authentication request from the network;	57
4.	1[c]: the terminal identifying the communication channel through which the authentication request was received;	58
5.	1[d]: the terminal determining a service code associated with the identified communication channel; and	59
6.	1[e]: the terminal sending an authentication response to the network, wherein the authentication response depends on the identified communication channel in that the response is calculated on the basis of the information in the authentication request and the determined service code, thereby securely including information regarding the identified communication channel through which the authentication request was received into the response.....	61
B.	Claim 2: Method according to claim 1, wherein the terminal comprises an identity module and a service interface (SI) module configured to securely communicate with the identity module and to identify the communications channel through which the authentication request was received.....	64
C.	Claim 3	66
1.	3[pre]: Method according to claim 1, wherein the authentication request comprises authentication information[,] the method further comprising the steps of:	66
2.	3[a]: the terminal modifying the authentication information on the basis of the identified	

	communications channel; and the terminal generating the authentication response on the basis of the modified authentication information.	67
D.	Claim 4	68
1.	4[pre]: Method according to claim 1, wherein the authentication request comprises authentication information, the method further comprising:.....	68
2.	4[a]: the terminal generating the authentication response;	69
3.	4[b]: the terminal modifying the authentication response on the basis of the identified communications channel.....	69
E.	Claim 5	70
1.	5[pre]/5[a]: Method according to claim 1, the method further comprising: the terminal sending a service request via a predetermined communications channel to the network;.....	70
2.	5[b]: the network generating an expected service code on the basis of the type of communications channel the service request was sent to the network; and	71
3.	5[c]: determining on the basis of the expected service code an expected response.	72
F.	Claim 6	74
1.	6[pre]/6[a]: Method according to claim 5, the method further comprising: comparing the expected response with the authentication response sent by the terminal to the network; and	74
2.	6[b]: determining the terminal to be in an un-trusted state if the authentication response is not equal to the expected response.....	74
G.	Claim 7: Method according to claim 1, wherein the terminal comprises a 2G or 3G type radio interface, a Bluetooth radio	

	interface, a WLAN interface, a digital enhanced cordless (DECT) radio interface or an Ethernet data interface.	75
H.	Claim 13: A computer program product comprising software code portions configured for, when run in the memory of a terminal, executing the method according to claim 1.	76
XII.	THE BOARD SHOULD NOT EXERCISE ITS DISCRETION TO DENY INSTITUTION	76
A.	<i>Fintiv</i>	76
B.	§314(a)	77
C.	§325(d)	77
XIII.	Conclusion.....	77

EXHIBIT LIST

Ex.	Description
1001	U.S. Patent No. 8,881,235 (“’235 Patent”)
1002	File History for U.S. Patent No. 8,881,235
1003	Declaration of Dr. Kevin Almeroth
1004	<i>Curriculum vitae</i> of Dr. Kevin Almeroth
1005	WIPO Int’l Publication No. WO 2004/032557 (“Naslund”)
1006	3GPP Technical Specification 33.402 Version 8.1.1, “Security aspects of non-3GPP accesses” (published October 14, 2008)
1007	Version History of 3GPP Technical Specification 33.402 (available at https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2297)
1008	J. Arkko, et al., “Improved Extensible Authentication Protocol Method for 3 rd Generation Authentication and Key Agreement (EAP-AKA’),” RFC 5448 Draft version 9 (published October 24, 2008) (available at https://datatracker.ietf.org/doc/html/draft-arkko-eap-aka-kdf-09)
1009	RFC 5448 Drafts Version History (available at https://datatracker.ietf.org/doc/draft-arkko-eap-aka-kdf/history/)
1010	3GPP Technical Specification 33.402 Version 8.2.0, “Security aspects of non-3GPP accesses” (published December 16, 2008)
1011	S3-081498 Change Request to Technical Specification 33.402 (presented November 10-14, 2008) (available at https://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_42/Docs/SP-080739.zip)
1012	Directory Listing /ftp/tsg_sa/TSG_SA/TSGS_42/Docs (available at https://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_42/Docs?sortby=sizerev)

Petition for *Inter Partes* Review
U.S. Patent No. 8,881,235

1013	<i>Ericsson Inc. v. Koninklijke KPN N.V.</i> , IPR2023-00582, Exhibit 1012, Declaration of Craig Bishop
1014	U.S. Pat. No. 8,413,209 (“Aldera”) (prior art under 35 U.S.C. §102(a))
1015	<i>Koninklijke KPN N.V. v. Telefonaktiebolaget LM Ericsson, Ericsson Inc.</i> , No. 2:21-CV-00113-JRG (E.D. Tex. Mar. 16, 2022), Claim Construction Order
1016	RFC 4187, “Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA),” IETF (January 2006)
1017	RFC 4187 History (available at https://datatracker.ietf.org/doc/rfc4187/)

LIST OF CHALLENGED CLAIMS

Claim	Limitation
1[pre]	Method for service-based authentication of a terminal to a network, the terminal comprising one or more communications interfaces for setting-up a communication channel with the network, the method comprising:
1[a]	the terminal sending a service request for access to a network service;
1[b]	the terminal receiving in response to the service request an authentication request from the network;
1[c]	the terminal identifying the communication channel through which the authentication request was received;
1[d]	the terminal determining a service code associated with the identified communication channel; and
1[e]	the terminal sending an authentication response to the network, wherein the authentication response depends on the identified communication channel in that the response is calculated on the basis of the information in the authentication request and the determined service code, thereby securely including information regarding the identified communication channel through which the authentication request was received into the response.
2	Method according to claim 1, wherein the terminal comprises an identity module and a service interface (SI) module configured to securely communicate with the identity module and to identify the communications channel through which the authentication request was received.

Claim	Limitation
3[pre]	Method according to claim 1, wherein the authentication request comprises authentication information the method further comprising the steps of:
3[a]	the terminal modifying the authentication information on the basis of the identified communications channel; and the terminal generating the authentication response on the basis of the modified authentication information.
4[pre]	Method according to claim 1, wherein the authentication request comprises authentication information, the method further comprising:
4[a]	the terminal generating the authentication response;
4[b]	the terminal modifying the authentication response on the basis of the identified communications channel.
5[pre]	Method according to claim 1, the method further comprising:
5[a]	the terminal sending a service request via a predetermined communications channel to the network;
5[b]	the network generating an expected service code on the basis of the type of communications channel the service request was sent to the network; and
5[c]	determining on the basis of the expected service code an expected response.
6[pre]	Method according to claim 5, the method further comprising:

Claim	Limitation
6[a]	comparing the expected response with the authentication response sent by the terminal to the network; and
6[b]	determining the terminal to be in an un-trusted state if the authentication response is not equal to the expected response.
7	Method according to claim 1, wherein the terminal comprises a 2G or 3G type radio interface, a Bluetooth radio interface, a WLAN interface, a digital enhanced cordless (DECT) radio interface or an Ethernet data interface.
8[pre]	Service interface module for use in a terminal, the service interface module comprising:
8[a]	a receiver configured to receive an authentication signal from the network via one of the communications interfaces of the terminal;
8[b]	a channel identifier configured to identify the communication channel through which the authentication signal was received and provide a service code associated with the identified communication channel;
8[c]	a channel interface configured to establish a secure communication channel between the module and an identity module of the terminal; and
8[d]	a modifier configured to modify an authentication response of the identity module on the basis of the service code associated with the identified communication channel.

Claim	Limitation
9	An identity module for establishing a safe communication channel with a service interface module as claimed in claim 8, the identity module comprising: a calculator for calculating a response upon receipt of an authentication request; and a modifier for modifying the response on the basis of a predetermined mathematical function using a service code associated with the identified communication channel.
10[pre]	A terminal for accessing network services, the terminal comprising (i) an operating system having memory configured to store program instructions and (ii) a service interface module configured to identify a communication channel through which an authentication request is received, wherein the program instructions are executable by the terminal to:
10[a]	receive an authentication request from the network;
10[b]	determine the communication channel through which the authentication request is received;
10[c]	determine a service code associated with the identified communication channel via which the authentication request was received by the terminal; and
10[d]	send in response to an authentication request a modified response to the network wherein the modification depends on the determined service code.
11[pre]	A network node for service-based authentication of a terminal to a network, the network node comprising:
11[a]	a receiver configured to receive an authentication data request;

Claim	Limitation
11[b]	a first generator configured to determine an expected service code associated with the type of communication channel via which the authentication data request was received by the network; and
11[c]	a second generator configured to generate in response to the receipt of an authentication data request a modified expected response, wherein the modification of the expected response depends on the determined expected service code.
12[pre]	A system for service based authentication to a network, comprising:
12[a]	a terminal configured to receive an authentication request from the network, to determine a service code associated with the type of communication channel via which the authentication request was received by the terminal, and to send in response to the authentication request a modified response to the network, wherein the modification depends on the determined service code;
12[b]	a network node configured to receive an authentication data request and determine an expected service code associated with the type of communication channel via which the authentication data request was received by the network and configured to generate in response to the receipt of the authentication data request a modified expected response wherein the expected response depends on the determined expected service code and configured to compare the modified response with the modified expected response.

Claim	Limitation
13	A computer program product comprising software code portions configured for, when run in the memory of a terminal, executing the method according to claim 1.

I. INTRODUCTION

The '235 patent is directed to authenticating a user terminal, such as a cell phone, on a cellular network. The '235 patent acknowledges that “authentication and key agreement (AKA)” was (and still is) the authentication mechanism for cellular networks. Yet the '235 patent describes its purported improvement over AKA as “*easily* achieved” and “*only* requir[ing]” one simple thing: that the terminal and network node agree on the identity of the communication channel on which they communicate (which the patent calls a “service code”), and use that service code in the authentication messages. Ex. 1001, 1:63-2:24. The '235 patent admits that the rest of its claimed invention is otherwise disclosed by well-known AKA methodologies.

Yet before the earliest filing date of the '235 patent, the 3GPP group responsible for standardizing the 3rd Generation of cellular technologies had already proposed and published the AKA standard for authenticating devices, the 3GPP Technical Specification 33.402 (“TS-33.402”). These revisions covered the same technology claimed by the '235 patent—specifically the determination of the “access network identity” of the channel on which the authentication request was received, and using it to generate and encrypt the authentication response. TS-33.402 explains that this method allows the user terminal and server to mutually authenticate that they are operating on the correct channel communication.

Indeed, the idea of using a channel's service code (or identifier) to modify an authentication response was well-known. Another reference which was filed by Ericsson ("Naslund") also describes a user terminal using a service code of the communication channel on which an authentication request is received to determine which sub-application to use to generate a response.

For these reasons, the challenged claims of the '235 patent are unpatentable.

II. MANDATORY DISCLOSURES

Pursuant to 37 C.F.R. § 42.8(a)(1), the following mandatory notices are provided as part of this Petition.

A. Standing

Petitioner certifies that it is not barred or estopped from requesting review of the Challenged Claims.

B. Real Party in Interest

The real parties-in-interest are Samsung Electronics America, Inc. and Samsung Electronics Co., Ltd.

C. Related Matters

Petitioner filed a declaratory judgment of non-infringement against the '560 patent in related district court litigation captioned *Samsung Electronics Co. Ltd et al, v. Koninklijke KPN N.V. et al*, 1:24-cv-01433-UNA (D. Del.).

The '560 patent was previously asserted in *Koninklijke KPN N.V. v. Telefonaktiebolaget LM Ericsson, Ericsson Inc.*, No. 2:21-CV-00113-JRG (E.D.

Tex. Mar. 16, 2022), which was dismissed following the parties' settlement. The Court issued a claim construction order that is discussed below.

D. Lead and Back-Up Counsel (37 C.F.R. § 42.8(b)(3)) and Service Information (37 C.F.R. § 42.8(b)(3)-(4))

Petitioner provides the following counsel and service information. Pursuant to 37 C.F.R. § 42.10(b), a Power of Attorney accompanies this Petition. Petitioner agrees to accept electronic service at the email addresses listed below.

LEAD COUNSEL	BACK-UP COUNSEL
James M. Glass (Reg. No. 46729) jimglass@quinnemanuel.com	John T. McKee (Reg. No. 65,926) johnmckee@quinnemanuel.com
QUINN EMANUEL URQUHART & SULLIVAN, LLP 51 Madison Ave, 22nd Floor New York, New York 10010 Tel: (212) 849-7000 Fax: (212) 849-7100	QUINN EMANUEL URQUHART & SULLIVAN, LLP 51 Madison Avenue, 22 nd Floor New York, NY 10010 Tel: (212) 849-7000 Fax: (212) 849-7100
	Quincy Lu (Reg. No. 76,954) quincylu@quinnemanuel.com
	QUINN EMANUEL URQUHART & SULLIVAN, LLP 1109 First Avenue, Suite 210 Seattle, WA 98101 Tel: (206) 905-7000 Fax: (206) 905-7100
	Ron Hagiz (<i>pro hac vice</i> forthcoming) ronhagiz@quinnemanuel.com
	QUINN EMANUEL URQUHART & SULLIVAN, LLP

Petition for *Inter Partes* Review
U.S. Patent No. 8,881,235

	51 Madison Avenue, 22nd Floor New York, NY 10010 Tel: (212) 849-7000 Fax: (212) 849-7100 Landon Smith (Reg. No. 79,248) landonsmith@quinnemanuel.com QUINN EMANUEL URQUHART & SULLIVAN, LLP 300 W 6th St, Suite 2010 Austin, TX 78701 Tel: (737) 667-6100 Fax: (737) 667-6110 Leon Lin (<i>pro hac vice</i> forthcoming) leonlin@quinnemanuel.com QUINN EMANUEL URQUHART & SULLIVAN, LLP 1200 Abernathy Road NE Building 600, Suite 1500 Atlanta, GA 30328 Tel: (404) 482-3502 Fax: (404) 681-8290
--	---

E. Payment of Fees (37 C.F.R. § 42.15(a))

The undersigned authorizes the Office to charge the fee required for this Petition for Inter Partes Review to Deposit Account No. 50-5708. Any additional fees that might be due are also authorized.

III. GROUNDS

Petitioner requests cancellation of claims 1–13 on the following grounds:

Ground	Reference(s)	Basis	Claims
--------	--------------	-------	--------

1	TS-33.402 alone, or in view of Arkko	§103	1, 3-7, 11-13
2	TS-33.402 (with or without Arkko), Aldera	§103	2, 8-10, 13
3	Naslund	§103	1-7, 13

Ground 1 relies on TS-33.402, a draft of what eventually became a 3GPP standard for mobile devices to connect to non-3GPP access networks. It describes a mobile device that uses EAP-AKA to send and receive authentication requests to a server, wherein both use the same ***network access identity*** that identifies the communication channel being used to exchange EAP-AKA messages. The network access identity is used to generate matching encryption keys and matching response values on both ends to authenticate the device. Arkko provides additional teachings regarding the network access identity and was incorporated into the TS-33.402 standard. EX1003, ¶94.

Ground 2 further relies on Aldera, which teaches authentication using the claimed service interface module and identity module.

Ground 3 relies on Naslund, which describes a mobile device receiving authentication requests and processing the request based on the communication channel on which it is received. The processing is performed by a specific sub-application for the channel, which is identified using a code. EX1003, ¶186.

IV. LEVEL OF ORDINARY SKILL IN THE ART

A person of ordinary skill in the art (“POSITA”) as of December 15, 2009 would have had an undergraduate degree in computer science, computer engineering, electrical engineering, physics, or a related field, with at least two years of experience working with cellular telecommunications, radio-access network architectures, or cellular network security and management. EX1003, ¶47. Less work experience may be compensated by a higher level of education or vice versa. *Id.* Petitioners’ expert exceeded this definition by the priority date. *Id.*

V. TECHNOLOGY OVERVIEW (EX1003, ¶¶48-53)

Telecommunication networks enable the connection of user terminals, *e.g.*, mobile phones, personal computers, handheld devices, etc.

One important issue relating to mobile telecommunications is security: avoiding the interception of communications between the terminal and the network; ensuring that the network that a terminal connects to is the one intended by the user; and preventing malicious actors from accessing and transmitting malware to a terminal by falsely mimicking a network. A variety of tools are used to help maintain the integrity of the connection between a terminal and a network.

