

Declaration of Kevin C. Almeroth, Ph.D.
U.S. Patent No. 8,881,235

IN THE 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.

Case No. IPR2025-00512

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

**DECLARATION OF KEVIN C. ALMEROOTH, PH.D. IN SUPPORT OF
PETITION FOR INTER PARTES REVIEW OF
UNITED STATES PATENT NO. 8,881,235**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	BACKGROUND AND QUALIFICATIONS	2
III.	LEGAL STANDARDS	14
	A. Obviousness	15
	B. Claim Construction.....	20
IV.	PERSON OF ORDINARY SKILL IN THE ART AND THE TIME OF THE ALLEGED INVENTION	21
V.	THE '235 PATENT	22
	A. Background of Technology.....	22
	B. Description of the '235 Patent's Specification	24
	C. The '235 Patent's Prosecution History	26
	D. Claim Construction.....	28
	1. "service code" / "expected service code"	29
	2. "communication channel"	30
	3. "authentication data request"	30
	4. "service interface module"	31
	5. "identity module"	32
VI.	Overview of the Prior Art	33
	A. TS-33.402 (Ex. 1006).....	33
	1. TS-33.402 Was Published on October 14, 2008	34
	2. Arkko Was Published on October 24, 2008	35
	B. Naslund (Ex. 1005).....	37
VII.	Grounds of Rejection	38
	A. Ground 1: TS-33.402 Alone or in View of Arkko Render Obvious Claims 1, 3-7, and 11-13.....	38

1.	Claim 1.....	38
	(i) 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:.....	38
	(ii) 1[a]: the terminal sending a service request for access to a network service;.....	40
	(iii) 1[b]: the terminal receiving in response to the service request an authentication request from the network;.....	40
	(iv) 1[c]: the terminal identifying the communication channel through which the authentication request was received;.....	41
	(v) 1[d]: the terminal determining a service code associated with the identified communication channel; and	46
	(vi) 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.....	46
2.	Claim 3.....	49
	(i) 3[pre]: Method according to claim 1, wherein the authentication request comprises authentication information[,], the method further comprising the steps of:	49
	(ii) 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.	49
3.	Claim 4.....	51
	(i) 4[pre]: Method according to claim 1, wherein the authentication request comprises authentication information, the method further comprising:.....	51
	(ii) 4[a]: the terminal generating the authentication response;	51

(iii)	4[b]: the terminal modifying the authentication response on the basis of the identified communications channel.....	51
4.	Claim 5.....	52
(i)	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;.....	52
(ii)	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.	52
5.	Claim 6.....	54
(i)	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.....	54
(ii)	6[b]: determining the terminal to be in an un-trusted state if the authentication response is not equal to the expected response.....	55
6.	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.....	55
7.	Claim 11.....	56
(i)	11[pre]: A network node for service-based authentication of a terminal to a network, the network node comprising:	56
(ii)	11[a]: a receiver configured to receive an authentication data request;	56
(iii)	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	57
(iv)	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.....	57

8.	Claim 12.....	58
	(i) 12[pre]: A system for service based authentication to a network, comprising:.....	58
	(ii) 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;.....	58
	(iii) 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.	58
9.	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.	59
B.	Ground 2: TS-33.402 (With or Without Arkko) in View of Aldera Render Obvious Claims 2, 8-10, and 13	59
1.	Motivation to Combine	60
2.	Claim 8.....	63
	(i) 8[pre]: Service interface module for use in a terminal, the service interface module comprising:.....	63
	(ii) 8[a]: a receiver configured to receive an authentication signal from the network via one of the communications interfaces of the terminal;.....	66
	(iii) 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;.....	67

(iv)	8[c]: a channel interface configured to establish a secure communication channel between the module and an identity module of the terminal; and	68
(v)	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.	70
3.	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.	71
4.	Claim 10.....	72
(i)	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:	72
(ii)	10[a]: receive an authentication request from the network;.....	74
(iii)	10[b]: determine the communication channel through which the authentication request is received;.....	74
(iv)	10[c]: determine a service code associated with the identified communication channel via which the authentication request was received by the terminal; and	74
(v)	10[d]: send in response to an authentication request a modified response to the network wherein the modification depends on the determined service code.....	74
5.	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.	75
6.	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.....	75

C.	Ground 3: Naslund Renders Obvious Claims 1-7	76
1.	Claim 1	76
	(i) 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:.....	76
	(ii) 1[a]: the terminal sending a service request for access to a network service;.....	77
	(iii) 1[b]: the terminal receiving in response to the service request an authentication request from the network;.....	80
	(iv) 1[c]: the terminal identifying the communication channel through which the authentication request was received;.....	81
	(v) 1[d]: the terminal determining a service code associated with the identified communication channel; and	82
	(vi) 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.	84
2.	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.....	87
3.	Claim 3.....	89
	(i) 3[pre]: Method according to claim 1, wherein the authentication request comprises authentication information[,], the method further comprising the steps of:	89
	(ii) 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.	90
4.	Claim 4.....	92

(i)	4[pre]: Method according to claim 1, wherein the authentication request comprises authentication information, the method further comprising:.....	92
(ii)	4[a]: the terminal generating the authentication response;	92
(iii)	4[b]: the terminal modifying the authentication response on the basis of the identified communications channel.....	92
5.	Claim 5.....	93
(i)	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;.....	93
(ii)	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	94
(iii)	5[c]: determining on the basis of the expected service code an expected response.	96
6.	Claim 6.....	97
(i)	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.....	97
(ii)	6[b]: determining the terminal to be in an un-trusted state if the authentication response is not equal to the expected response.....	97
7.	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.....	98
8.	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.	99

VIII. CONCLUSION.....99

I. INTRODUCTION

1. I have been retained by Samsung Electronics America, Inc. and Samsung Electronics Co., Ltd. (“Petitioner”) as an independent expert consultant in this proceeding before the United States Patent and Trademark Office (“PTO”) against Koninklijke KPN N.V. (“Patent Owner”) regarding U.S. Patent No. 8,881,235 (“the ’235 patent”) (Ex. 1001).¹ I have been asked to submit this Declaration on behalf of Petitioner.

2. I have been asked to consider whether certain references disclose or render obvious the features recited in claims 1-13 (collectively, the “Challenged Claims”) of the ’235 patent. My opinions are set forth below. Based on my experience and expertise, it is my opinion that the prior art renders obvious all limitations of the Challenged Claims, as I discuss in detail below.

3. I am being compensated at a rate of \$850 per hour for my work in this proceeding. My compensation is in no way contingent on the nature of my findings, the presentation of my findings in testimony, or the outcome of this or any other proceeding. I have no other interest in this proceeding.

¹ Where appropriate, I refer to exhibits that I understand are to be attached to the petition for *Inter Partes* Review of the ’235 patent.