One method of establishing a secure communication channel between a terminal and a network is the Authentication and Key Agreement (“AKA”) protocol. The “Authentication” component of the AKA protocol ensures that the terminal

attempting to connect to a network is legitimate and that its identity can be verified by the network. The “Key Agreement” component of the AKA protocol ensures that the same key (*i.e.*, a series of letters and/or numbers used by a cryptographic algorithm to encode and decode data) is used by both the terminal and the network to facilitate secure communication between the two, thereby ensuring confidentiality.

The AKA protocol essentially involves the transmission of data between the terminal and the network, and the use of cryptographic tools to encode, decode, and compare the data that is exchanged in order to carry out the necessary authentication and encryption. The terminal begins the process by transmitting a service request to the network. The network’s mobile switching center (“MSC”) receives the service request and transmits an authentication request to the Authentication Center (“AuC”). In response to the authentication request, the AuC generates a random number *RAND* and sends it to the MSC, which it in turn forwards the *RAND* to the terminal’s identity module. The terminal uses the stored cryptographic key to carry out the mathematical calculations required by the specific AKA protocol that is being applied to the connection. The terminal calculates a response *RES* which is transmitted by the terminal back to the network’s MSC. Meanwhile, the AuC—which stores the same cryptographic key used by the terminal—generates an expected response *XRES* using both the same key and *RAND* that was processed by

the identity module. Having received *XRES* from the AuC, the MSC—which now possesses both *RES* and *XRES*—compares the two values and subsequently authenticates the terminal if the two values match.

VI. THE '235 PATENT

A. Overview

U.S. Pat. No. 8,881,235 is directed to “service-based authentication” of a user terminal wherein the user terminal has a number of “communications interfaces,” and determines which interface was used for receiving an authentication request. The user terminal generates an authentication response and uses the service code of the identified communication interface to generate the authentication response. EX1003, ¶¶54-58.

B. Prosecution History

The '235 Patent was filed on December 15, 2009. As initially drafted, independent claim 1 did not recite the determination of a service code or calculating the response on the basis of the service code. EX1002, 295. Instead, such limitations were recited in claim 2. However, the determination of a service code was found in the other independent claims as initially drafted.

The examiner’s first rejection relied on Naslund as anticipating claim 1. EX1002, 119. The examiner also relied on the combination of Naslund and a 3GPP paper published by Ericsson as rendering obvious claims 2 and the other independent claims directed to determining a service code. *Id.*, 122-123. In particular, the

examiner mapped Ericsson's disclosure of a "service identifier Sid" as the recited service code. *Id.*

In response, applicant did not contest that Naslund anticipated then-pending claim 1. Instead, applicant amended claim 1 by incorporating the limitations of claim 2 and argued that, in Ericsson, "there is little explanation given about what is meant by this service identifier and no explanation that suggests it corresponds to a service code." *Id.*, 91, 99. Applicant also noted that there was no "disclosure that the service Sid is associated with a communication channel through which a authentication request has been received." *Id.*

The examiner again rejected the claims. In the examiner's second rejection, the examiner concluded that the amended claim 1 was obvious in view of Naslund and U.S. Pat. Pub. No. 2006/0148483 ("Howard"). In particular, the examiner argues that Howard discloses "receiving an authentication response signal in the channel, the contents of which depend on the context [service code] of the authentication request signal." EX1002, 62.

In response, the applicant argued that Howard lacked "an explanation of what is meant by 'context,'" since the word "context" only appeared in the Abstract and nowhere else. EX1002, 48. Instead, applicant noted that Howard describes the authentication response "depends on the random number included in the authentication request signal" and speculated that "the term 'context' as written in

the abstract might actually be a typographic error, and should in fact be written as ‘content’.” *Id.*, 49. Regardless, the applicant argued that Howard does not disclose that the context is a “service code,” since “the service code described in the claim is associated with an identified communication channel and is a determinable code actually identifiable within the terminal,” whereas “there is no such determinable code disclosed in Howard.” *Id.*

Following these arguments, the examiner issued a Notice of Allowance, stating that “[n]o reason for allowance is needed as the record is clear in light of applicant’s arguments and amendment.” *Id.*, 15-16. In other words, the examiner agreed with the applicant that the prior art did not disclose a service code.

However, as discussed below, the examiner was incorrect that Naslund does not disclose a service code. EX1003, ¶¶59-66. Naslund does, in fact, disclose a code associated with a sub application that is particular to a communication code. In addition, TS-33.402 discloses a “access network identity” which is the name of a particular communication channel.

VII. CLAIM CONSTRUCTION

Except as discussed below, Petitioners have applied the plain and ordinary meaning understood by a POSITA at the time of the alleged invention, in the context of the ’235 Patent and its prosecution history. *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005); EX1003, ¶¶67-69.

A. “service code” / “expected service code”

In *Koninklijke KPN N.V. v. Telefonaktiebolaget LM Ericsson, Ericsson Inc.*, No. 2:21-CV-00113-JRG (E.D. Tex. Mar. 16, 2022) (“EDTX Action”), the Court concluded that a “service code” is a coined term and therefore “cannot be construed broader than the disclosure in the specification.” EX1015, 63 (quoting *Indacon, Inc. v. Facebook, Inc.*, 824 F.3d 1352, 1357 (Fed. Cir. 2016)).

In view of the specification, the Court construed a “service code” as a “code that identifies a communication channel” and an “expected service code” as “expected code that identifies a communication channel.” EX1015, 64. Petitioners submit that these terms need not be construed because they are disclosed or rendered obvious by the prior art under any reasonable interpretation, including as construed by the Court. EX1003, ¶¶70-71.

B. “communication channel”

In the EDTX Action, the Court did not expressly construe this term but instead concluded it would have its plain meaning. EX1015, 67. The Court rejected Defendants’ proposed construction of “a channel extending between a terminal and an access node” and agreed with Plaintiff that a “communication channel” includes a channel between two terminals. *Id.*, 66. Petitioners submit that this term need not be construed because it is disclosed or rendered obvious by the prior art under any reasonable interpretation. EX1003, ¶72.

C. “authentication data request”

In the EDTX Action, the Court did not expressly construe this term but instead concluded it should have its plain meaning. EX1015, 71. The Court rejected Defendants’ argument that the limitation should be either rewritten as a “service request” or held to be indefinite. The Court rejected Defendants’ argument as an implicit argument that the term lacks written description support, which was premature at the claim construction stage, and found that the claim could be readily understood. Petitioners submit that this term need not be construed because it is disclosed or rendered obvious by the prior art under any reasonable interpretation. EX1003, ¶73.

D. “service interface module”

The term “service interface module”¹ is not a means-plus-function term and should be given its plain meaning. The term is recited in claims 2, 8, and 10. For claim 8, the term lacks a recited function and comprises several structural elements. EX1001, cl. 8 (“[T]he service interface module comprising: a receiver ..., a channel identifier ..., a channel interface ..., a modifier”); EX1003, ¶¶74-77. By contrast, both claims 2 and 10 recite that the “service interface module” is “configured to”

¹ This term was not at issue in the EDTX Action because it is only recited in claims that were not asserted.

“identify the communications channel through which the authentication request was received.” Claim 2 further recites that it is “configured to securely communicate with the identity module.”

However, a fundamental canon of construction is that “[b]ecause claim terms are normally *used consistently throughout the patent*, the usage of a term in one claim *can often illuminate* the meaning of the same term in other claims.” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1314 (Fed. Cir. 2005). Departure from this principle requires something “clear from the specification and prosecution history that the terms have different meanings at different portions of the claim.” *Paragon Solutions, LLC v. Timex Corp.*, 566 F.3d 1075, 1087 (Fed. Cir. 2009). Nothing in the intrinsic record indicates that “service interface module” has different meanings in different claims. EX1003, ¶78. Indeed, claim 8 recites that its “service interface module” has “a channel identifier configured to identify the communication channel through which an authentication request was received,” which is identical language to the recited function of the “service interface module” of claims 2 and 10. *Id.*

Accordingly, because the term “service interface module” in claim 8 lacks a recited function but recites sufficient structure, the term does not invoke §112(6) even as recited in claims 2 and 10 because there is no reason to interpret the claims differently. It should be given its plain meaning. EX1003, ¶78.

Alternatively, if “service interface module” invokes §112(6), its recited function is “to identify the communications channel through which the authentication request was received” and the corresponding structure is 5:56-6:7, 7:45-54, or their equivalents. EX1003, ¶79.

E. “identity module”

The claimed “identity module”² either lacks a recited function or has sufficient structure, and thus is not a means-plus-function term. EX1003, ¶¶80-82. As an initial matter, a POSITA would have understood that an “identity module” has a well-known structure inclusive of a Subscriber Identity Module (SIM) device typically found on mobile devices. EX1003, ¶81; see EX1001, 6:32-39 (“The identity module 120 ... may comprise a Subscriber Identity Module (SIM)”). Thus, the term on its own connotes sufficient structure. *MTD Products v. Iancu*, 933 F.3d 1336, 1341 (Fed. Cir. 2019) (“[A] critical question is whether the claim term is used in common parlance or by persons of skill in the pertinent art to designate structure, including either a particular structure or a class of structures.”). Moreover, the term’s appearance in claims 2 and 8 lack any recited function. And while claim 9 recites a function of “establishing a safe communication channel with a service

² This term was not at issue in the EDTX Action because it is only recited in claims that were not asserted.

interface module,” it also recites sufficient structure, such as comprising “a calculator” and a “modifier.”

VIII. OVERVIEW OF THE PRIOR ART

A. TS-33.402 (EX1006)

3GPP Technical Specification 33.402 version 8.1.1 (“TS-33.402”) is directed to “security aspects of non-3GPP accesses.” EX1003, ¶83. In particular, it describes how a 3GPP terminal can authenticate itself with a non-3GPP network using a protocol called EAP-AKA. Several steps are described. The most pertinent is that, following a request for access to the network from the user terminal, the network transmits to the user terminal a EAP Request/AKA Identity message. In particular, the EAP Request message is transformed using CK’ and IK’ keys which are generated from an “access network identity,” the identifier of the access network used for communication. Along with the EAP Request message is a message authentication code, or MAC.

Upon receipt of the EAP Request, the UE (user equipment) generates an EAP Response. Generating the response involves the UE generating the “access network identity and deriving the CK’ and IK’ keys in order to check the received MAC and generate a response MAC. EX1003, ¶84.

1. TS-33.402 Qualifies as Prior Art

TS-33.402 was published by at least October 2008 and therefore qualifies as prior art under pre-AIA 35 U.S.C. §102(a). EX1003, ¶85. TS-33.402 is a Technical

Specification published by the 3rd Generation Partnership Project, *i.e.* 3GPP. As explained by Craig Bishop, who worked as a Rapporteur³ for 3GPP from 1998 to 2003, and confirmed by Dr. Almeroth, 3GPP is a well-known standards organization tasked with developing protocols for mobile telecommunications. EX1013. A POSITA would have been well-aware of their documents and publication practices. EX1003, ¶85.

As Mr. Bishop explains it, 3GPP technical specifications, which would include TS-33.402, are publicly accessible with reasonable diligence as of the date they were uploaded to 3GPP's FTP server. EX1013; EX1003, ¶86. Indeed, at least one PTAB panel has found that this is true of all 3GPP documents. *Samsung Electronics Co., Ltd. v. Huawei Technologies Co., Ltd.*, IPR2017-01487, Paper 45 (Dec. 10, 2018) (“[A]ll 3GPP documents[] were generated with intent to distribute them to interested members of the telecommunications industry. They were uploaded to 3GPP's FTP server without restriction or expectation of confidentiality, and were indefinitely maintained there. They have been available for downloading (copying) from the FTP server since being uploaded, and can be shared with others without restriction. Under such circumstances, the documents are publicly accessible.”).

³ A Rapporteur is the “prime contact point on technical matters and for information on progress throughout the drafting phases.” https://www.3gpp.org/ftp/Information/Working_Procedures/3GPP_WP.htm

TS-33.402 was uploaded to 3GPP's file server on October 14, 2008. EX1007. As a result, TS-33.402 became a "printed publication" on that date, and Exhibit 1006 is a true and correct copy of that publication. EX1003, ¶87.

2. Arkko (EX1008) Qualifies as Prior Art

Arkko is the October 24, 2008 draft of what would eventually become RFC 5448, which proposes an update to the EAP-AKA authentication method called EAP-AKA'. EX1003, ¶¶88-89. As discussed in fuller detail below, Arkko provides additional implementation details regarding TS-33.402's use of an "access network identity" as part of its authentication scheme.

Arkko was published on October 24, 2008 and therefore qualifies as prior art. Arkko is a document published by the Internet Engineering Task Force ("IETF") and is available on the IETF's website. EX1003, ¶89. According to Dr. Almeroth, who has had significant involvement with the IETF, the IETF is a well-known standards organization that publishes thousands of standards for protocols used on the Internet, including the protocols that make up the backbone of the Internet, such as TCP and IP. EX1003, ¶90. As a result, a POSITA would have been well aware of their publication practices.

By 2008, the IETF regularly published drafts of RFC's on its website as soon as they were distributed to the relevant IETF group. EX1003, ¶91. RFC drafts were generally drafted by a working group (in Arkko's case, the Network Working

Group), and then disseminated to the public via the IETF website and an email announcement with a link to the newly-published document. *Id.* As a result, the publication date on the face of Arkko and as found on the IETF's website is a reliable indicia of its publication status as well as its authenticity on the date it was published. *Id.* Moreover, the IETF's version history for RFC 5448 available on the IETF website confirms that Arkko was automatically uploaded to the IETF's website on October 24, 2008. EX1009, 2. Thus, Dr. Almeroth concludes that a POSITA would have been able to locate Arkko with reasonable diligence by that time and that Exhibit 1009 is a true and correct copy of Arkko when it was first published. EX1003, ¶¶91-92.

B. Naslund (EX1005)

WO 2004/032557A1 ("Naslund") was published on April 15, 2004 and therefore qualifies as prior art under pre-AIA 35 U.S.C. §102(b). EX1003, ¶93. Naslund provides a modification to the well-known AKA methodology for authenticating a user terminal. In particular, Naslund describes that the server transmits an AKA authentication request, and that the user terminal generates an authentication response. Naslund further teaches that the response is generated by one of a number of "security enhancing applications ... for encapsulating AKA responses in a more secure algorithm." In particular, Naslund describes determining which channel the request came from and then selecting a sub application assigned

to that channel to generate the response. Naslund teaches that “it may be advantageous to customize the security processing by providing a number of different sub applications and selecting among the sub applications ***depending*** on the ***particular*** type of [communication] ***interface*** used by the terminal.” EX1005, 20:1-7. By doing this, “the mobile itself is capable of detecting when a request for SIM access comes over less secure interfaces, and taking appropriate actions accordingly.” *Id.*, 19:25-27.

IX. GROUND 1: TS-33.402 ALONE OR IN VIEW OF ARKKO RENDERS OBVIOUS CLAIMS 1, 3-7, AND 11-13

A. Claim 1

1. **1[pre]: Method for service-based authentication of a terminal to a network, the terminal comprising one or more communications interfaces for setting-up a communication channel with the network, the method comprising:**

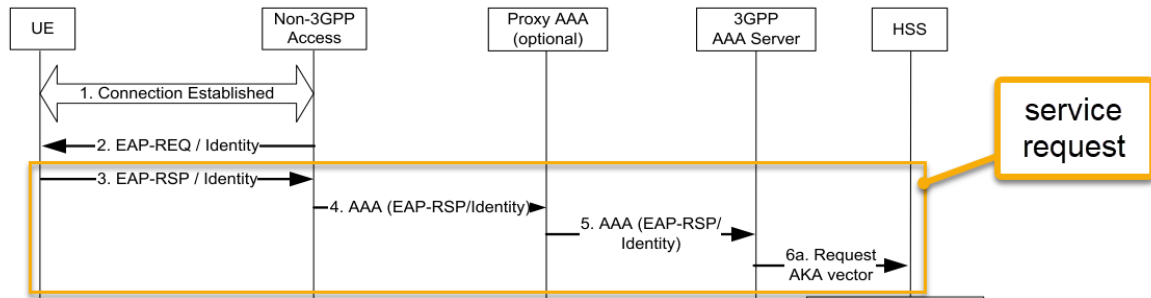
“Method for service-based authentication of a terminal to a network”: To the extent this preamble is limiting, TS-33.402 discloses a method for service-based authentication of a UE, *i.e.* ***terminal***, to a network. EX1006, 10 (“Access ***authentication*** for non-3GPP access in EPS shall be based on EAP-AKA”). The authentication is ***service-based*** because, as discussed below, it depends on properly identifying the communication channel of the authentication communications. EX1003, ¶¶95-96.

“terminal comprising one or more communications interfaces for setting-up a communication channel with the network”: TS-33.402 discloses a terminal

capable of supporting 3GPP and non-3GPP access technologies for setting-up a communication channel with a network. EX1006, 10 (“If the terminal supports 3GPP access capabilities, the credentials ... shall reside on the UICC.”); *id.* (“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.”). TS-33.402 therefore discloses a terminal with at least one communication interface for setting-up a communication channel with a 3GPP network, and a communication interface for accessing each of the non-3GPP networks. EX1003, ¶¶97.

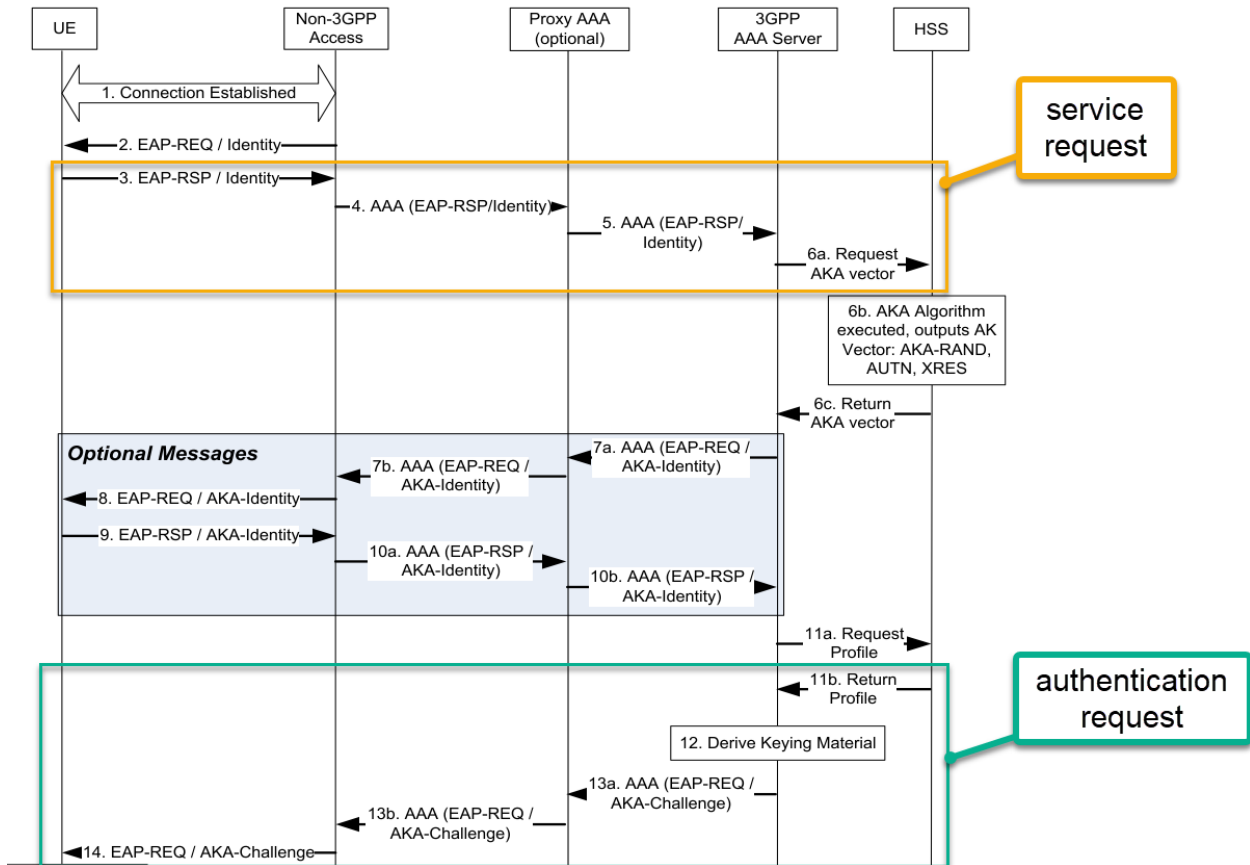
2. 1[a]: the terminal sending a service request for access to a network service;

TS-33.402 discloses a “UE [*i.e.*, ***terminal***] send[ing] an EAP Response/Identity message [*i.e.*, ***service request***].” EX1006, 13. This request “is routed towards the proper 3GPP AAA Server” reflecting “[the UE’s] identity” which, “in the case of first authentication, [is the UE’s] IMSI” and a message “indicat[ing] EAP-AKA.” EX1006, 13. Figure 6.2-1 illustrates the steps comprising a service request sent from the terminal to the network. EX1006, Fig. 6.2-1; EX1003, ¶¶98-99.



3. 1[b]: the terminal receiving in response to the service request an authentication request from the network;

TS-33.402 discloses the 3GPP AA Server sends an EAP Request/AKA-Challenge message (*i.e.* **authentication request**) to the UE (*i.e.* **terminal**). Specifically, a “3GPP AAA Server sends” a “EAP Request/AKA_Challenge message” to the terminal via an authenticator, with that message containing “RAND, AUTN, a message authentication code (MAC).” EX1006, 15. Figure 6.2-1 illustrates the steps comprising an authentication request sent by the network to the terminal in response to a service request. EX1006, Fig. 6.2-1; EX1003, ¶¶100-01.



4. 1[c]: the terminal identifying the communication channel through which the authentication request was received;

TS-33.402 teaches that after receiving the EAP Request/AKA-Challenge message (*i.e.*, **authentication request**), the UE obtains the “access network identity,” *i.e.* **identifies the communication channel through which the authentication request was received**. TS-33.402 explains that the “access network identity” is “the identity of the access network in which the authenticator [*i.e.* server] resides” and is “defined separately for each access network type.” *Id.*, 13. In other words, the “access network identity” **identifies** the particular network that it received the

authentication request, and therefore ***identifies the communication channel*** for that particular network. EX1003, ¶¶102-03.

In addition, a POSITA would have understood that the October 24, 2008 draft of RFC 5448 (“Arkko”) provides further detail regarding the “access network identity” used in the EAP-AKA method described in TS-33.402. EX1003, ¶104. Arkko explains that the access network identity is a “network name” “constructed as specified in [3GPP.24.302] for ‘Access Network Identity.’” EX1008, 7. And as with the “access network identity” described in TS-33.402, Arkko explains that the “[s]erver determines the network name and ensures the given access network is authorized to use the claimed name,” which is then sent to the terminal as part of the EAP-AKA authentication method. *Id.*, 5. Arkko then explains that the terminal “determines what the network name should be, based on e.g., what access technology it is using” and compares that network name with the one received by the server “for discrepancies.” *Id.*; EX1003, ¶105.

Arkko explains that the “network name” is the name “of the access network for which the authentication is being performed.” *Id.*, 6. With respect to the terminal’s determination of the “network name,” Arkko notes that it “is constructed based on local observations” such as the terminal “know[ing] which access technology it is using on the link,” *i.e.* the network name ***identifies the communication channel on which it receives the authentication request***. *Id.*, 7.

Arkko further notes that the “network name consists of the name of the access technology” and optionally “some operator identified that was advertised in a link layer beacon.” *Id.*; EX1003, ¶106.

A POSITA would have considered the “access network identity” described in TS-33.402 to be the same as that described in Arkko. EX1003, ¶107. Indeed, Arkko incorporates TS-33.402 by reference, noting that Arkko defines “EAP-AKA” which has “a new key derivation function specified in [3GPP.33.402].” *Id.*, 3; *see also id.*, 20 (defining “[3GPP.33.402]” as “3GPP Draft Technical Specification 33.402 v 8.0.0, June 2008”).

Moreover, a POSITA would have considered it obvious combine TS-33.402 with Arkko’s teachings with respect to the “network name.” EX1003, ¶108. Indeed, that combination is precisely what the 3GPP group did in the next revision (version 8.2.0) of TS-33.402 as published on December 16, 2008, a single day after the earliest filing date of the ’235 patent. EX1010; EX1007. Specifically, in the December 16, 2008 revision, TS-33.402 states that it would incorporate “EAP-AKA’ as defined” in Arkko. EX1010, 14; *see id.*, 7 (noting that reference [23] is “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.”). Such revisions were contemplated in the October 2008 version of TS-33.402 (version 8.1.1), where it states “[t]here is

ongoing work at the IETF regarding the transport of the access network identity in EAP-AKA.” EX1006, 15.

Moreover, the version 8.2.0 revisions of TS-33.402 incorporating Arkko were distributed to the group and considered at the November 10-14, 2008 3GPP SA3 Working Group meeting in Kyoto, Japan. EX1011 (“Alignment of draft-arkko-eap-aka-kdf which defines EAP-AKA”); EX1012 (showing that the Change Request was uploaded to 3GPP’s site on December 4, 2008). Thus, prior to the ’235 patent, ordinary artisans of the 3GPP working group did in fact consider it obvious to combine TS-33.402 with Arkko. EX1003, ¶109.

In addition, a POSITA would have been motivated to combine TS-33.402 and Arkko because of the well-known benefits of incorporating the “network name” in the EAP-AKA authentication request. EX1003, ¶110. Arkko notes that the network name is used to derive encryption keys which “limits the effects of compromised access network nodes and keys,” *i.e.* the well-known benefit of reducing the effectiveness of attacks on the network. EX1008, 3. A POSITA would have further been motivated to have the terminal determine the “network name” because, as taught in Arkko, the name can be checked against the name derived by the server for any “discrepancies,” upon which “authentication is aborted.” EX1008, 5. Because the encryption keys are derived using the network name, a POSITA would be motivated to include this mechanism to ensure the network name is correct and

authentic in order to increase the security of the system. EX1003, ¶110. A POSITA would have had a reasonable expectation of success in this combination because Arkko provides sufficient detail in implementing the determination of the “network name,” and indeed, as discussed in Arkko itself, the format of the “network name” had been standardized in 3GPP TS 24.302, which provides “the normative specification for the construction” of the network name. *Id.*; EX1008, 7; *id.*, 20 (noting that “[3GPP.24.302]” is “3GPP Draft Technical Specification 24.302 v 1.0.0, September 2008”).

5. **1[d]: the terminal determining a service code associated with the identified communication channel; and**

As discussed above in limitation 1[c], TS-33.402 discloses a terminal that determines an access network identity, *i.e.* **service code**. The access network identity is a **service code** because it is an identifier that corresponds to the communication channel through which an authentication request was received by the terminal. EX1003, ¶¶111-12. The access network identity also **identifies the communication channel**, since it is the specific identifier for that particular access network. EX1006, 13. Further, as explained in Arkko, the access network identity “consists of the name of the access technology” and optionally “some operator identified that was advertised in a link layer beacon.” EX1008, 7. Arkko also explains that the access network identity is “a multiple of 4 bytes,” which a POSITA would

understand to mean is encoded into binary and is therefore a **code**. *Id.*, 6; EX1003, ¶112.

6. **1[e]: the terminal sending an authentication response to the network, wherein the authentication response depends on the identified communication channel in that the response is calculated on the basis of the information in the authentication request and the determined service code, thereby securely including information regarding the identified communication channel through which the authentication request was received into the response.**

“the terminal sending an authentication response to the network”: TS-33.402 discloses that, after having received the authentication request, the “UE [*i.e.*, **terminal**] sends [an] EAP Response/AKA-Challenge [*i.e.*, **authentication response**]” to the “3GPP AAA Server” via the “authenticator in the access network.” EX1006, 15; EX1003, ¶¶113-14.

“wherein the authentication response depends on the identified communication channel in that the response is calculated on the basis of the information in the authentication request and the determined service code”: TS-33.402 teaches that the EAP Response/AKA-Challenge (*i.e.* **authentication response**) is calculated using the request’s AUTN and MAC values (*i.e.* **information in the authentication request**) as well as the access network identity (*i.e.* **service code of the identified communication channel**). EX1003, ¶115.

In particular, the response includes a “new MAC” which is generated using “new keying material,” specifically the keys CK’ and IK’, which are computed using

the “access network identity,” *i.e.* **service code**. EX1006, 16 (“(CK’, IK’) = F(CK, IK, <**access network identity**>)”), (“The access network identity ... is input to key derivation to obtain CK’, IK’).

In addition, the response is generated using the request’s AUTN and MAC values, *i.e.* **on the basis of information in the authentication request**. For AUTN, the response (“RES”) is not generated unless “AUTN is correct.” EX1006, 15. And following the computing CK’ and IK’, a “key MSK” is computed to “check[] the received MAC with the new derived keying material.” *Id.* The UE then “calculates a new MAC value covering the EAP [response] message with the new keying material.” *Id.* Accordingly, the authentication response, comprising both the new MAC value and the RES value, is calculated on the basis of the information in the authentication request and the determined service code. EX1003, ¶¶116-17.

“thereby securely including information regarding the identified communication channel through which the authentication request was received into the response”: As discussed above, the calculation performed by the terminal, (CK’, IK’) = F(CK, IK, <access network identity>, is used to generate an authentication response. CK’ and IK’ are encryption keys, as the function F “is a key derivation function” that is able to generate secure cryptographic values. EX1006, 13. TS-33.402 further explains that “new keying material” is derived “from the new computed CK’, IK’” which is then used to “calculate[] a new MAC

value covering the EAP message,” *i.e.* ***the authentication response***. EX1006, 14.

Thus, because the response can only be authenticated if both the terminal and server use the same access network identity. EX1003, ¶118. In other words, the response itself will inform the server whether or not the terminal properly identified the correct communication channel—if it did, then the response indicates a proper authentication. *Id.* Thus, the response ***includes information regarding the identified communication channel***.

B. Claim 3

1. **3[pre]: Method according to claim 1, wherein the authentication request comprises authentication information[,] the method further comprising the steps of:**

TS-33.402 discloses that the authentication request includes “a message authentication code (MAC),” and thus the authentication request is ***authentication information***. EX1006, 15; EX1003, ¶119.

2. **3[a]: the terminal modifying the authentication information on the basis of the identified communications channel; and the terminal generating the authentication response on the basis of the modified authentication information.**

As discussed in limitation 1[c] and 1[d], TS-33.402 discloses that the encryption keys CK’ and IK’ are derived from the access network identity, *i.e.* ***identified communications channel***. TS-33.402 further discloses that the CK’ and IK’ are used to derive “new keying material, including the key MSK” which is in turn used to “check[] the received MAC.” EX1006, 15. A POSITA would

understand that the MAC is a keyed hash of the authentication request. EX1008, 12 (“The MAC algorithm is HMAC-SHA-256-128, a keyed hash value.”). Thus, checking the MAC involves the terminal using the MAC algorithm (specifically HMAC-SHA-256-128) and the new keying material to **modify** the authentication request, *i.e.* **authentication information**, to generate the keyed hash in order to match its value with the received MAC. EX1003, ¶¶120-21.

TS-33.402 discloses that “check[ing] the received MAC” includes sending an authentication response **only if** the received MAC is confirmed to be correct, *i.e.* **generating the authentication response on the basis of the modified authentication information**. As Dr. Almeroth explains, the purpose of the MAC, a “message authentication code” and the fact that it is a keyed hash, is to allow the recipient (*i.e.* the terminal) to ensure the message is authentic and not altered. EX1003, ¶122. Thus, the keyed hash calculated by the terminal will only match the received MAC if the message was not altered. *Id.* TS-33.402 further explains that if the MAC check fails, the “EAP AKA process will be terminated.” Ex. 1006, 16; *see also* EX1008, 14 (explaining that if the MAC is incorrect, the terminal “fails the authentication”). In other words, no response will be transmitted.

C. Claim 4

1. **4[pre]: Method according to claim 1, wherein the authentication request comprises authentication information, the method further comprising:**

As discussed above for claim 3, TS-33.402 discloses an authentication request comprising authentication information. EX1003, ¶123.

2. **4[a]: the terminal generating the authentication response;**

As discussed above for limitation 1[e], TS-33.402 discloses a terminal generating the authentication response, EAP Response/AKA-Challenge. EX1003, ¶124.