4. All of my opinions stated in this Declaration are based on my own personal knowledge and professional judgment. I am over 18 years of age and, if I am called upon to do so, I would be competent to testify as to the matters set forth in this Declaration.

II. BACKGROUND AND QUALIFICATIONS

5. I am currently a Professor Emeritus in the Department of Computer Science at the University of California, Santa Barbara (UCSB). While at UCSB, I held faculty appointments and was a founding member of the Computer Engineering (CE) Program, Media Arts and Technology (MAT) Program, and the Technology Management Program (TMP). I also served as the Associate Director of the Center for Information Technology and Society (CITS) from 1999 to 2012. I have been a faculty member at UCSB since July 1997.

6. I hold three degrees from the Georgia Institute of Technology: (1) a Bachelor of Science degree in Information and Computer Science (with minors in Economics, Technical Communication, and American Literature) earned in June 1992; (2) a Master of Science degree in Computer Science (with specialization in Networking and Systems) earned in June 1994; and (3) a Doctor of Philosophy (Ph.D.) degree in Computer Science (Dissertation Title: Networking and System Support for the Efficient, Scalable Delivery of Services in Interactive Multimedia System, minor in Telecommunications Public Policy) earned in June 1997. During

my education, I took a wide variety of courses as demonstrated by my minor. My undergraduate degree also included a number of courses more typical of a degree in electrical engineering including digital logic, signal processing, and telecommunications theory.

7. One of the major concentrations of my research over the past 30+ years has been the delivery of multimedia content and data between computing devices, including through various network architectures. In my research, I have studied large-scale content delivery systems, and the use of servers located in a variety of geographic locations to provide scalable delivery to hundreds or thousands of users simultaneously. I have also studied smaller-scale content delivery systems in which content is exchanged between individual computers and portable devices. My work has emphasized the exchange of content more efficiently across computer networks, including the scalable delivery of content to many users, mobile computing, satellite networking, delivering content to mobile devices, and network support for data delivery in wireless networks.

8. In 1992, the initial focus of my research was on the provision of interactive functions (e.g., VCR-style functions like pause, rewind, and fast-forward) for near video-on-demand systems in cable systems; in particular, how to aggregate requests for movies at a cable head-end and then how to satisfy a multitude of requests using one audio/video stream broadcast to multiple receivers

simultaneously. This research has continually evolved and resulted in the development of techniques to scalably deliver on-demand content, including audio, video, web documents, and other types of data, through the Internet and over other types of networks, including over cable systems, broadband telephone lines, and satellite links.

9. An important component of my research has been investigating the challenges of communicating multimedia content, including video, between computers and across networks including the Internet. Although the early Internet was used mostly for text-based, non-real time applications, the interest in sharing multimedia content, such as video, quickly developed. Multimedia-based applications ranged from downloading content to a device to streaming multimedia content to be instantly used. One of the challenges was that multimedia content is typically larger than text-only content, but there are also opportunities to use different delivery techniques since multimedia content is more resilient to errors. I have worked on a variety of research problems and used a number of systems that were developed to deliver multimedia content to users. One content-delivery method I have researched is the one-to-many communication facility called “multicast,” first deployed as the Multicast Backbone, a virtual overlay network supporting one-to-many communication. Multicast is one technique that can be used on the Internet to provide streaming media support for complex applications like video-on-demand,

distance learning, distributed collaboration, distributed games, and large-scale wireless communication. The delivery of media through multicast often involves using Internet infrastructure, devices and protocols, including protocols for routing and TCP/IP.

10. Starting in 1997, I worked on a project to integrate the streaming media capabilities of the Internet together with the interactivity of the web. I developed a project called the Interactive Multimedia Jukebox (IMJ). Users would visit a web page and select content to view. The content would then be scheduled on one of a number of channels, including delivery to students in Georgia Tech dorms delivered via the campus cable plant. The content of each channel was delivered using multicast communication.

11. In the IMJ, the number of channels varied depending on the capabilities of the server including the available bandwidth of its connection to the Internet. If one of the channels was idle, the requesting user would be able to watch their selection immediately. If all channels were streaming previously selected content, the user's selection would be queued on the channel with the shortest wait time. In the meantime, the user would see what content was currently playing on other channels, and because of the use of multicast, would be able to join one of the existing channels and watch the content at the point it was currently being transmitted.

12. The IMJ service combined the interactivity of the web with the streaming capabilities of the Internet to create a jukebox-like service. It supported true Video-on-Demand when capacity allowed, but scaled to any number of users based on queuing requested programs. As part of the project, we obtained permission from Turner Broadcasting to transmit cartoons and other short-subject content. We also connected the IMJ into the Georgia Tech campus cable television network so that students in their dorms could use the web to request content and then view that content on one of the campus's public access channels.

13. More recently, I have also studied issues concerning how users choose content, especially when considering the price of that content. My research has examined how dynamic content pricing can be used to control system load. By raising prices when systems start to become overloaded (i.e., when all available resources are fully utilized) and reducing prices when system capacity is readily available, users' capacity to pay as well as their willingness can be used as factors in stabilizing the response time of a system. This capability is particularly useful in systems where content is downloaded or streamed on-demand to users.

14. As a parallel research theme, starting in 1997, I began researching issues related to wireless devices and sensors. In particular, I was interested in showing how to provide greater communication capability to "lightweight devices," i.e., small form-factor, resource-constrained (e.g., CPU, memory, networking, and

power) devices. Starting in 1998, I published several papers on my work to develop a flexible, lightweight, battery-aware network protocol stack. The lightweight protocols we envisioned were similar in nature to protocols like Bluetooth, Universal Plug and Play (UpnP) and Digital Living Network Alliance (DLNA).

15. From this initial work, I have made wireless networking—including ad hoc, mesh networks and wireless devices—one of the major themes of my research. My work in wireless networks spans the protocol stack from applications through to the encoding and exchange of data at the data link and physical layers.

16. At the application layer, even before the large-scale “app stores” were available, my research looked at building, installing, and using apps for a variety of purposes, from network monitoring to support for traditional computer-based applications (e.g., content retrieval) to new applications enabled by ubiquitous, mobile devices. For example, my research has looked at developing applications for virally exchanging and tracking “coupons” through “opportunistic contact” among mobile wireless devices (i.e., communication among devices moving into communication range with each other). In many of the courses I have taught there is a project component. Through these projects I have supervised numerous efforts to develop new “apps” for download and use across a variety of mobile platforms.

17. Toward the middle of the protocol stack, my research has also looked to build wireless infrastructure support to enable communication among a set of

mobile devices unaided by any other kind of network infrastructure. These kinds of networks are useful either in challenged network environments (e.g., when a natural disaster has destroyed existing infrastructure) or when suitable support for network communication never existed. The deployment of such networks (or even the use of traditional network support) are critical to support services like disaster relief, catastrophic event coordination, and emergency services deployment.