3. **4[b]: the terminal modifying the authentication response on the basis of the identified communications channel.**

TS-33.402 discloses modifying the authentication response by generating a MAC value. EX1003, ¶125. TS-33.402 discloses that the terminal “calculates a new MAC value covering the EAP message [*i.e. authentication response*] with the new keying material.” EX1006, 15. As discussed in limitation 3[a], a POSITA would understand that generating a MAC value involves using a keyed hash algorithm and a key on the response to transform it into a keyed hash, *i.e. modify the authentication response*. EX1003, ¶125. TS-33.402 further discloses that the “new keying material” is derived from CK’ and IK’, which is itself derived from the “access network identity,” *i.e. the identified communications channel*. EX1006,

15. Thus, the keyed hash, *i.e. modification of the authentication response*, is performed on the *basis of the identified communications channel*.

D. Claim 5

1. **5[pre]/5[a]: Method according to claim 1, the method further comprising: the terminal sending a service request via a predetermined communications channel to the network;**

As discussed above for limitation 1[a], TS-33.402 discloses a terminal sending a service request to the network over a communications channel. TS-33.402 teaches that, prior to the request, the UE and access network (*i.e. communications channel to the network*) establish a connection “using a procedure specific to the non-3GPP access network.” EX1006, 13. The request is also transported “using a protocol specific to this access network.” *Id.* Thus, a POSITA would understand that the UE must format its request using the specific protocol of the *communications channel to the network*. EX1003, ¶¶126-27. Accordingly, the UE has *predetermined* the communications channel over which the service request will be transported.

2. **5[b]: the network generating an expected service code on the basis of the type of communications channel the service request was sent to the network; and**

5[c]: determining on the basis of the expected service code an expected response.

TS-33.402 discloses that the network server calculates an authentication vector containing XRES (*i.e. expected response*) using the expected access network

identity (*i.e.* ***expected service code***), which is the identity of the ***communications channel the service request was sent to the network***. EX1003, ¶¶128-29.

TS-33.402 discloses that the network server “generates an authentication vector,” which is then “transform[ed] ... into a new authentication vector” using the access network identity, *i.e.* ***expected service code***. EX1006, 13 (“The HSS then transforms this authentication vector into a new authentication vector by computing $(CK', IK') = F(CK, IK, <access\ network\ identity>)$ ”), *id.* (the new authentication vector is “treat[ed] ... like any other authentication vector”). In other words, the network server uses the “access network identity” to generate the keys CK' and IK', which are then used to generate the “new authentication vector.” *Id.*; EX1003, ¶130.

The server’s “access network identity” is an ***expected service code*** because it is used to generate new keying material CK' and IK' on both the server and the UE. EX1006, 15 (“The UE then computes $(CK', IK') = F(CK, IK, <access\ network\ identity>$ in ***the same way as the HSS***.”). Thus, the access network identity on the server must match the access network identity used by the client. EX1003, ¶131. If there is a mismatch, then the new keying material will not match and authentication fails. *Id.*

TS-33.402 teaches that the authentication vector contains “XRES.” EX1006, 32; *see also* EX1016, 4 (“The authentication vector contains ... an ***expected result***

part XRES”).⁴ The XRES value is used by the server to check the “received RES” sent in the UE’s authentication response. EX1006, 15; 12 (“Verifies that AT-RES = XRES”); EX1003, ¶132. Thus, the authentication vector is *an expected response*, and it is determined on the basis of the *expected service code*.

E. Claim 6

1. **6[pre]/6[a]: Method according to claim 5, the method further comprising: comparing the expected response with the authentication response sent by the terminal to the network; and**

As discussed above for limitations 5[b] and 5[c], TS-33.402 discloses a network server that compares an expected authentication message to the authentication response sent by the terminal. EX1006, 13 (“Verifies that AT-RES = XRES”); EX1003, ¶134.

2. **6[b]: determining the terminal to be in an un-trusted state if the authentication response is not equal to the expected response.**

TS-33.402 teaches that a failed comparison between the expected authentication response and the received authentication response results in a failed authentication (*i.e.*, the terminal is in *an un-trusted state*). EX1006, 15 (“The 3GPP AAA Server [*i.e.*, network] *checks* the received MAC and compares XRES to the

⁴ Exhibit 1016 describes EAP-AKA and was publicly available by the IETF on January 2006. EX1017; EX1003, ¶133.

received RES. ... ***If all checks ... are successful***, the 3GPP AAA Server shall send the message EAP Request/AKA-Notification ... The authenticator in the access network informs the UE about the successful authentication”). TS-33.402 teaches that if the check fails, “EAP AKA process will be terminated,” leaving the UE in an ***un-trusted state*** where it cannot perform any functions that require authentication. EX1003, ¶¶135-36.

F. Claim 7: Method according to claim 1, wherein the terminal comprises a 2G or 3G type radio interface, a Bluetooth radio interface, a WLAN interface, a digital enhanced cordless (DECT) radio interface or an Ethernet data interface.

TS-33.402 is directed to a terminal comprising a 3G type radio interface. In particular, TS-33.402 is a standard promulgated by the standards body ***3rd Generation Partnership Project***, which standardized ***3G cellular technology***. EX1003, ¶¶137-38. TS-33.402 is also specifically directed to “E-UTRAN and CDMA2000,” which are 3G technologies. EX1006, 1; EX1003, ¶138.

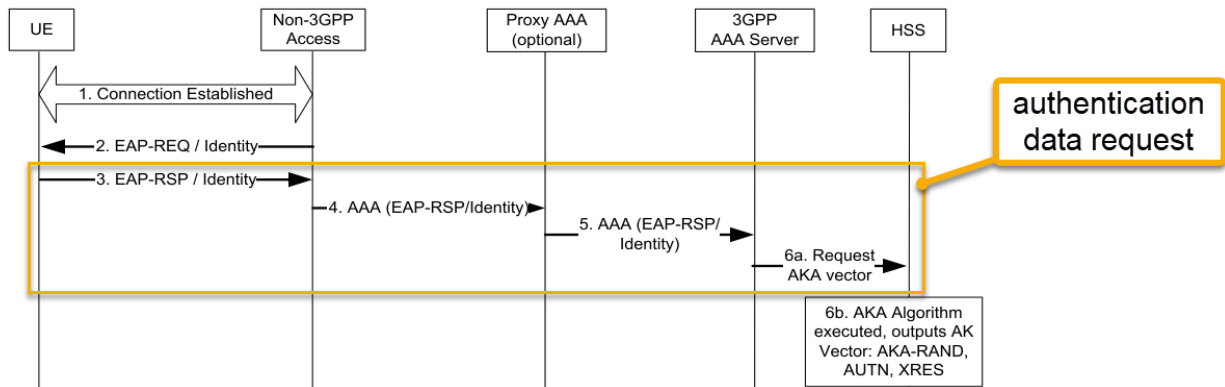
G. Claim 11

1. 11[pre]: A network node for service-based authentication of a terminal to a network, the network node comprising:

As discussed in limitations 1[pre] and 1[a], TS-33.402 discloses a network server (*i.e. network node*) that provides ***service-based authentication of a terminal to a network***. EX1003, ¶139.

2. 11[a]: a receiver configured to receive an authentication data request;

As discussed in limitation 1[a], the network server receives an “EAP Response/Identity message,” *i.e. an authentication data request*. EX1006, 13; Fig. 6.2-1. This message is an *authentication data request* because it is a request containing data for authenticating the terminal with the network server. EX1003, ¶140. This request can be first received by one or more “AAA proxies,” *i.e. a receiver*, which then route the message to a 3GPP AAA Server, as depicted in Figure 6.2-1. *Id.*; EX1003, ¶140.



3. 11[b]: a first generator configured to determine an expected service code associated with the type of communication channel via which the authentication data request was received by the network; and

As discussed above for limitation 5[b], the network server determines the access network identity, *i.e. an expected service code*. The network access identity is “included by the authenticator in the Diameter message” to the 3GPP AAA Server.

EX1006, 13. Accordingly, the 3GPP AAA Server, *i.e.* **first generator**, determines the access network identity. EX1003, ¶¶141-42.

4. **11[c]: a second generator configured to generate in response to the receipt of an authentication data request a modified expected response, wherein the modification of the expected response depends on the determined expected service code.**

As discussed above for limitation 5[c], the network server's HSS (*i.e.* **second generator**) generates a "new authentication vector" containing an XRES value (*i.e.* **modified expected response**). The "new authentication vector" is a **modified expected response** because it is formed by "transform[ing]" an "authentication vector ... by computing $(CK', IK') = F(CK, IK, \langle \text{access network identity} \rangle$." EX1006, 15. Because the transformation relies on the access network identity, the **modification depends on the determined expected service code**. EX1003, ¶¶143-44.

H. Claim 12

1. **12[pre]: A system for service based authentication to a network, comprising:**

See 1[pre]. EX1003, ¶145.

2. **12[a]: a terminal configured to receive an authentication request from the network, to determine a service code associated with the type of communication channel via which the authentication request was received by the terminal, and to send in response to the authentication request a modified response to the network, wherein the modification depends on the determined service code;**

See limitations 1[b], 1[c], 1[d], and 4[b]. EX1003, ¶146.

3. **12[b]: a network node configured to receive an authentication data request and determine an expected service code associated with the type of communication channel via which the authentication data request was received by the network and configured to generate in response to the receipt of the authentication data request a modified expected response wherein the expected response depends on the determined expected service code and configured to compare the modified response with the modified expected response.**

See claim 11. The network server (*i.e.* **network node**) compares XRES (*i.e.* **modified expected response**) with the RES value received from the terminal (*i.e.* **modified response**). EX1006, 15; EX1003, ¶147.

- I. **Claim 13: A computer program product comprising software code portions configured for, when run in the memory of a terminal, executing the method according to claim 1.**

As discussed in claim 1, TS-33.402 (alone or in view of Arkko) recite the method of claim 1 as performed by user equipment (*i.e.* **terminal**). A POSITA would have understood that “user equipment,” a well-known term of art, includes cellular devices which comprise **memory** which store a **computer program comprising software code**. EX1003, ¶148.

X. GROUND 2: TS-33.402 (WITH OR WITHOUT ARKKO) IN VIEW OF ALDERA RENDER OBVIOUS CLAIMS 2, 8-10, AND 13

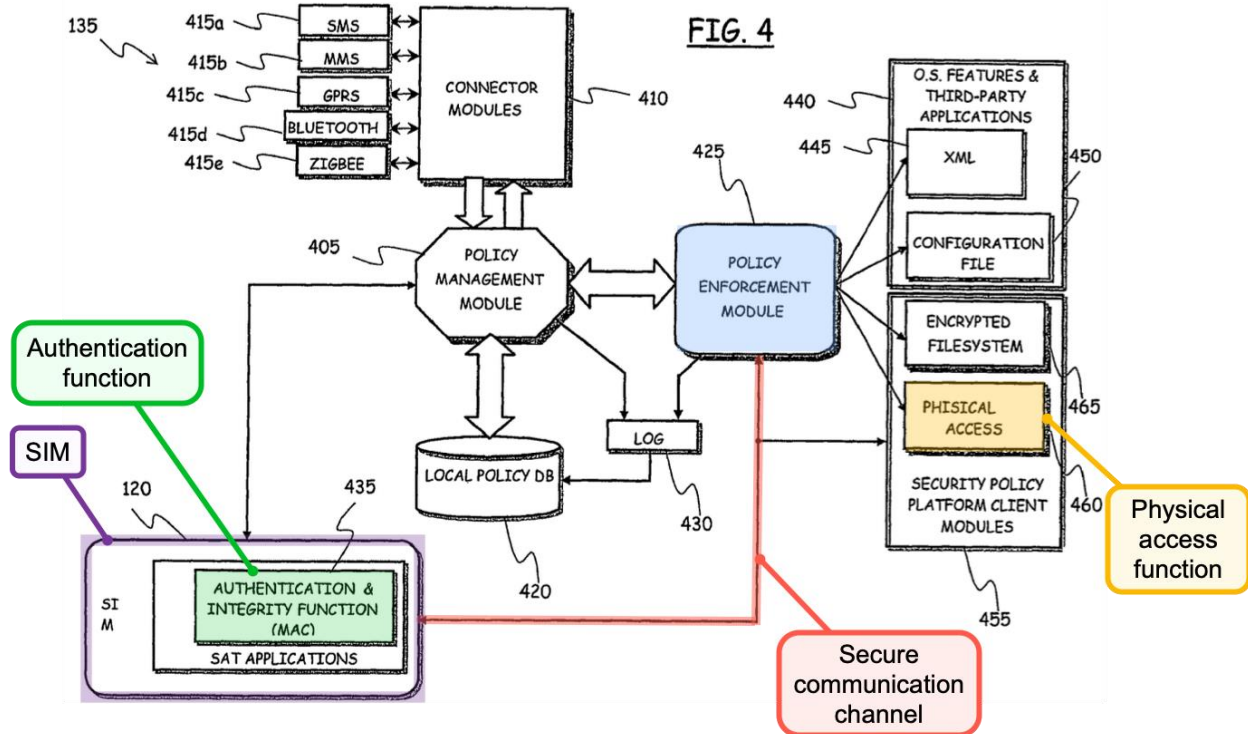
Although TS-33.402 describes a method for performing authentication based on the identified communication channel and Arkko provides further clarification on said authentication method, they do not expressly disclose the hardware components used to perform such methods. However, Aldera describes a service

interface module and identity module and a POSITA would have considered it obvious to combine TS-33.402's methods with Aldera's hardware. EX1003, ¶149.

A. Motivation to Combine

A POSITA would have been motivated to combine TS-33.402's (and optionally Arkko's) description of authentication with the system components described in Aldera. EX1003, ¶¶150-56.

In particular, Aldera describes a "policy management module 405" and its "interface component 505" receive messages from a network via a "connectors module 410" that is coupled to several communication channels. EX1014, 18:50-52; Fig. 5. The policy enforcement module "control[s] the physical access of the user to the [terminal], and a function 465 for the encryption of the file system, or of files or folder of files of the [terminal]." EX1014, 24:28-35.



The policy enforcement module communicates with a SIM via a secure communication channel.

A POSITA would have found it obvious to combine TS-33.402 and Aldera such that TS-33.402's determination of the "access network identity," *i.e.* **determining a communication channel and its service code**, as well as the encryption of the authentication response are performed using the policy enforcement module and its encryption function. TS-33.402 does not specify the specific hardware components of the user terminal for performing its methods, beyond that it is the "USIM" that "computes RES, IK and CK." EX1006, 15. TS-33.402 merely states that it is the "UE" (*i.e.* **user terminal**) which computes the UK' and IK' keys based on the "access network identity" and the "new keying material."

Id. TS-33.402 also states that the “UE calculates a new MAC value covering the EAP message with the new keying material,” again without specifying which component of the user terminal performs this function. *Id.* Thus, a POSITA would be motivated to give effect to TS-33.402’s teachings by implementing such functions into Aldera’s policy management module. EX1003, ¶153.

A POSITA would be further motivated by Aldera itself, which states that the “policy management module” is desirable for “implementing and ensuring the enforcement of desired security policies on the mobile communications devices.” EX1014, 1:43-45. Aldera further teaches that through the use of its system, “a much higher security level can be achieved by providing a mechanism adapted to guarantee the authenticity and integrity of the security policies to be enforced.” *Id.*, 2:49-52. This provides further motivation to incorporate Aldera’s teachings. EX1003, ¶154.

A POSITA would have had a reasonable expectation of success in the combination. Aldera provides significant detail regarding the implementation of its hardware components. TS-33.402 also provides implementation details regarding its methods. Implementation of TS-33.402 using Aldera’s components would therefore have been straightforward and within the skill of an ordinary artisan. EX1003, ¶155.

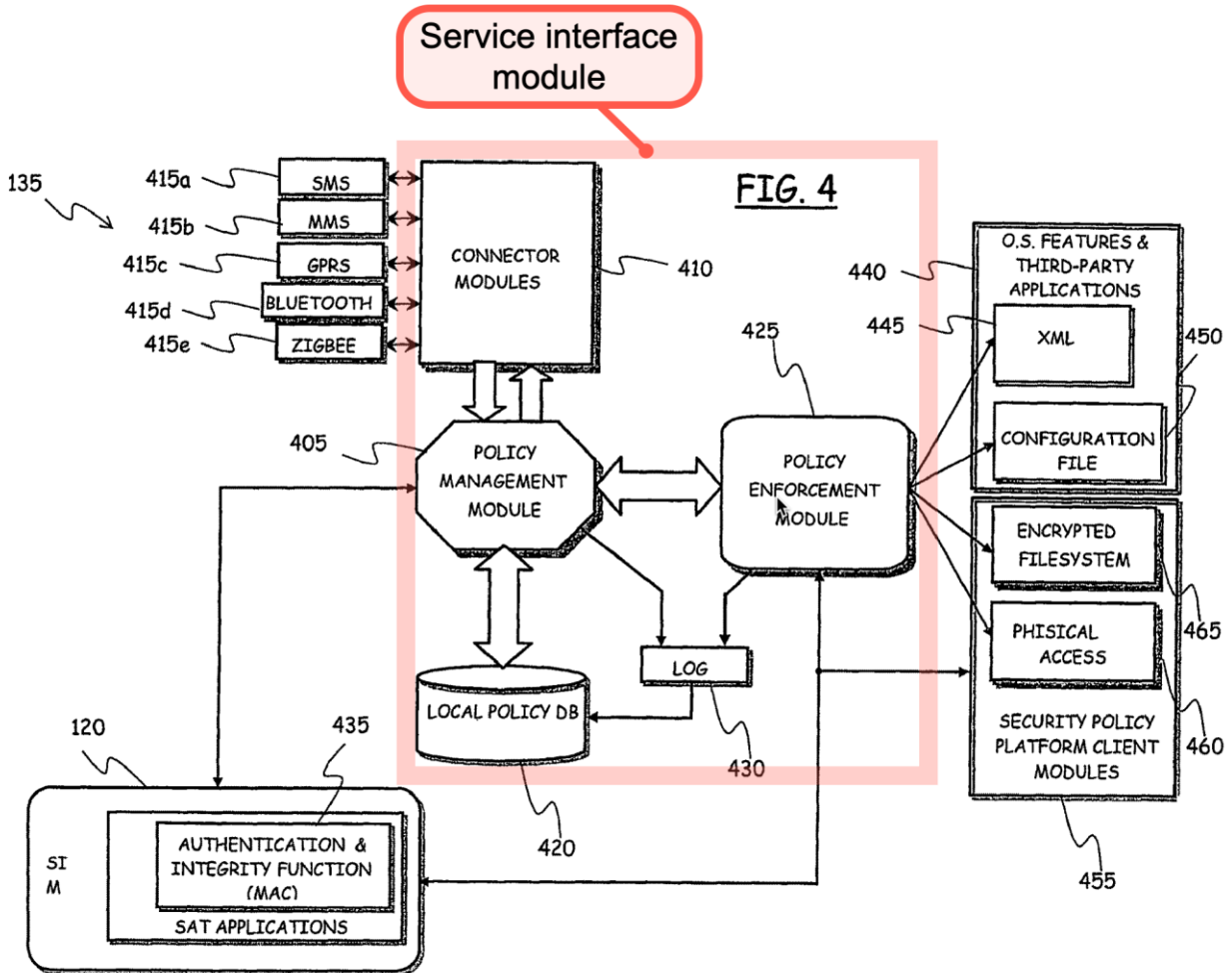
Finally, TS-33.402, Aldera and the '235 patent are directed to the same field of endeavor, namely, authentication within a cellular network. EX1001, Abstract; EX1006, 6; EX1014, Abstract (“A system for enforcing security policies on mobile communications devices”); EX1003, ¶156.

B. Claim 8

1. 8[pre]: Service interface module for use in a terminal, the service interface module comprising:

To the extent this preamble is limiting, Aldera discloses a service interface module for use in a terminal as discussed below. Specifically, Aldera discloses a “platform client ... located at the mobile communications device [*i.e.*, **terminal**] ... [that] is in particular adapted to communicate with the platform server 140 [*i.e.*, the network] for ... receiving the security policies and other signaling [*e.g.*, authentication signals], to locally store the received security policies, and to enforce the security policies locally to the mobile communications device 115.” EX1014, 7:65-8:6. The platform client, which Aldera describes as being a component that is “resident on the mobile communications device [*i.e.*, **terminal**],” is a **service interface module**. EX1014, 8:43-44; EX1003, ¶¶157-58. A schematic of the platform client (*i.e.*, **service interface module**) is shown below in Figure 4. EX1014, Fig. 4. Note that service interface module disclosed by Aldera does not comprise the SIM (*i.e.*, an **identity module**); the service interface module and the SIM are identified as two separate components in Figure 1 shown below. EX1014, Fig. 1.

As discussed above, it would have been obvious to use these components taught by Aldera to perform the methods described in TS-33.402. EX1003, ¶158.



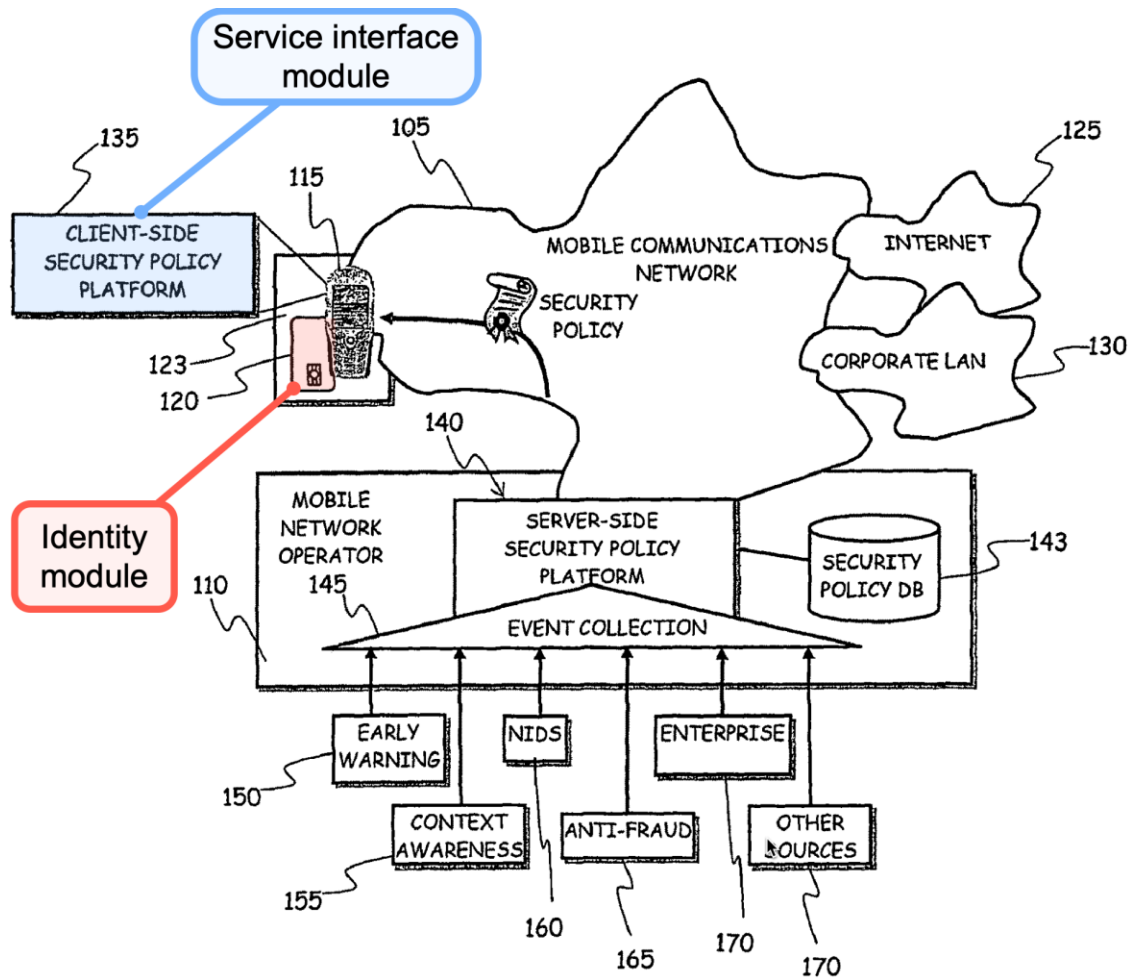
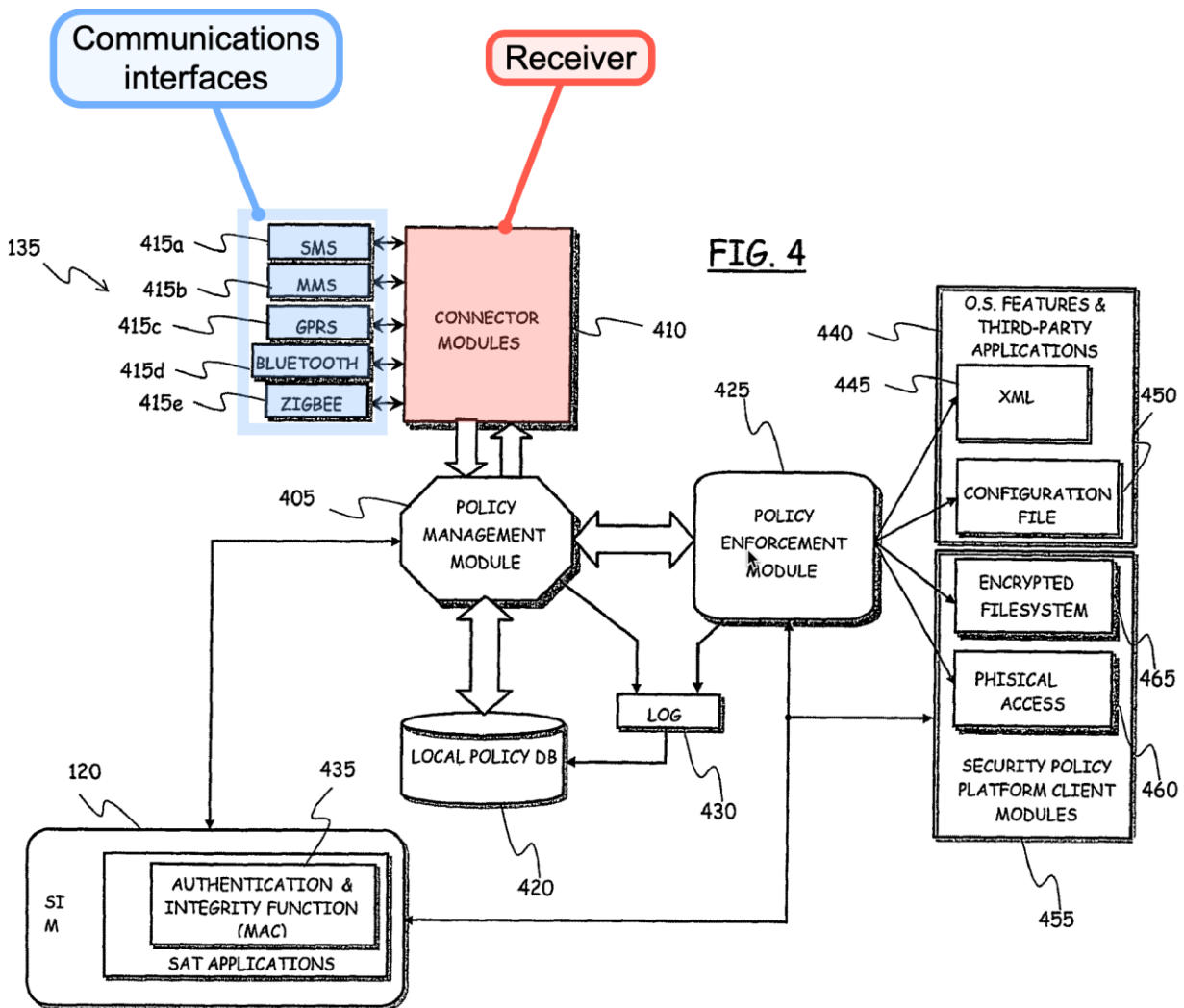


FIG. 1

If “service interface module” is construed as invoking §112(6), its recited function is “to identify the communications channel through which the authentication request was received” and the corresponding structure is 5:56-6:7, 7:45-54, or their equivalents. EX1003, ¶159. Such structure includes a receiver and multiple interfaces. As discussed above, Aldera’s platform client has the same structure. *Id.*

2. **8[a]: a receiver configured to receive an authentication signal from the network via one of the communications interfaces of the terminal;**

Aldera discloses a “connectors module 410 [*i.e.* **receiver**] to multiple **communication interfaces** 415a-415e **of the** mobile communication device [*i.e.*, **terminal**].” EX1014, 18:11-15. The connectors module **receives** communication signals (*e.g.*, **authentication signals**) from the communication interfaces, themselves having had received the communication signals **from the network**. EX1014, 18:16-19 (“The policy management module 405 is responsible of the ... commands/messages [*e.g.*, **authentication signals**] **received** (**through** the connectors module 410) **from the** server side 140 of the platform [*i.e.*, **network**].”). The connectors module therefore functions as a receiver configured to receive authentication signals from the network through the communication interfaces of the terminal. EX1003, ¶¶160-61; EX1014, 19:2-9 (“[T]he policy management module ... is forwarded the messages **received by the connectors module** 410. In particular, when a message from the platform server 140 [*i.e.*, the network] is **received**, the connectors module 410 notifies the policy management module 405[.]”). An illustration of these components is presented in Figure 4 shown below. EX1014, Fig. 4.



3. 8[b]: a channel identifier configured to identify the communication channel through which the authentication signal was received and provide a service code associated with the identified communication channel;

As discussed in Ground 1, limitations 1[c] and 1[d], TS-33.402 alone or in view of Arkko discloses *identifying the communication channel through which the authentication signal was received and providing a service code associated with the identified communication channel*. EX1003, ¶¶162-63.

As discussed in limitation 8[pre], Aldera discloses a service interface module.

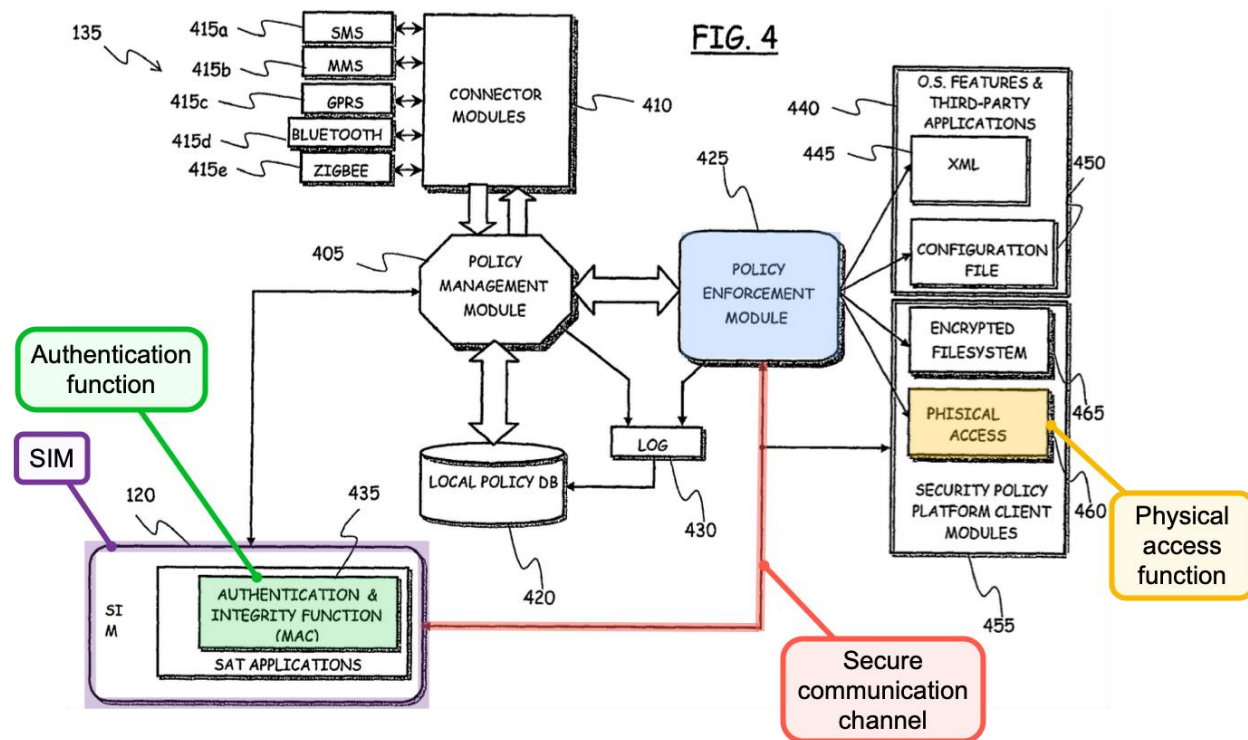
As discussed in the Motivation to Combine, it would have been obvious to combine Aldera's teaching of a service interface module with TS-33.402 (alone or in view of Arkko), which would result in a **channel identifier** that performs the disclosed channel identification and provision of a service code. EX1003, ¶164.