18. Yet another theme is monitoring wireless networks, in particular different variants of IEEE 802.11 compliant networks, to (1) understand the operation of the various protocols used in real-world deployments, (2) use these measurements to characterize use of the networks and identify protocol limitations and weaknesses, and (3) propose and evaluate solutions to these problems. I have successfully used monitoring techniques to study wireless data link layer protocol operation and to improve performance by enhancing the operation of such protocols. For wireless protocols, this research includes functions like network acquisition and channel bonding.

19. One theme in my wireless network research has been cross-layer solutions and innovations. As mentioned above, with greater wireless device use and network support, we envisioned new application paradigms and services, for example, when mobile devices come into contact with each other. Instead of relying on existing infrastructure to relay communication, the devices are able to discover

each other and communicate directly. Other examples include discovering and using location information to enhance users' experiences. Network support and novel applications span use a variety of network architectures supporting users on foot, in vehicles, and across varying terrains and environments. Finally, we studied how communication efficiency can be supported through intelligent handoffs as well as location and movement prediction.

20. Protecting networks, including their operation and content, has been an underlying theme of my research almost since the beginning of my research career. Starting in 2000, I have been involved in several projects that specifically address security, network protection, and firewalls. After significant background work, a team on which I was a member successfully submitted a \$4.3M grant proposal to the Army Research Office (ARO) at the Department of Defense to propose and develop a high-speed intrusion detection system. Key aspects of the system included associating streams of packets and analyzing them for viruses and other malware. Once the grant was awarded, we spent several years developing and meeting the milestones of the project. A number of my students worked on related projects and published papers on topics ranging from intrusion detection to developing advanced techniques to be incorporated into firewalls. I have also used firewalls, including their associated malware detection features, in developing techniques for the classroom to ensure that students are not distracted by online content.

21. My recent work ties some of the various threads of my past research together. I have investigated content delivery in online social networks and proposed reputation management systems in large-scale social networks and marketplaces. On the content delivery side, I have looked at issues of caching and cache placement, especially when content being shared and the cache has geographical relevance. We were able to show that effective caching strategies can greatly improve performance and reduce deployment costs. Our work on reputation systems showed that reputations have economic value, and as such, creates a motivation to manipulate reputations. In response, we developed a variety of solutions to protect the integrity of reputations in online social networks. The techniques we developed for content delivery and reputation management were particularly relevant in peer-to-peer communication and recommendations for downloadable “apps.”

22. As an important component of my research program, I have been involved in the development of academic research into available technology in the market place. One aspect of this work is my involvement in the Internet Engineering Task Force (IETF). The IETF is a large and open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. I have been involved in various IETF groups including many content delivery-related working

groups like the Audio Video Transport (AVT) group, the MBone Deployment (MBONED) group, Source Specific Multicast (SSM) group, the Inter-Domain Multicast Routing (IDMR) group, the Reliable Multicast Transport (RMT) group, the Protocol Independent Multicast (PIM) group, etc. I have also served as a member of the Multicast Directorate (MADDOGS), which oversaw the standardization of all things related to multicast in the IETF. Finally, I was the Chair of the Internet2 Multicast Working Group for seven years.

23. My involvement in the research community extends to leadership positions for several academic journals and conferences. I am the co-chair of the Steering Committee for the ACM Network and System Support for Digital Audio and Video (NOSSDAV) workshop and on the Steering Committees for the International Conference on Network Protocols (ICNP), ACM Sigcomm Workshop on Challenged Networks (CHANTS), and IEEE Global Internet (GI) Symposium. I have served or am serving on the Editorial Boards of IEEE/ACM Transactions on Networking, IEEE Transactions on Mobile Computing, IEEE Network, ACM Computers in Entertainment, AACE Journal of Interactive Learning Research (JILR), and ACM Computer Communications Review. I have co-chaired a number of conferences and workshops including the IEEE International Conference on Network Protocols (ICNP), IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), International Conference on

Communication Systems and Networks (COMSNETS), IFIP/IEEE International Conference on Management of Multimedia Networks and Services (MMNS), the International Workshop On Wireless Network Measurement (WiNMee), ACM Sigcomm Workshop on Challenged Networks (CHANTS), the Network Group Communication (NGC) workshop, and the Global Internet Symposium, and I have served on the program committees for numerous conferences.

24. Furthermore, in the courses I taught at UCSB, a significant portion of my curriculum covered aspects of the Internet and network communication including the physical and data link layers of the Open System Interconnect (OSI) protocol stack, and standardized protocols for communicating across a variety of physical media such as cable systems, telephone lines, wireless, and high-speed Local Area Networks (LANs). The courses I have taught also cover most major topics in Internet communication, including data communication, multimedia encoding, and mobile application design. My research and courses have covered a range of physical infrastructures for delivering content over networks, including cable, Integrated Services Digital Network (ISDN), Ethernet, Asynchronous Transfer Mode (ATM), fiber, and Digital Subscriber Line (DSL). For a complete list of courses I have taught, see my curriculum vitae (CV).

25. In addition, I co-founded a technology company called Santa Barbara Labs that was working under a sub-contract from the U.S. Air Force to develop very

accurate emulation systems for the military's next generation internetwork. Santa Barbara Labs' focus was in developing an emulation platform to test the performance characteristics of the network architecture in the variety of environments in which it was expected to operate, and, in particular, for network services including Ipv6, multicast, Quality of Service (QoS), satellite-based communication, and security. Applications for this emulation program included communication of a variety of multimedia-based services, including video conferencing and video-on-demand.

26. In addition to having co-founded a technology company myself, I have worked for, consulted with, and collaborated with companies for nearly 30 years. These companies range from well-established companies to start-ups and include IBM, Hitachi Telecom, Turner Broadcasting System (TBS), Bell South, Digital Fountain, RealNetworks, Intel Research, Cisco Systems, and Lockheed Martin.

27. Through my graduate education, leadership with CITS, involvement in TMP, role in the development of the Internet2 infrastructure, and consulting with ISPs, I have gained a strong understanding in the role of the Internet in our society and the challenges of deploying large-scale production networking infrastructure. CITS, since its inception, has looked at the role of the Internet in society, including how the evolution of technology have created communication opportunities and challenges, including, for example through disruptive technologies like P2P. TMP

looks to focus on non-purely technical issues, including, for example, state-of-the-art business methods, strategies for successful technology commercialization, new venture creation, and best practices for fostering innovation. Through my industry collaborations and Internet2 work, I have developed significant experience in the challenges of deploying, monitoring, managing, and scaling communication infrastructure to support evolving Internet services like streaming media, conferencing, content exchange, social networking, and e-commerce.

28. I am a Member of the Association of Computing Machinery (ACM) and a Fellow of the Institute of Electrical and Electronics Engineers (IEEE).

29. Additional details about my employment history, fields of expertise, courses taught, and publications are further included in my CV attached as Ex. 1004.