4. 8[c]: a channel interface configured to establish a secure communication channel between the module and an identity module of the terminal; and

The platform client (*i.e.*, service interface module) disclosed by Aldera also includes a component called a “**policy enforcement module** 425 [that] applies the security policies ... to the specified functions, services, applications, [and] modules of [both] the mobile communications device 115 [*i.e.*, **terminal**] ... [and] the platform client 135 [*i.e.*, **service interface module**].” EX1014, 24:19-30. The functions covered by the policy enforcement module are “globally indicated by [component] 455, [and] may include ... a **function 460 controlling the physical access** of the user to the [terminal], and a function 465 for the encryption of the file system, or of files or folder of files of the [terminal].” EX1014, 24:31-35. The **policy enforcement module** is illustrated in Figure 4, shown below. EX1014, Fig. 4.

Specifically, Aldera teaches that **policy enforcement module's physical access function 460** “may request the inputting of a PIN” and other identifying information of the terminal that “is then passed to the **authentication function 435** of the **SIM**”

which “further check[s] whether that device [*i.e.* **terminal**] is entitled to interact with the **SIM**.” EX1014, 24:48-57. Aldera further teaches that “[t]he **function** 460 [from the platform client, *i.e.*, service interface module] may be adapted to block the **SIM** after a predetermined number ... of erroneous PIN inputtings.” EX1014, 24:59-62. The platform client’s **policy enforcement module** is therefore configured to establish a **secure communication channel** between the platform client (*i.e.*, service interface module) and the **SIM** (*i.e.*, identity module of the terminal). EX1003, ¶¶165-67.



5. **8[d]: a modifier configured to modify an authentication response of the identity module on the basis of the service code associated with the identified communication channel.**

As discussed above for limitation 8[c], Aldera discloses a component of the platform client called a **policy enforcement module** that is capable of “controlling

the physical access of the user to the [terminal], and a **function 465 for the encryption** of the file system, or of files or folder of files of the [terminal].” EX1014, 24:30-35.

The **encryption function 465** (*i.e.*, **modifier**) “is adapted to encrypt [*i.e.*, modify] the whole file system, or single files or file folders” by “invok[ing] an encryption function implemented in the **SIM**, e.g. a SAT application, e.g. the **authentication function 435**.” EX1014, 24:66-25:8; EX1003, ¶¶168-69.

As discussed above in Ground 1, limitation 4[b], TS-33.402 discloses ***modifying an authentication response of the identity module on the basis of the service code associated with the identified communication channel*** by encrypting the authentication response to generate a new MAC value. EX1003, ¶170. As also discussed above, it would have been obvious to perform this function using Aldera’s **encryption function 465** (*i.e.*, **modifier**).

- C. **Claim 9: An identity module for establishing a safe communication channel with a service interface module as claimed in claim 8, the identity module comprising: a calculator for calculating a response upon receipt of an authentication request; and a modifier for modifying the response on the basis of a predetermined mathematical function using a service code associated with the identified communication channel.**

“An identity module for establishing a safe communication channel with a service interface module as claimed in claim 8”: As discussed above in connection with limitations 8[c] and 8[d], Aldera discloses both an ***identity module*** and a ***secure***

communication channel between that identity module and a service interface module. EX1003, ¶¶171-72.

“[A] calculator for calculating a response upon receipt of an authentication request”: As discussed in limitation 1[e], TS-33.402 describes generating an authentication response to an authentication request. As also discussed above, a POSITA would have considered it obvious to perform the generation of the authentication response pursuant to TS-33.402 using Aldera’s policy management module and encryption function. EX1003, ¶173.

“[A] modifier for modifying the response on the basis of a predetermined mathematical function using a service code associated with the identified communication channel”: As discussed in Ground 1, limitation 4[b], TS-33.402 alone or in view of Arkko describes modifying the response using the service code, specifically, using a keyed hash algorithm on the authentication response to generate a MAC value. EX1003, ¶174. The keyed hash algorithm is the HMAC-SHA-256-128 algorithm, *i.e. a predetermined mathematical function*. EX1008, 12.

D. Claim 10

- 1. 10[pre]: A terminal for accessing network services, the terminal comprising (i) an operating system having memory configured to store program instructions and (ii) a service interface module configured to identify a communication channel through which an authentication request is received,**

wherein the program instructions are executable by the terminal to:

“A terminal for accessing network services”: As discussed above for claim 8, Aldera discloses a terminal for accessing network services. EX1003, ¶¶175-76.

“[T]he terminal comprising (i) an operating system having memory configured to store program instructions ... wherein the program instructions are executable by the terminal”: Aldera discloses a terminal comprising an operating system having memory configured to store program instructions executable by the terminal. EX1014, 7:41-43 (“The operation of the mobile communications device [i.e., **terminal**] is governed by an **operating system**.”); *id.*, 7:12-16 (“The **memory** 260, in combination with the processor 255 [of the **terminal**], includes at least one software application [i.e., **program instructions**] for **managing** the communication with the mobile communications network[.]”); *id.*, 7:29-32 (“[A]t least some of the shown units can be realized at least in part by means of **software programs** stored in the **memory** 260 and performing the same function when executed by the processor 255 [i.e., **terminal**].”); EX1003, ¶177.

“[T]he terminal comprising ... (ii) a service interface module configured to identify a communication channel through which an authentication request is received”: As discussed above for claim 8, TS-33.402 in view of Aldera renders obvious this limitation. EX1003, ¶178.

2. **10[a]: receive an authentication request from the network;**

See limitation 8[a]. EX1003, ¶179.

3. **10[b]: determine the communication channel through which the authentication request is received;**

See limitation 8[b]. EX1003, ¶180.

4. **10[c]: determine a service code associated with the identified communication channel via which the authentication request was received by the terminal; and**

See limitation 8[c]. EX1003, ¶181.

5. **10[d]: send in response to an authentication request a modified response to the network wherein the modification depends on the determined service code.**

See limitation 8[d]. EX1003, ¶182.

- E. **Claim 13: A computer program product comprising software code portions configured for, when run in the memory of a terminal, executing the method according to claim 1.**

Aldera teaches that various terminal components and functions “can also be realized at least partly by means of [a] *software program* resident in the *memory* and *executed* by the processor of the mobile communications device [*i.e., terminal*].” EX1014, 7:33-36. A POSITA would have understood that a software program could also be used to realize a method involving the terminal, such as the method according to claim 1. EX1003, ¶¶183-84.

- F. **Claim 2: Method according to claim 1, wherein the terminal comprises an identity module and a service interface (SI) module configured to securely communicate with the identity module and**

to identify the communications channel through which the authentication request was received.

As discussed in limitation 8[pre] and 8[c], Aldera discloses ***a service interface module that securely communicates with an identity module***. As discussed in limitation 8[b], TS-33.402 in view of Aldera renders obvious that the service interface module ***identifies the communication channel through which the authentication request was received***. EX1003, ¶184.

XI. GROUND 3: NASLUND RENDERS OBVIOUS CLAIMS 1-7

A. Claim 1

- 1. 1[pre]: Method for service-based authentication of a terminal to a network, the terminal comprising one or more communications interfaces for setting-up a communication channel with the network, the method comprising:**

“Method for service-based authentication of a terminal to a network”: To the extent the preamble is limiting, Naslund discloses this limitation. Naslund teaches the “issu[ance] [of] a policy to ... subscribers[] dictating if the mobile ***terminal*** should accept an insecure negotiation in a foreign[] visited network.” EX1005, 20:23-25. More specifically, Naslund teaches that the terminal “examin[es] incoming AKA [***authentication*** and key agreement] parameters[] and customiz[ing] the subsequent ***security processing*** in dependence on the ***network/operator identity [i.e. service]***.” EX1005, 21:2-3. Thus, Naslund teaches that a terminal processes authentication requests based on the “network/operator identity,” *i.e. based on a service*. EX1003, ¶¶187-88.

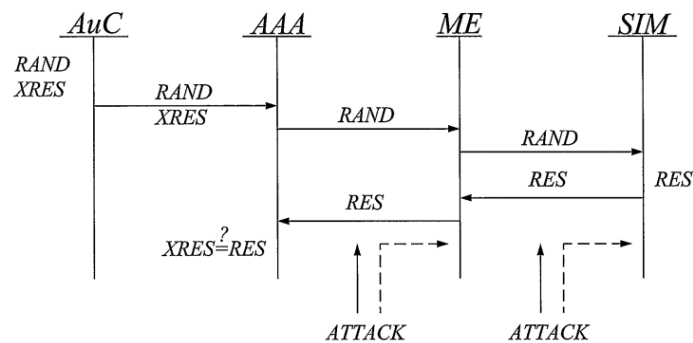
“[T]erminal comprising one or more communications interfaces for setting-up a communication channel with the network”: Naslund discloses a “**terminal** (mobile) [that] may be configured to determine whether the AKA request initially comes over the normal **network interface**, or over another interface such as Bluetooth or IRDA (Infrared Data Association) interfaces.” EX1005, 19:23-25. This “network interface” sets up a communication channel with a, for example, “GSM” or “UMTS” network. *Id.*, 19:9-10; EX1003, ¶189.

2. 1[a]: the terminal sending a service request for access to a network service;

Naslund discloses that the AKA authentication protocol is for “authenticat[ing] [a terminal] to ... **services** [such as] **network access**.” EX1005, 3:5-7; *see also* 13:3-4 (“[A] mobile phone or a personal computer [*i.e.*, a **terminal**] which generally has **some form of network communication capabilities**.”). A POSITA would have understood that access to a network would be initiated by the user terminal sending a **request for access**. EX1003, ¶190. Without an access request from the terminal, the network would not know if and when to initiate an authentication process with the terminal that is needed to facilitate the terminal’s access to the network service. *Id.*

Indeed, Figure 1 of Naslund depicts a typical AKA authentication protocol. Naslund uses protocol, but provides a version with additional steps to enhance security. EX1005, 25:7-27. As explained by Naslund, the first step of authenticating

a user terminal is the network's "subscriber database/authentication center, commonly referred to as an AuC in the context of mobile communication systems," generating "an expected response XRES ... based on knowledge of the secret key," as well as a "challenge RAND." EX1005, 2:1-4; *see also* 25:3-4 ("Network generates RAND, calculates MAC (key, RAND, RAND', ...) and sends RAND and MAC to the SIM."). The secret key is a "user credential" unique to the user. EX1005, 1:22-24. The "expected response XRES" is sent to an "Authorization, Authentication and Accounting" (AAA) server, while the "challenge RAND" is sent to the user terminal so that it "computes the response RES," which is sent to the AAA to determine if it "matches the expected response [XRES]." *Id.*, 2:7-10; EX1003, ¶191.



(Prior Art)

Fig. 1

Thus, a POSITA would understand that in order to initiate the AuC generating the "expected response XRES ... based on knowledge of the secret key," the AuC would need to know the specific user that it is authenticating. A POSITA would

understand that this could only be done if the user's terminal first requests access to the network to initiate the authentication protocol. EX1003, ¶192. The network would not otherwise know that the user's terminal needs to be authenticated. *Id.*

Notably, during prosecution, the applicant did not dispute that Naslund discloses this limitation. EX1002, 99; EX1003, ¶193.

Alternatively, a POSITA would have considered it obvious for the terminal to send a service request for access prior to initiating the AKA authentication protocol. A POSITA would have considered it obvious that, in order for the network to initiate the authentication protocol (*i.e.* the AuC generating an expected response XRES using a user's secret key), the network would need to know the particular user and their user key in order to authenticate. EX1003, ¶194. A POSITA would consider it obvious to have the user terminal request access to the network by identifying the user in order to give effect to this teaching in Naslund. *Id.* A POSITA would have also been motivated by the fact that having the user terminal request network access provides a simple and efficient means for the network to determine that a user terminal requires authentication. *Id.* A POSITA would have reasonably expected such a request to succeed because network access requests were well-known in the art and implementation would have been within the skill of an ordinary artisan. *Id.*

3. 1[b]: the terminal receiving in response to the service request an authentication request from the network;

Naslund discloses that “[i]n normal GSM AKA, the *network sends an authentication request* together with a RAND, and the [terminal’s] SIM simply replies with a response RES.” EX1005, 25:9-11; *see also id.*, 2:6-9 (“The *challenge RAND [i.e., authentication request]* ... is *sent to the terminal* ME (Mobile Equipment), which assisted by the security device computes the response RES.”). Naslund’s invention uses this “normal” AKA protocol, but provides additional steps to enhance security. *Id.*, 25:7-27 (“This authentication can be extended ...”). Figure 11 (reproduced below) offers an illustration of the *SIM* (a component of the terminal) receiving an *authentication request* from the network in the form of a challenge *RAND*. EX1005, Fig. 11; EX1003, ¶¶195-96.

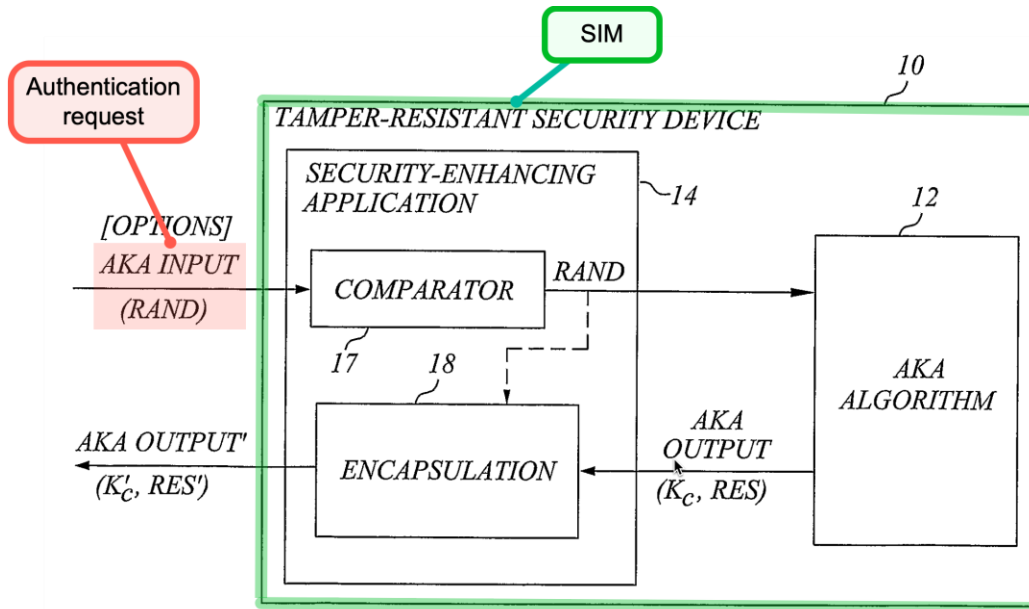


Fig. 11

4. 1[c]: the terminal identifying the communication channel through which the authentication request was received;

Naslund discloses identifying whether the authentication request came over a a normal network interface or some other interface, *i.e.* **identifying the communication** channel. Specifically Naslund discloses that a “**terminal** (mobile) [that] may be configured to **determine** whether [an] AKA request [*i.e.*, **authentication request**] initially comes over the normal network interface, or over another interface such as Bluetooth or IRDA [*i.e.*, **identifying the communication channel**],” with the “origin of the request may ... be [being] determined by the terminal based on port identification (IR Port, Bluetooth Port, Normal Radio Interface Port, etc.).” EX1005, 19:23-29; EX1003, ¶¶197-98.

5. **1[d]: the terminal determining a service code associated with the identified communication channel; and**

Naslund discloses that in order to process the security request, a specific security-enhancing sub application for the request is selected. Thus, Naslund describes determining the code of the appropriate security-enhancing sub application, *i.e. a service code*, that is based on and associated with whether the request came over a normal network interface or some other interface like Bluetooth, IR, or WLAN, *i.e. associated with the identified communication channel*. EX1003, ¶¶199-200.