30. Based on my professional experience, I believe I am qualified to testify as an expert on matters related to the patent at issue.

III. LEGAL STANDARDS

31. Petitioner' attorneys have explained to me the legal standards that apply in this case. My understanding of those standards is described below. I am not an attorney, and I do not have formal training in the law regarding patents. I have used my understanding of the following legal principles set forth in this section in reaching my opinions.

32. I understand that, in this proceeding, Petitioner have the burden of proving that the challenged claims are invalid by a preponderance of the evidence.

A. Obviousness

33. I have been informed that a claim is invalid as obvious under 35 U.S.C. § 103 (pre-AIA) if the differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious at the time of the invention to a person of ordinary skill in the art. I have been informed that the following matters are relevant to determining whether the claimed invention would have been obvious: (1) the scope and content of the prior art, (2) the difference or differences between the patent claim and the prior art, (3) the level of ordinary skill in the art at the time the invention of the patent, and (4) any secondary considerations or objective indicia of non-obviousness.

34. I have been informed that the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. When a claim simply arranges prior art elements with each performing the same function it had been known to perform and yields no more than one would expect from such an arrangement, then such a combination is obvious. When a patent claims a structure already known in the prior art altered by the mere substitution of one element for another known in the field, the combination is likely to be obvious unless the combination yields an unpredictable result.

35. I have been informed that when a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a person of ordinary skill in the art can implement a predictable variation, such a variation is likely unpatentable. For the same reason, if a technique has been used to improve one device, and one of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill. One question to consider is whether the improvement is more than predictably using prior art elements according to their established functions.

36. I have been informed that it may often be necessary, in a validity analysis, to consider whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue. This can be accomplished by looking to interrelated teachings of multiple patents or other publications or pieces of prior art; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by one of ordinary skill in the art.

37. I have been informed that a validity analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim; it is appropriate to take account of the inferences and creative steps that a person of

ordinary skill in the art would employ. I have been informed that a person of ordinary skill in the art is a person of ordinary creativity, not an automaton.

38. I have been informed that a claim composed of several elements is not proved obvious merely by demonstrating that each element was, independently, known in the prior art. I have been informed that it can be important to identify a reason that would have prompted a person of ordinary skill in the art in the relevant field to combine the elements in the way the claimed new invention does. I am told that one way that subject matter can be proved obvious is by noting there existed at the time of the invention a known problem for which there was an obvious solution encompassed by the patent's claims. I have been informed that any need or problem known in the field of endeavor at the time of the claimed invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.

39. I have been informed that one should not assume that a person of ordinary skill in the art attempting to solve a problem will be led only to those elements of prior art designed to solve the same problem. Instead, I have been informed that since familiar items may have obvious uses beyond their primary purposes, in many cases a person of ordinary skill in the art will be able to fit the teachings of multiple prior art references together like pieces of a puzzle.

40. I have been informed that, when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable

solutions, persons of ordinary skill in the art have good reason to pursue the known options within their technical grasp. If this leads to the anticipated success, the product was likely not accomplished by innovation but by using ordinary skill and common sense. I have been informed that, in such an instance, the fact that the combination was obvious to try may show that the combination was obvious.

41. I have been informed that, when determining whether a claimed combination would have been obvious, the correct analysis is not whether a person of ordinary skill in the art, writing on a blank slate, would have chosen the particular combination of elements described in the claim. Instead, I have been informed that the correct analysis considers whether one of ordinary skill, facing the wide range of needs created by developments in the field of endeavor, would have seen a benefit to selecting the combination claimed.

42. I have been informed that, when determining whether a claimed invention is obvious, any “secondary considerations” of non-obviousness identified by the patentee should also be considered. These secondary considerations can include:

- commercial success of the invention, causally related to the invention itself rather than to companion factors, such as advertising or attractive packaging;

- the invention taught away from the technical direction followed by those skilled in the art;
- a long-felt but unsatisfied need for the invention while the needed implementing arts and elements had long been available;
- the invention achieves results unexpected to those skilled in the art;
- copying of the invention by competitors as distinguished from their independent development
- unsuccessful attempts by those skilled in the art to make the invention;
- acquiescence by the industry to the patent's validity by honoring the patent through taking licenses or not infringing the patent, or both; and
- skepticism, disbelief in or incredulity by those skilled in the art that the patentee's approach worked.

43. I have been informed that, for the above information to impact the obviousness of a patent claim, there must be a nexus between the alleged secondary

considerations and the claims. In addition, I have been informed that the burden of introducing evidence of secondary considerations generally is on the Patent Owner. If the Patent Owner or its expert should assert secondary considerations of non-obviousness, I reserve the right to provide a Declaration addressing assertions of non-obviousness due to secondary considerations.

B. Claim Construction

44. I have been informed that claim terms are typically given their plain and ordinary meanings, as would have been understood by a person of ordinary skill in the art at the time of the earliest alleged priority date. I have further been informed that when considering the meaning of any terms in the Challenged Claims of the '235 patent, I should apply the plain and ordinary meaning of those terms. I have further been informed that in considering the meaning of the claims, one must consider the language of the claims, the specification, and the prosecution history of record.

45. I have been informed that in general, a preamble limits the invention if it recites essential structure or steps, or if it is necessary to give life, meaning, and vitality to the claim. I have further been informed that a preamble is not limiting where a patentee defines a structurally complete invention in the claim body and uses the preamble only to state a purpose or intended use for the invention. I have further been informed that dependence on a particular disputed preamble phrase for antecedent basis may limit claim scope because it indicates a reliance on both the

preamble and claim body to define the claimed invention. I have further been informed that clear reliance on the preamble during prosecution to distinguish the claimed invention from the prior art transforms the preamble into a claim limitation because such reliance indicates use of the preamble to define, in part, the claimed invention.

IV. PERSON OF ORDINARY SKILL IN THE ART AND THE TIME OF THE ALLEGED INVENTION

46. I have been asked to assume that the '235 patent is entitled to its earliest alleged priority date of December 15, 2008. *See* Ex. 1001. Beyond this assumption, I have not undertaken an analysis to determine the earliest priority date to which the '235 patent is entitled.

47. Based on the materials and information I have reviewed and based on my experience in the technical areas relevant to the '235 patent, a person of ordinary skill in the art at the time of the alleged invention of the '235 patent would have had at least a Bachelor's degree in Electrical Engineering, Computer Engineering, Computer Science or equivalent, and at least two years of experience with computer networking technology. More education can supplement practical experience and vice versa. Based on my knowledge and experience, including as discussed above in Section II, I exceeded the level of skill of a person of ordinary skill in the art at the time of the alleged invention of the '235 patent and can provide opinions regarding the knowledge of a person of ordinary skill in the art as of that time. My opinions

herein are, where appropriate, based on my understandings as to a person of ordinary skill in the art at that time. I myself had more than these capabilities at the time of the alleged invention of the '235 patent.

V. THE '235 PATENT

A. Background of Technology

48. Below I provide a summary of the technology at issue, which is the updating of a base station's neighbor cell list.

49. Telecommunication networks enable the connection of user terminals, *e.g.*, mobile phones, personal computers, handheld devices, etc., to each other or other network resources and nodes.

50. As with any communication network, the security of transmissions is a high priority. Such security concerns include the avoidance of communication interception and authenticating terminals to ensure they are who they claim to be. Ultimately, the network must discern who is a legitimate user and who is a malicious actor, in order to prevent the latter from unauthorized access and transmission. A variety of tools are used to help maintain the integrity of the connection between a terminal and a network.

51. One traditional and well-known method for securing communication channels 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. Keys are used to encrypt communications, and telecommunication networks typically use symmetric cryptography wherein the same key is used to both encrypt and decrypt a message. Hence the need for both terminal and network to use the same key—but also not share that key to unauthorized parties.

52. 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 identity module

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.

53. Note that the two values can **only** match if the terminal and network used the same *RAND* and the same cryptographic key. This can mitigate attacks from malicious actor. For example, a malicious actor would not be able to pretend to be an authorized user, because the malicious actor will lack the necessary cryptographic key needed for generating the proper *RES* value.

B. Description of the '235 Patent's Specification

54. The '235 patent to Muller *et al.* was filed as a PCT application and claims priority to a European application filed December 15, 2008.

55. The '235 patent is titled “Service-based authentication to a network.” It is directed to a system for authenticating a terminal with a network node where the authentication response depends on whether the terminal and network node agree on the identity of the communication channel. Ex. 1001 at Abstract.

56. The '235 patent acknowledges that GSM uses AKA, but alleges that it is “vulnerable to so-called false base station attacks wherein an attacker pretends to

be a valid base station.” Ex. 1001, 1:35-41. The ’235 patent further acknowledges that GSM mitigates such attacks with “mutual authentication,” but that does not resolve “man-in-the-middle attacks, wherein a mobile device of an attacker may use authentication information from the (U)SIM of the victim in order to obtain access to the network” which “allows network access [by the malicious actor] as if the connection was set up by the victim.” Ex. 1001, 1:49-56.

57. The ’235 patent therefore claims to solve this issue by “allow[ing] the network to determine through which communication channel authentication information is transmitted to the network,” which is “*easily* achieved by identifying the communication interface through which the authentication request is received.” Ex. 1001, 1:63-2:19. The ’235 patent notes that this method is “compatible with all or at least most existing and proposed AKA’s,” as it “*only* requires determination of the communication channel through which the request was received and secure insertion of information regarding the communication channel into the response.” Ex. 1001, 2:20-24.

58. But as I discuss below, prior to the earliest priority date of the ’235 patent, the 3GPP had already proposed using AKA in this manner—where both terminal and network node identify the communication channel and use such identification in matching authentication responses.

C. The '235 Patent's Prosecution History

59. I have reviewed the prosecution history of the '235 patent and summarize it below.

60. 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. Ex. 1002, 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.

61. The examiner's first rejection relied on Naslund as anticipating claim 1. Ex. 1002, 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.*

62. In response, applicant did not contest that Naslund anticipated then-pending claim 1. The applicant's actions are consistent with the descriptions of the prior art in the '235 patent, which admit that the patent's only purported improvement over traditional AKA methods was the use of a "service code." Instead, applicant amended claim 1 by incorporating the "service code" 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.*

63. 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 argued 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.” Ex. 1002, 62.

64. 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. Ex. 1002, 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.*

65. 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.

66. However, as I discuss below in Ground 3, the examiner was incorrect that Naslund does not disclose a service code. 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.

D. Claim Construction

67. For the purposes of my analysis in this IPR proceeding, I understand that the words of a claim are given their plain meaning that those words would have had to a POSITA at the time of the alleged invention. I also understand that the structure of the claims, the specification, and the prosecution history may also be used to better construe a claim insofar as the plain meaning of the claims cannot be understood. Moreover, I understand that even treaties and dictionaries may be used, albeit under limited circumstances, to determine the meaning attributed by a POSITA to a claim term at the time of filing. Furthermore, I understand that a Patent

Owner's own apparent interpretation of certain terms in related proceedings can be considered to determine the meaning of patent claims in an IPR proceeding.

68. I have followed this approach in my analysis, and, except as explicitly stated below, I have applied the plain and ordinary meaning of those terms as they would have been interpreted by a POSITA at the time the invention was made (not today). For purposes of my analysis here, I have used December 15, 2008, the date of the European application to which the '235 patent claims priority, as the date of the invention.

69. I further note that Patent Owner had previously asserted the '235 patent in a litigation brought against Ericsson, *Koninklijke KPN N.V. v. Telefonaktiebolaget LM Ericsson, Ericsson Inc.*, No. 2:21-CV-00113-JRG (E.D. Tex. Mar. 16, 2022) ("Ericsson Litigation"). Prior to that case settling, the Court had construed certain terms of the '235 patent, although it appears that only claims 1, 4-7, and 11 were asserted. Ex. 1015. These terms are also discussed below.

1. "service code" / "expected service code"

70. In the Ericsson Litigation, the Court concluded that a "service code" is a coined term and therefore "cannot be construed broader than the disclosure in the specification." Ex. 1015, 63.

71. 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.” Ex. 1015, 64. For purposes of my analysis, I have applied this construction below. I do not otherwise provide any opinion on whether “service code” is a coined term that lacks a plain meaning.

2. “communication channel”

72. In the Ericsson Litigation, the Court declined to expressly construe this term and instead concluded it was have its plain meaning. Ex. 1015, 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. I have applied this understanding to my analysis below.

3. “authentication data request”

73. In the Ericsson Litigation, the Court did not expressly construe this term but instead concluded it should have its plain meaning. Ex. 1015, 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. I have applied its plain meaning below, which is a data request for authentication.

4. “service interface module”

74. This term was not at issue in the Ericsson Litigation, because it is only recited in claims 2, 8, and 10 which do not appear to have been asserted.

75. I understand that terms can be considered “means-plus-function” terms wherein the term recites a function but lacks a claimed structure and thus the term is limited to the structure described in the specification and their equivalents. I further understand that if a term has sufficient claimed structure, it is not a means-plus-function term. I also understand that terms that do not use the word “means” are presumed not to be means-plus-function terms, but that the term “module” is frequently construed as a “means-plus-function” term.

76. In my opinion, “service interface module” is not a means-plus-function term and should instead be given its plain meaning. I note the following. In claim 8, the term does not have a recited function. Instead, claim 8 recites a “service interface module” which comprises several structural elements, such as a “receiver,” a “channel identifier,” a “channel interface,” and a “modifier.” Thus, in my opinion, a POSITA would consider “service interface module” as recited in claim 8 to have sufficient claimed structure.