Specifically, Naslund teaches that “the AKA request is re-routed to the security enhancing application by the terminal ... when the request comes over the Bluetooth or IRDA interface,” noting that “it may be advantageous to customize the security processing by providing a number of different sub applications and selecting among the sub applications *depending* on the *particular* type of [communication] *interface* used by the terminal.” EX1005, 20:1-7. By doing this, “the mobile itself is capable of detecting when a request for SIM access comes over less secure interfaces, and taking appropriate actions accordingly.” *Id.*, 19:25-27. In “selecting among the sub applications depending on the particular type of interface,” the terminal is determining the appropriate sub application to use for processing based on the *identified communication channel*. EX1003, ¶201.

Naslund further discloses that the sub application has a **service code** assigned to it. Naslund’s Table 1 (reproduced below) shows that for each **communication interface** there is a corresponding **label** denoting the “**Security-enhancing sub application**,” and these **labels** serve as **service codes** to reflect a particular **communication channel**. EX1005, Table 1. Thus, in determining the sub application for processing, Naslund’s system **determines a service code associated with the identified communication channel**. EX1003, ¶202. As can be seen, these codes **identify the communication channel** for the particular network/operator. *Id.* For example, the code “01” identifies the “Normal” communication channel for the “Home” network, whereas the code “02” identifies the “Bluetooth” communication channel.

Table I

Security conditions			Security mode	
Environment	Network/Operator	Interface	Normal AKA	Security-enhancing sub application
Mobile	Home	Normal	Enabled	-
PC	Home	Normal	Disabled	01
Mobile	Home	Bluetooth	Disabled	02
Mobile	Home	IR	Disabled	03
Mobile	Home	WLAN	Disabled	04
Mobile	Visited	Normal	-	05 (negotiation)
Mobile	Operator A	Normal	Disabled	06
Mobile	Operator B	Normal	Disabled	07
...				...
PC	Visited	WLAN	Disabled	01,04,05

As discussed above, the examiner considered Naslund during prosecution, but did not rely on Naslund to find disclosure of a “service code associated with the

identified communication channel.” Instead, the examiner initially relied on Ericsson’s “service identifier,” and then Howard’s “context.” EX1002, 122-123, 62. The applicant successfully argued that neither Ericsson nor Howard explained how those elements were service codes associated with a communication channel—indeed, Howard’s “context” appeared to be a typographical error that should have been “content.” EX1003, ¶203.

But the examiner committed a material error by failing to appreciate the full scope of Naslund’s disclosure, especially the disclosure discussed above of sub application codes associated with different communication channels. EX1003, ¶204. The examiner overlooked that each communication channel is assigned a particular sub application for processing appropriate for that communication channel, and that these sub applications are identified by a code. *Id.* Naslund’s sub application code is clearly a “determinable code” “associated with an identified communication channel,” which was the applicant’s description of a “service code.” *Id.*

6. **1[e]: the terminal sending an authentication response to the network, wherein the authentication response depends on the identified communication channel in that the response is calculated on the basis of the information in the authentication request and the determined service code, thereby securely including information regarding the**

identified communication channel through which the authentication request was received into the response.

As explained herein, Naslund teaches the use of a selected security-enhancing application—chosen based on the communication channel through which an authentication request was received—to generate an authentication response that securely contains information regarding the communication channel. EX1003, ¶205.

“the terminal sending an authentication response to the network”: Naslund discloses that the security-enhancing sub application provides an **authentication response** which is sent *to the network*. Naslund is directed to generating AKA requests and responses, *i.e. an authentication response*, by using “security enhancing application[s] ... for encapsulating AKA responses in a more secure algorithm.” EX1005, 6:13-15. As with the a typical AKA protocol, the AKA response is “sent back to the AAA server,” *i.e. sent to the network*. *Id.*, 2:9-10; EX1003, ¶206.

As illustrated in Figure 11, the terminal transmits an **authentication response** RES’. EX1003, ¶207.

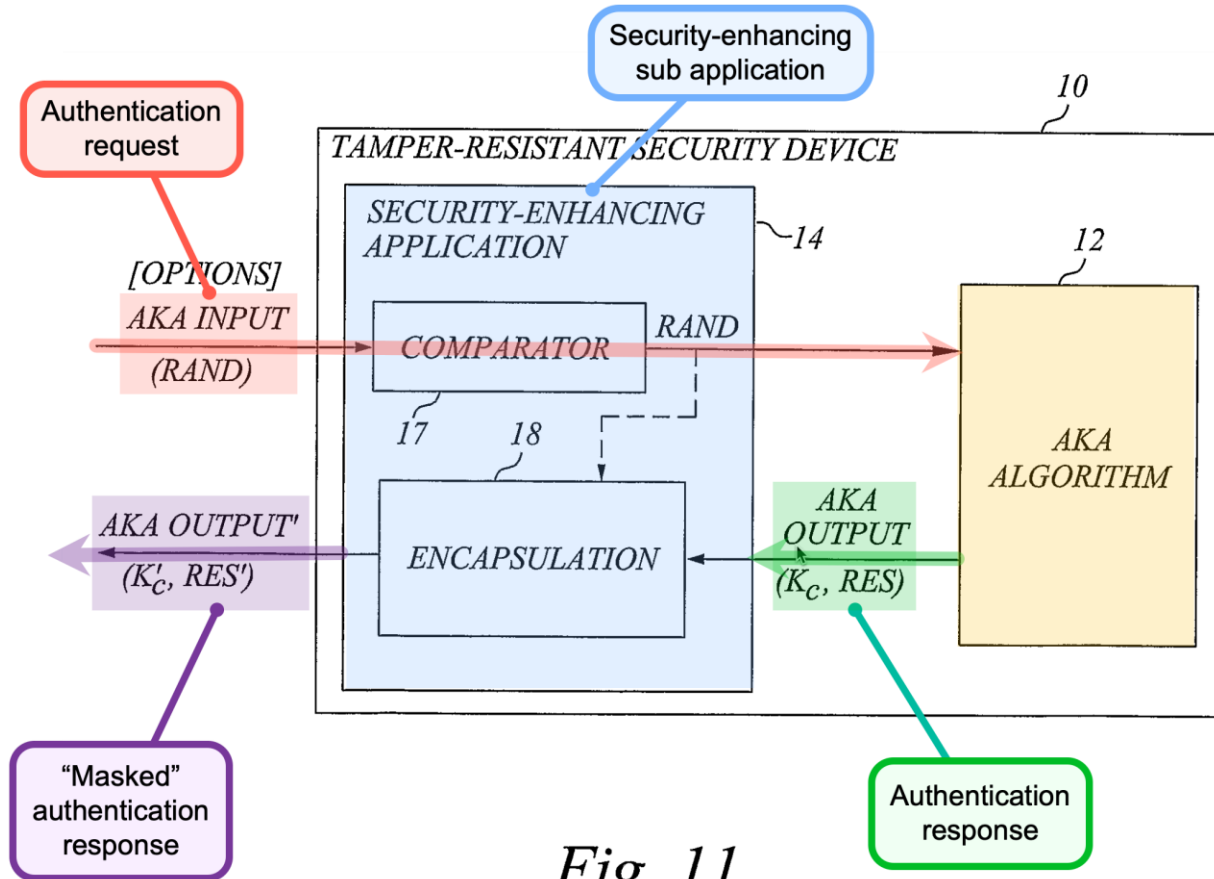


Fig. 11

“wherein the authentication response depends on the identified communication channel in that the response is calculated on the basis of the information in the authentication request and the determined service code”: Naslund teaches that the authentication response RES’ is calculated using the RAND value from the authentication request, *i.e. calculated on the basis of the information in the authentication request*. EX1003, ¶208. Specifically, Naslund teaches that “[t]he AKA algorithms compute a response and/or one or more keys **based on the challenge RAND** (and the stored security key).” EX1005, 14:26-28. As discussed in limitaiton 1[b], the challenge RAND is the **authentication request**.

Naslund further teaches that the response RES' depends on the security-enhancing sub application used to generate it, *i.e. calculated on the basis of the determined service code*. As discussed in limitation 1[d], Naslund discloses “customiz[ing] the security processing” that is to be applied by the SIM on an authentication request “by providing a number of different customized security-enhancing modules or sub applications, and selecting among these modules in dependence on the environment.” EX1005, 17:3-8. The selected security-enhancing sub application is dependent on the service code, and therefore the RES' is, by extension, calculated based on the service code. EX1003, ¶209.

“thereby securely including information regarding the identified communication channel through which the authentication request was received into the response”: A consequence of the additional processing performed by the security-enhancing sub application is to securely embed information about the identified communication channel into RES'. EX1003, ¶210. The output from the security-enhancing process (*i.e.*, RES') will reflect some information about the identified channel given how the specific security-enhancing sub application applied to RES corresponds to a specific identified communication channel. *Id.*

- B. Claim 2: Method according to claim 1, wherein the terminal comprises an identity module and a service interface (SI) module configured to securely communicate with the identity module and**

to identify the communications channel through which the authentication request was received.

The '235 Patent describes an identity module as a Universal Integrated Circuit Card (“UICC”) that contains an application for performing authentication and securely accessing network services (*e.g.*, SIM card, USIM card). EX1001, 6:32-48. Naslund’s Figure 4 “illustrates a user *terminal* 20, such as a mobile phone or a personal computer, which generally has *some form of network communication capabilities* 25 and a *tamper-resistant security device* 10[.]” EX1005, Fig. 4, 13:2-5. The “tamper-resistant security device” is an **identity module** because it stores user credentials and is designed to perform “authentication and/or key agreement based at least partly on [those user credentials].” EX1005, 12:21-29. Indeed, Naslund describes the “tamper-resistant security device” as “a SIM,” much like how the '235 Patent identifies the identity module as a SIM. EX1005, 20:25-26; EX1001, 6:32-48; EX1003, ¶¶211-12.

The '235 Patent describes an SI module “as a central access point to wired and wireless network services and comprises for that purpose a number of service interfaces,” with each service interface associated with a particular mode of signal transmission to/from the terminal (*e.g.*, radio-frequency, Bluetooth, WLAN, Ethernet). EX1001, 5:56-6:11. The '235 Patent further describes an SI module as “provid[ing] a secure communication channel ... with the UICC ... connected to the SI module.” EX1001, 8:1-3.

A POSITA would have understood the module labeled in Naslund's Figure 4 as the "network communication unit(s) (GSM, W-CDMA, Bluetooth, ...)" is an **SI module** because how the network communication unit(s) 25: (i) serves as the terminal's "central access point" for various **network services** (e.g., 2G, 3G, Bluetooth), and (ii) has a **direct communication channel** to the tamper-resistant security device (i.e., **identity module**). EX1003, ¶¶213-14; EX1005, Fig. 4.

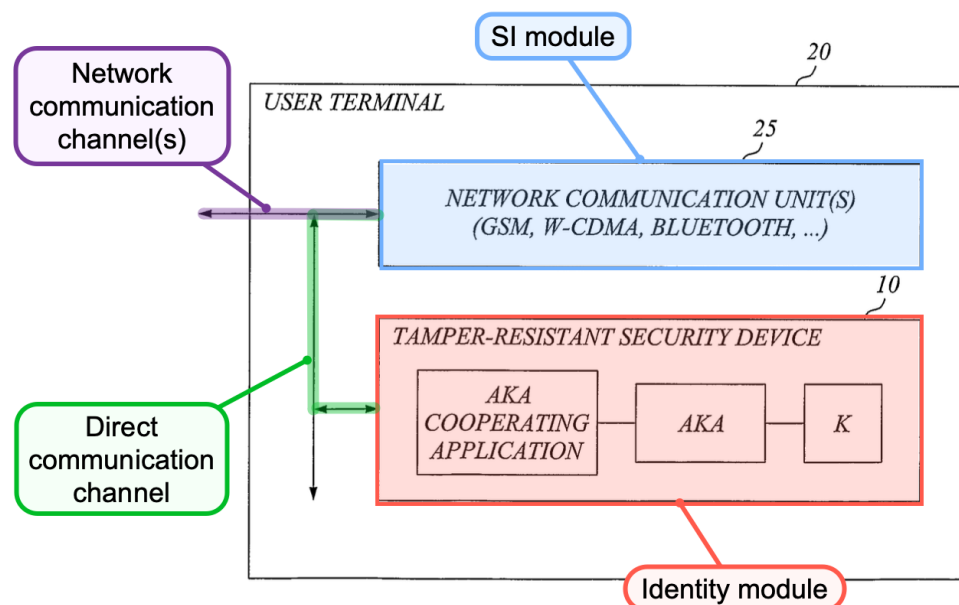


Fig. 4

C. Claim 3

1. 3[pre]: Method according to claim 1, wherein the authentication request comprises authentication information[,] the method further comprising the steps of:

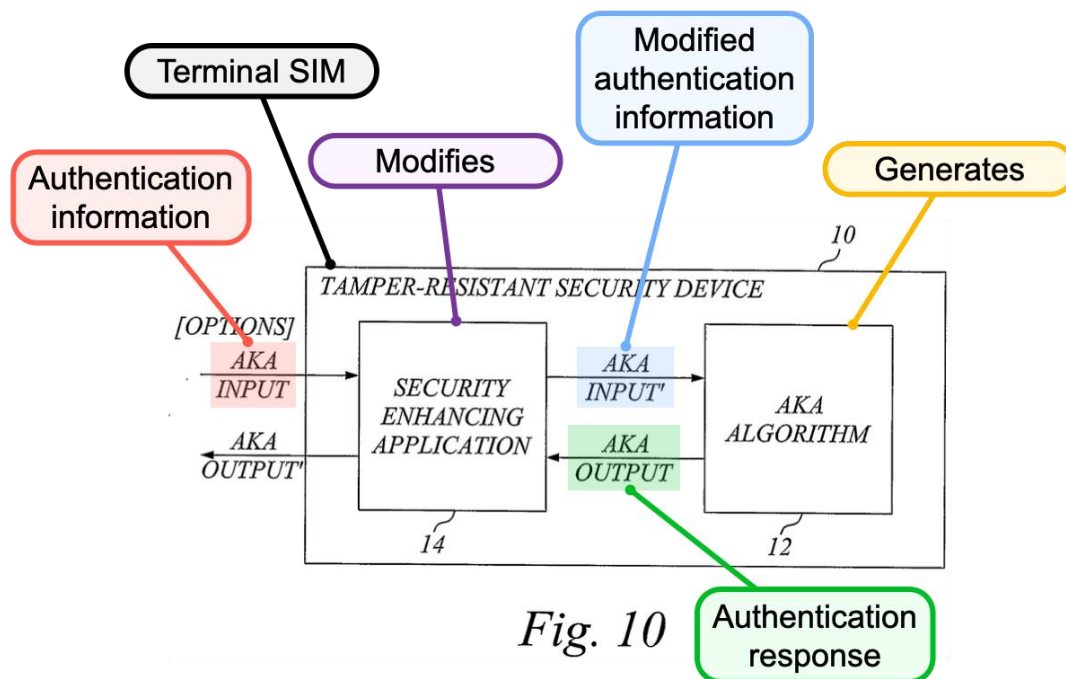
As discussed above in connection with claim 1, Naslund discloses both the method described in claim 1 and an authentication request comprising authentication information. EX1003, ¶¶215-16.

2. **3[a]: the terminal modifying the authentication information on the basis of the identified communications channel; and the terminal generating the authentication response on the basis of the modified authentication information.**

As discussed above in connection with limitations 1[d] and 1[e], the specific security-enhancing sub application that is used by the identity module (*i.e.*, SIM) is selected on the basis of the identified communications channel. Naslund notes that “[t]he encapsulation of AKA keys/responses suggested in the EAP SIM protocol generally implies manipulation of AKA **output** parameters,” and goes on to suggest that “[i]t is however also possible to **manipulate input parameters to the AKA process.**” EX1005, 25:28-26:1. Such manipulation of the input parameters to the AKA process would mean that the authentication request (*i.e.*, **authentication information**) is processed (*i.e.*, **manipulated**) by the security-enhancing sub application on the basis of the identified communications channel (since the specific sub application used to manipulate the authentication information is selected on the basis of the identified communications channel). EX1003, ¶217.