77. However, such structure is not claimed in claims 2 and 10, which instead recite that the “service interface module” is “configured to” “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.”

78. But it is my understanding that a claim term is to be construed consistently across claims of the same patent, and that there must be a clear indication in the specification or prosecution history that the same term in different claims mean different things. In my opinion, nothing in the specification or prosecution history indicates that “service interface module” has a different meaning in claim 8 versus claims 2 and 10. The specification does not make a distinction between “service interface modules.” Indeed, I note that claim 2 and 10’s function of “identify[ing] the communications channel” is actually recited in claim 8 as being performed by its channel identifier. This indicates to a POSITA that the terms have the same, consistent meaning. Thus, it is my opinion that the term is not a means-plus-function term and should be given its plain meaning.

79. However, if the Board is inclined to construe the term as a means-plus-function term, in my opinion, its recited function is “to identify the communications channel through which the authentication request was received” and its corresponding structure is 5:56-6:7, 7:45-54, or their equivalents.

5. “identity module”

80. The term “identity module” was also not at issue in the Ericsson Litigation. In my opinion, the term has a plain meaning and a well-understood

structure, and thus is not a means-plus-function. I understand that a term that is used in common parlance or has a conventional meaning among ordinary artisans that is understood to have structure cannot be a means-plus-function term. In my opinion, that is the case here.

81. An “identity module” has a well-understood meaning and structure. In particular, it includes such structures like a “Subscriber Identity Module (SIM),” which is found in the typical cellular device. An “identity module” can also include a UMTS SIM, or a USIM. Indeed, I note the ’235 patent itself concludes that an identity module includes SIM and USIM. Ex. 1001, 6:32-39. Thus, the term itself connotes sufficient structure to a POSITA.

82. I further note that the term lacks any recited function in claims 2 and 10, and while in claim 9 it “establish[es] a safe communication channel with a service interface module,” claim 9 also recites that it has several structural elements such as “a calculator” and a “modifier.” This gives further reason not to construe the term as a means-plus-function term.

VI. OVERVIEW OF THE PRIOR ART

A. TS-33.402 (Ex. 1006)

83. 3GPP Technical Specification 33.402 version 8.1.1 (“TS-33.402”) is directed to “security aspects of non-3GPP accesses.” 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.

84. 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 same CK' and IK' keys in order to check the received MAC and generate a response MAC.

1. TS-33.402 Was Published on October 14, 2008

85. In my opinion, TS-33.402 was published by at least October 2008 by the 3rd Generation Partnership Project, *i.e.* 3GPP. I have reviewed the declaration of Mr. Craig Bishop who worked as a Rapporteur² for 3GPP from 1998 to 2003. I am also familiar with 3GPP as an organization as well as its publication practices, and

² 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

agree with his description of 3GPP. 3GPP is a well-known standards organization tasked with developing protocols for mobile telecommunications. In my opinion, a POSITA would have been well-aware of their documents and publication practices.

86. 3GPP technical specifications, including TS-33.402, were generally uploaded to the 3GPP FTP server on the date indicated on the document, in this case, October 14, 2008. Ex. 1006, 1. The 3GPP website also lists TS-33.402 as being available October 14, 2008. Ex. 1007. In my opinion, the date of publication indicated on the document and as indicated on the 3GPP website were reliable indicators of the publication date of that document. It is also my opinion that, based on 3GPP's publication practices, the documents available on 3GPP's website as of today are true and correct copies of the documents on the day they were uploaded, unless indicated otherwise. This applies to TS-33.402.

87. Thus, it is my opinion that TS-33.402 was publicly accessible to a POSITA with reasonable diligence by October 14, 2008. It is also my opinion that Exhibit 1006 is a true and correct copy of TS-33.402 on or around the date it was first made publicly available.

2. Arkko Was Published on October 24, 2008

88. Related to TS-33.402 is the October 24, 2008 draft of what would eventually become RFC 5448 ("Arkko"). Ex. 1008. This draft proposes an update to the EAP-AKA authentication method called EAP-AKA'. 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.

89. Arkko was published on October 24, 2008 by the Internet Engineering Task Force ("IETF") and was published (and still is published) on the IETF's website. The October 24, 2008 date appears on the face of the document as well as the IETF website. Ex. 1008, Ex. 1009.

90. As I discussed above in my Background, I have had significant involvement with the IETF and am therefore familiar with their publication practices. Any ordinary artisan would likewise be familiar with the IETF's publication practices. 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.

91. A POSITA would have understood that since the 1990s, the IETF has published RFC's and drafts of such RFC's on its website as they became available. Such documents were generally drafted by a working group and then disseminated to the public for comments via the IETF website and an email announcement with a link to the document. As a result, it is my opinion that the publication date on the face of these documents is a reliable indicia of its public availability, and that a POSITA would be able to locate IETF documents with reasonable diligence by that

date. These dates are confirmed by the IETF website (<https://datatracker.ietf.org>) which lists the same dates of publication for each respective document.

92. I am also familiar with how IETF maintains the documents on its website. In my opinion, documents downloaded today reflect how they existed when they were first published, unless otherwise indicated. Thus, it is my opinion that Exhibit 1008 is a true and correct copy of Arkko on the date it was published, October 24, 2008.

B. Naslund (Ex. 1005)

93. WO 2004/032557A1 (“Naslund”) was published on April 15, 2004. 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.” Ex. 1005,

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.

VII. GROUNDS OF REJECTION³

A. Ground 1: TS-33.402 Alone or in View of Arkko Render Obvious Claims 1, 3-7, and 11-13

94. 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.

1. Claim 1

- (i) *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*

³ I am not aware of any secondary considerations of non-obviousness identified by Patent Owner. Nonetheless, in my opinion, none would overcome my opinions that each of the Challenged Claims is unpatentable, as explained throughout this Declaration. I reserve the right to address any purported secondary considerations of nonobviousness with respect to the '235 patent if Patent Owner later raises any.

communication channel with the network, the method comprising:

95. In my opinion, to the extent the preamble is limiting, it is disclosed by TS-33.402.

96. With respect to the limitation “***Method for service-based authentication of a terminal to a network,***” TS-33.402 discloses a method for service-based authentication of a UE, *i.e.* ***terminal***, to a network. Ex. 1006, 10 (“Access ***authentication*** for non-3GPP access in EPS shall be based on EAP-AKA”). As I discuss below, the authentication is ***service-based*** because it depends on properly identifying the communication channel of the authentication communications.

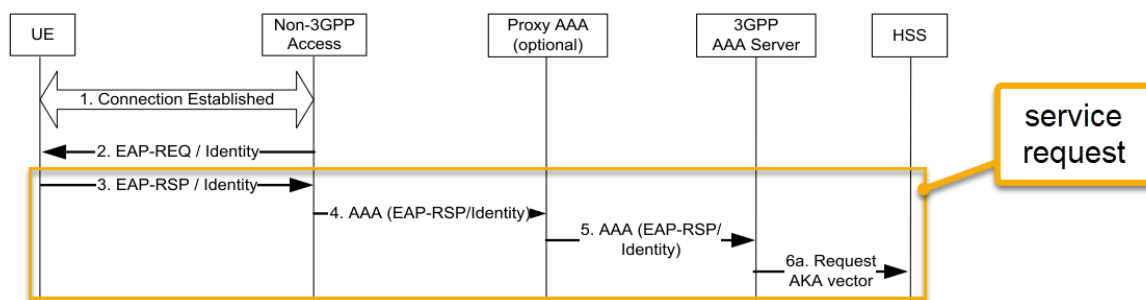
97. With respect to the limitation “***terminal comprising one or more communications interfaces for setting-up a communication channel with the network,***” TS-33.402 discloses a terminal capable of supporting 3GPP and non-3GPP access technologies for setting-up a communication channel with a network. Ex. 1006, 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.

(ii) 1[a]: the terminal sending a service request for access to a network service;

98. In my opinion, TS-33.402 discloses this limitation.

99. TS-33.402 discloses a “UE [i.e., **terminal**] send[ing] an EAP Response/Identity message [i.e., **service request**]” that “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.” Ex. 1006, 13. Figure 6.2-1 illustrates the steps comprising a service request sent from the terminal to the network. Ex. 1006, Fig. 6.2-1.

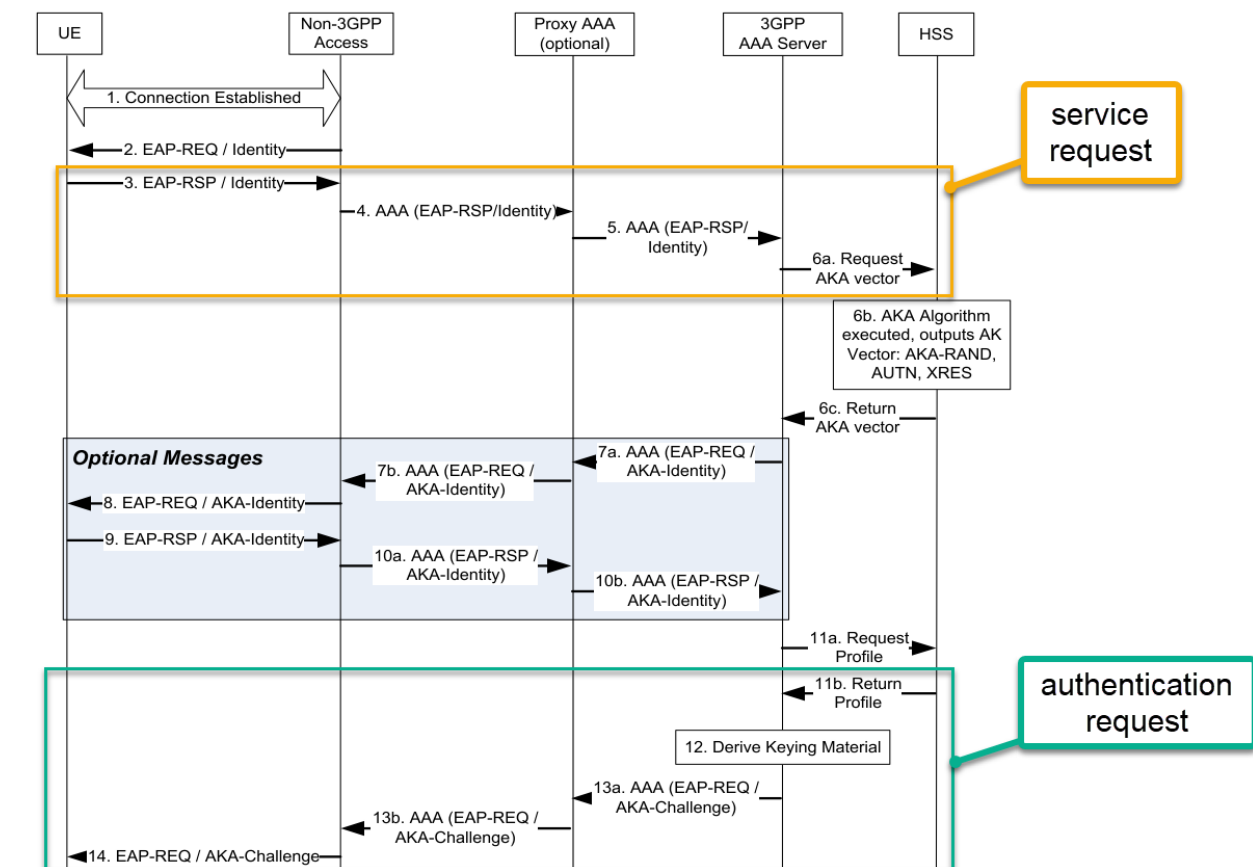


(iii) 1[b]: the terminal receiving in response to the service request an authentication request from the network;

100. In my opinion, TS-33.402 discloses this limitation.

101. 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 RAND, AUTN, a message authentication

code (MAC) ... to the authenticator in the access network in [the] EAP Request/AKA-Challenge message [i.e., **authentication request**] ... also includ[ing] the access network identity in this message,” after which “[t]he authenticator in the access **network** sends the EAP Request/AKA-Challenge message [i.e., **authentication request**] to the UE [i.e., **terminal**].” Ex. 1006, 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. Ex. 1006, Fig. 6.2-1.



- (iv) 1[c]: the terminal identifying the communication channel through which the authentication request was received;

102. In my opinion, TS-33.402 alone discloses. Alternatively, TS-33.402 in view of Arkko renders obvious this limitation.

103. 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.

104. In my opinion, such a disclosure in TS-33.402 is sufficient to establish that the “access network identity” identifies the communication channel. However, I note that an ordinary artisan would have also been aware Arkko’s descriptions of the “access network identity,” which would have informed the ordinary artisan’s understanding of TS-33.402’s disclosures.

105. In particular, Arkko explains that the access network identity is a “network name” “constructed as specified in [3GPP.24.302] for ‘Access Network Identity.’” Ex. 1008, 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.*

106. 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.*

107. Thus, in my opinion, A POSITA would have considered the “access network identity” described in TS-33.402 to be the same as that described in Arkko. This is made clear by the fact that 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”).