Separately, Naslund also teaches that “[t]he enhanced security processing may involve **manipulation of** output parameters and/or **input** parameters of the AKA process.” EX1005, 23:23-25. This idea is illustrated below in Figure 10, where a particular security enhancing application—which is selected on the basis of the identified communications channel—processes (*i.e.*, **modifies**) the incoming authentication request AKA INPUT (*i.e.*, **authentication information**) to yield a

modified authentication request *AKA INPUT'* (i.e., **modified authentication information**). EX1005, Fig. 10.; EX1003, ¶218. Subsequently, the AKA module receives *AKA INPUT'* and **generates** an **authentication response** *AKA OUTPUT* on the basis of *AKA INPUT'* (i.e., on the basis of the modified authentication information). *Id.*



D. Claim 4

1. 4[pre]: Method according to claim 1, wherein the authentication request comprises authentication information, the method further comprising:

As discussed above in connection with claim 1, Naslund discloses both the method described in claim 1 and an authentication request comprising authentication information. EX1003, ¶219.

2. **4[a]: the terminal generating the authentication response;**

See limitation 3[a]. EX1003, ¶220.

3. **4[b]: the terminal modifying the authentication response on the basis of the identified communications channel.**

As discussed above in connection with limitations 1[d], 1[e], and 3[a], the specific security-enhancing sub application that is used by the identity module (*i.e.*, the terminal's SIM) is selected on the basis of the identified communications channel. Further, as discussed above in connection with limitation 3[a], Naslund teaches that “[t]he enhanced security processing may involve ***manipulation*** [*i.e.*, ***modifying***] of ***output parameters*** and/or input parameters ***of the AKA process***.” EX1005, 23:23-25. This idea is illustrated below in Figure 10, where an AKA module has **generated** an **authentication response** *AKA OUTPUT* after having received an **authentication request** *AKA INPUT*'. EX1005, Fig. 10; EX1003, ¶221. Subsequently, a particular security enhancing application—which is selected on the basis of the identified communications channel—processes (*i.e.*, ***modifies***) the **authentication response** *AKA OUTPUT* to yield a **modified authentication response** *AKA OUTPUT*'. *Id.*

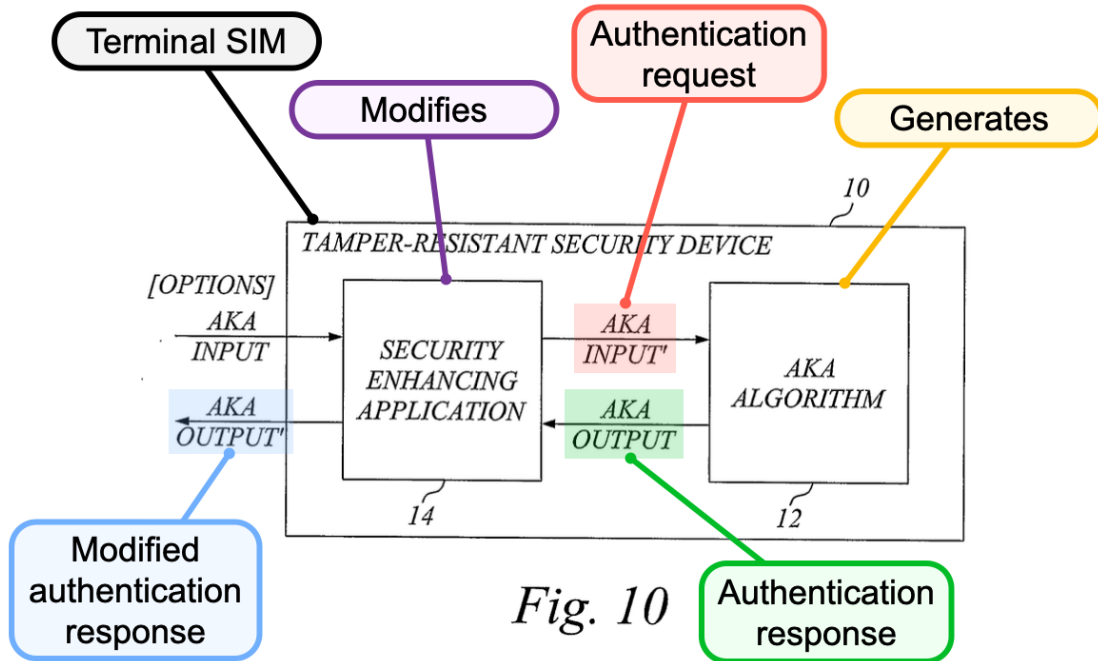


Fig. 10

E. Claim 5

1. **5[pre]/5[a]: Method according to claim 1, the method further comprising: the terminal sending a service request via a predetermined communications channel to the network;**

As discussed above for limitation 1[a], Naslund discloses or renders obvious a terminal sending a **service request** for access to a network service. Moreover, as discussed above in connection with limitations 1[c] and 1[d], and claim 2, Naslund discloses “a user **terminal** ... which generally has some form of **network communication capabilities** [e.g., GSM, W-CDMA, Bluetooth].” EX1005, 13:2-4, Fig. 4. A terminal capable of receiving a signal through a particular communications channel will also be capable of transmitting a signal via a predetermined communications channel because both signal reception and transmission involve the same components and mechanism. EX1003, ¶¶222-23. It would also have been

obvious to a POSITA to utilize the capability of receiving a signal via a particular communications channel to perform the operation of sending a signal via a predetermined communications channel to the network. *Id.*

2. 5[b]: the network generating an expected service code on the basis of the type of communications channel the service request was sent to the network; and

Naslund discloses a “**network server** supporting download of security and/or privacy enhancement applications or applets into a tamper-resistant security device [i.e., identity module].” EX1005, 15:28-29. The network server and its components are illustrated below in Figure 6. EX1005, Fig. 6.

Given the basic structure of the typical authentication protocol—where both the terminal and network have a copy of the same critical information with which to carry out their cryptographic algorithms (*e.g.*, key(s), authentication request data, etc.)—it is implicit in the teachings of Naslund that the network would also be capable of generating an expected service code on the basis of the type of communications channel the service request was sent to the network. EX1003, ¶¶224-26. As discussed above in connection with limitations 1[d] and 1[e], Naslund discloses a terminal that (i) determines a service code associated with the specific communication channel through which an authentication request was received, and (ii) transmits to the network an authentication response that was calculated in part on the basis of the determined service code. In order for the network to carry out an

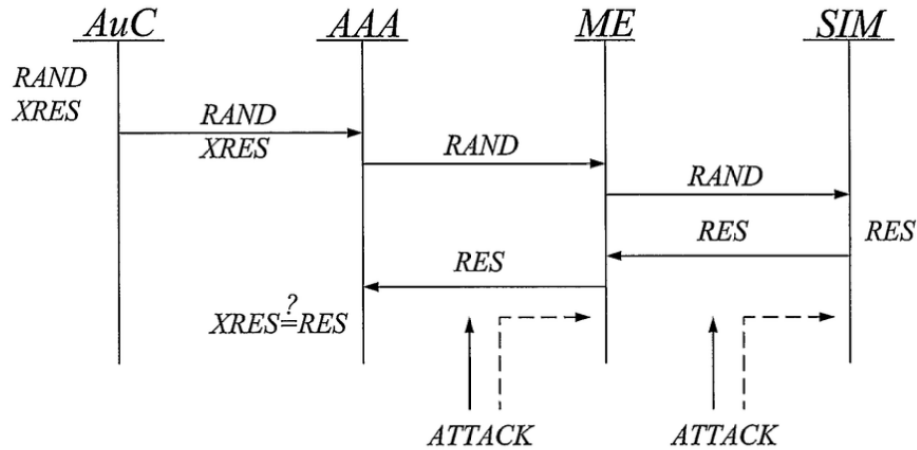
authentication procedure, the network must—as discussed above in the technology overview—have not only the same key and authentication request data used by the terminal, but also any other data that is used to calculate and secure the authentication response; otherwise, without the same elements used by the terminal’s identity module to calculate an authentication response, the authentication procedure can not be implemented. EX1003, ¶226. Moreover, the network server disclosed by Naslund in Figure 6 has all of the components necessary for identifying the communication channel and generating an expected service code: the applets 31, “which are normally under the control of the network operator ... and ‘signed’ by the operator,” would have been understood by a POSITA to be capable of supporting the encryption and/or authentication module 32 by generating a service code on the basis of the communication channel used by the service request. EX1003, ¶226. It is therefore implicit in Naslund that the network must be capable of generating an expected service code on the basis of the specific communication channel through which the terminal’s service request was received in order to perform authentication. *Id.*

3. 5[c]: determining on the basis of the expected service code an expected response.

Naslund discloses a network that is capable of determining “an expected response XRES [that] is generated based on knowledge of the secret key and a generated challenge RAND,” as discussed above in the technology overview.

EX1005, 2:3-4. An illustration of a typical authentication procedure wherein the network calculates an expected response *XRES* which it then uses to compare to the terminal's actual response *RES* is presented below in Figure 1. EX1005, Fig. 1. A POSITA would have found it obvious to use the idea of converting *RAND* to *XRES* to also convert the pairing (*RAND*, expected service code) to *XRES* given the ubiquity of hashing multiple inputs. EX1003, ¶¶227-28.

Separately, Naslund also teaches the “encapsulation of sensitive parameters by manipulating AKA output parameters” to “produce a resulting higher-security response $RES' [=] h(\text{key}, RES(1), \dots, RES(n))$ ” where “the n responses are combined to a single response [*i.e.*, RES'] by a keyed function [h].” EX1005, 23:28-24:7. A POSITA would have found it obvious to incorporate the expected service code as one of the inputs into h to calculate the expected response because the underlying mathematical idea of using multiple inputs to determine a “resulting higher-security response” using h is the same. EX1003, ¶229.



(Prior Art)

Fig. 1

F. Claim 6

1. **6[pre]/6[a]: Method according to claim 5, the method further comprising: comparing the expected response with the authentication response sent by the terminal to the network; and**

As discussed above in connection with limitation 5[c], Naslund discloses a network that compares the expected response with the actual authentication response sent by the terminal. EX1003, ¶230.

2. **6[b]: determining the terminal to be in an un-trusted state if the authentication response is not equal to the expected response.**

Naslund discloses a network that matches the expected and actual authentication response in its Figure 1 (reproduced below), and teaches that “if [the authentication response] matches the expected response [determined by the network], the user [*i.e.*, terminal] is authenticated.” EX1005, Fig. 1, 2:9-10. A

POSITA would have understood that the implication of a ***failed authentication*** procedure (*i.e.*, ***no match*** between the expected and actual authentication response) is that the terminal is in an ***un-trusted state***. EX1003, ¶¶231-32. Indeed, Naslund explains that the entire purpose of the authentication procedures it describes is so that “communicating parties ... can be certain that the other party is the alleged party,” and a POSITA would conclude that a failed authentication would mean the other party (*i.e.* ***the terminal***) is not to be trusted. EX1005, 1:10-13.

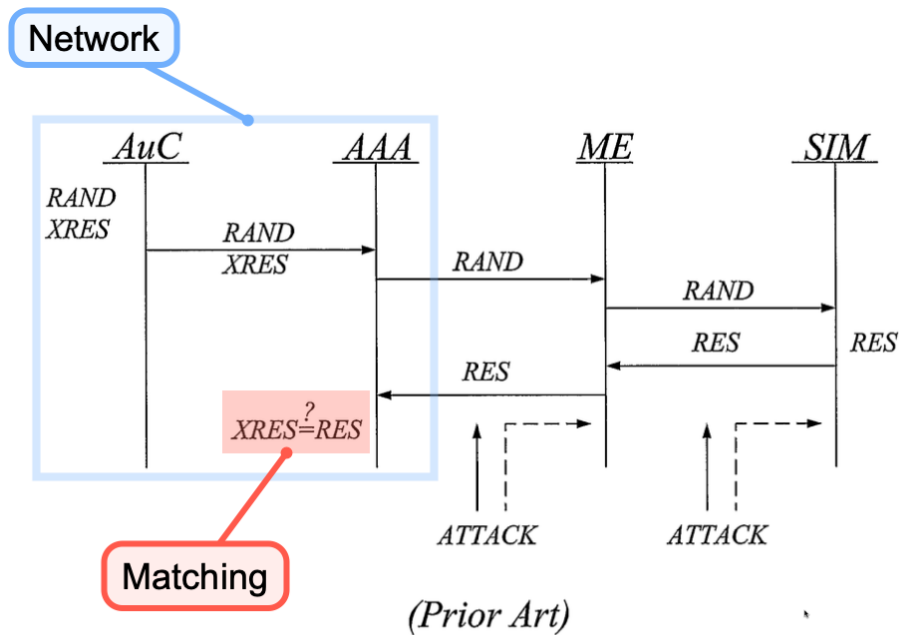


Fig. 1

- G. **Claim 7: Method according to claim 1, wherein the terminal comprises a 2G or 3G type radio interface, a Bluetooth radio interface, a WLAN interface, a digital enhanced cordless (DECT) radio interface or an Ethernet data interface.**

As discussed above in connection with claim 1, Naslund discloses the method described in claim 1. Moreover, as discussed above in connection with limitations

1[c] and 1[d], and claim 2, Naslund discloses a terminal comprising a 2G, 3G, or Bluetooth radio interface, a WLAN interface, or an Ethernet data interface. EX1003, ¶233. Further, a POSITA would have found it obvious to include DECT—which is a form of radio interface—among the other forms of radio interfaces, namely 2G, 3G, and Bluetooth. *Id.*

H. Claim 13: A computer program product comprising software code portions configured for, when run in the memory of a terminal, executing the method according to claim 1.

Naslund discloses that its disclosed methods are “understood” to be “a software implementation.” Ex. 1005, 9:13-16. A POSITA would understand and consider it obvious that “software” comprises *software code which are stored in memory and executed*. EX1003, ¶234.

XII. THE BOARD SHOULD NOT EXERCISE ITS DISCRETION TO DENY INSTITUTION

A. *Fintiv*

Fintiv Factors 1-5—concerning effects on (and of) parallel district court litigation—all favor institution because *there is no parallel litigation* concerning the validity of the ’235 patent between Petitioner and Patent Owner. Petitioner has filed a separate action concerning non-infringement of the ’235 patent but Petitioner did not challenge the validity of the ’235 patent. Further, the Petition’s merits are compelling (Factor 6), which alone demonstrates that the PTAB should not discretionarily deny institution under Fintiv.

B. §314(a)

The Board should not exercise discretionary authority under §314(a). There have been no previous or current IPRs involving the patent. Therefore, §314(a) and *General Plastics* do not provide a basis to deny the Petition.

C. §325(d)

The same or substantially the same prior art or arguments were **not** previously were presented to the Office. Neither TS-33.402 nor Aldera were cited by the examiner. As explained in Ground 3, limitation 1[d], while Naslund was substantively discussed by the examiner, the examiner never relied on it for limitation 1[d] and therefore materially erred by overlooking Naslund's disclosure of service codes associated with each identified communication channel. *See supra* Section XI.A.5. Thus, Petitioner's arguments regarding Naslund are substantively different than those provided by the Examiner.

XIII. CONCLUSION

Petitioner requests institution of an IPR and cancellation of the Challenged Claims.

Date: January 18, 2025

Petition for *Inter Partes* Review

U.S. Patent No. 8,881,235

Respectfully submitted,

By: /s/ James M. Glass

James M. Glass

Counsel for Petitioner

**CERTIFICATE OF COMPLIANCE WITH
TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS,
AND TYPE STYLE REQUIREMENTS**

1. This Petition complies with the type-volume limitation of 14,000 words, comprising 13,932 words, as counted using the Microsoft Word software that was used to prepare this paper, excluding the parts exempted by 37 C.F.R. § 42.24(a).

2. This Petition complies with the general format requirements of 37 C.F.R. § 42.6(a) and has been prepared using Microsoft® Word 2016 in 14-point Times New Roman.

Date: January 18, 2025

By: /s/ James M. Glass
James M. Glass
QUINN EMANUEL URQUHART
& SULLIVAN, LLP
51 Madison Avenue, 22nd Floor
New York, NY 10010
Tel: (212) 849-7000
Fax: (212) 849-7100

Counsel for Petitioner

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on January 20, 2025 true and correct copies of the foregoing document and supporting materials were served in its entirety on the Patent Owner at the following address of record as listed on Patent Center via Priority Mail Express® or Express Mail:

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
Re U.S. Pat. 8,881,235
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO IL 60606
UNITED STATES

Official Correspondence Address

Date: January 18, 2025

By: /s/ James M. Glass
James Glass
QUINN EMANUEL URQUHART
& SULLIVAN, LLP
51 Madison Avenue, 22nd Floor
New York, NY 10010
Tel: (212) 849-7000
Fax: (212) 849-7100

Counsel for Petitioner