108. It is also my opinion that a POSITA would have considered it obvious combine TS-33.402 with Arkko's teachings with respect to the "network name." In fact, it is well-known 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 mere day after the earliest filing date of the '235 patent, December 15, 2008. Ex. 1010. Specifically, in the December 16, 2008 revision, TS-33.402 states that it would incorporate "EAP-AKA' as defined" in Arkko. Ex. 1010, 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 TS-33.402 (*i.e.* version 8.1.1, the October 14, 2008 version), where it states "[t]here is ongoing work at the IETF regarding the transport of the access network identity in EAP-AKA." Ex. 1006, 15.

109. Moreover, although TS-33.402 Version 8.2.0 was not published until a day after the earliest filing date of the '235 patent, the changes in that version were distributed to the group and considered at the November 10-14, 2008 3GPP SA3 Working Group meeting in Kyoto, Japan. Ex. 1011 ("Alignment of draft-arkko-eap-aka-kdf which defines EAP-AKA"); Ex. 1012 (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.

110. It is also my opinion that 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. 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. Ex. 1008, 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.” Ex. 1008, 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. 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. Ex. 1008, 7; *id.*, 20 (noting

that “[3GPP.24.302]” is “3GPP Draft Technical Specification 24.302 v 1.0.0, September 2008”).

- (v) *1[d]: the terminal determining a service code associated with the identified communication channel; and*

111. In my opinion, TS-33.402 alone discloses, or in view of Arkko renders obvious, this limitation.

112. As I discussed above in limitation 1[c], TS-33.402 discloses a terminal that determines an access network identity, which is a **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. The access network identity also **identifies the communication channel**, since it is the specific identifier for that particular access network. Ex. 1006, 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.” Ex. 1008, 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.

- (vi) *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.

113. In my opinion, TS-33.402 discloses this limitation.

114. With respect to the limitation ***“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 [the] EAP Response/AKA-Challenge [*i.e.*, ***authentication response***] containing [the] calculated RES and the new calculated MAC value to the authenticator in the access ***network***,” with “[t]he authenticator in the access network [subsequently] send[ing] the EAP Response/AKA-Challenge packet to 3GPP AAA Server.” Ex. 1006, 15.

115. With respect to the limitation ***“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***).

116. In particular, TS-33.402 teaches that 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***.

Ex. 1006, 16 (“(CK’, IK’) = F(CK, IK, <access network identity>)”), (“The access network identity ... is input to key derivation to obtain CK’, IK’”).

117. In addition, the response is generated using the authentication 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.” Ex. 1006, 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.* Therefore, 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.

118. With respect to the limitation “*thereby securely including information regarding the identified communication channel through which the authentication request was received into the response,*” as I discussed above, the calculation performed by the terminal, “(CK’, IK’) = F(CK, IK, <access network identity>,” is used to generate an authentication response. Ex. 1006, 15. CK’ and IK’ are encryption keys, as the function F “is a key derivation function” that is able to generate secure cryptographic values. Ex. 1006, 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. Ex. 1006, 14. Thus, the response can only be authenticated if both the terminal and server use the same access network identity. 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. Thus, the response **includes information regarding the identified communication channel.**

2. Claim 3

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

119. In my opinion, TS-33.402 discloses this limitation. TS-33.402 discloses that the authentication request includes “a message authentication code (MAC),” and thus the authentication request is **authentication information.** Ex. 1006, 15.

(ii) *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.*

120. In my opinion, TS-33.402 discloses this limitation.

121. As I 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.” Ex. 1006, 15. A POSITA would understand that the MAC is a keyed hash of the authentication request. Ex. 1008, 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.

122. 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*. A POSITA would understand that the entire purpose of the MAC, a “message authentication code,” is to allow the recipient (*i.e.* the terminal) to ensure the message is authentic and not altered. Thus, the keyed hash calculated by the terminal will only match the received MAC if the message was not altered. Thus, a POSITA would understand or at least consider it obvious not to generate an authentication response unless the MAC is confirmed to be correct. To do otherwise would eliminate the entire purpose of the MAC. TS-33.402 explains that if the MAC check fails, the “EAP AKA process will be terminated.” Ex. 1006, 16; *see also* Ex. 1008, 14 (explaining that if the MAC is incorrect, the terminal “fails the authentication”). This means no authentication response will be transmitted.

3. Claim 4

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

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

- (ii) *4[a]: the terminal generating the authentication response;*

124. As I discussed above in connection with limitation 1[e], TS-33.402 discloses a terminal generating the authentication response, EAP Response/AKA-Challenge.

- (iii) *4[b]: the terminal modifying the authentication response on the basis of the identified communications channel.*

125. TS-33.402 discloses modifying the authentication response by generating a MAC value. 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.” Ex. 1006, 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*. 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*. Ex. 1006, 15. Thus,

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

4. Claim 5

- (i) 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*;

126. In my opinion, TS-33.402 discloses this limitation.

127. As I discussed above in connection with 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.” Ex. 1006, 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*. Accordingly, the UE has *predetermined* the communications channel over which the service request will be transported.

- (ii) 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.

128. In my opinion, TS-33.402 alone discloses, or in view of Arkko renders obvious, these limitations.

129. 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.***

130. 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*. Ex. 1006, 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.* Because CK' and IK' are encryption keys, a POSITA would understand that the authentication vector is “transform[ed]” via encryption using those keys.

131. 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. See Ex. 1006, 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. If there is a mismatch, then the new keying material will not match and authentication fails.

132. TS-33.402 teaches that the authentication vector contains “XRES.” Ex. 1006, 32; *see also* Ex. 1016, 4 (“The authentication vector contains ... an ***expected result part XRES***”). The XRES value is used by the server to check the “received RES” sent in the UE’s authentication response. Ex. 1006, 15; 12 (“Verifies that AT-RES = XRES”). Thus, the authentication vector is ***an expected response***, and it is determined on the basis of the ***expected service code***.

133. Exhibit 1016 describes EAP-AKA and was publicly available by the IETF on January 2006, the date listed on the face of the publication and the IETF website. *See* Exhibit 1017. As I discussed above, such dates from the IETF are reliable indicia of their authenticity and public availability.

5. Claim 6

- (i) 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*

134. In my opinion, TS-33.402 discloses this limitation. As I discussed above in connection with 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. Ex. 1006, 13 (“Verifies that AT-RES = XRES”).

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

135. In my opinion, TS-33.402 discloses this limitation.

136. 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***). Ex. 1006, 15 (“The 3GPP AAA Server [*i.e.*, network] ***checks*** the received MAC and compares XRES to the 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.

6. **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.**

137. In my opinion, TS-33.402 discloses this limitation.

138. 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***. TS-33.402 is also specifically directed to “Security aspects of non-3GPP accesses,” and gives as an example “interworking between E-UTRAN and CDMA2000.” Ex.

1006, 1. E-UTRAN is a 3G cellular technology. *Id.*, 19 (“E-UTRAN is described in detail in TS 36.300”), 6 (“3GPP TS 36.300: ‘Evolved Universal Terrestrial **Radio Access** (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN); Overall description; Stage 2’.”).

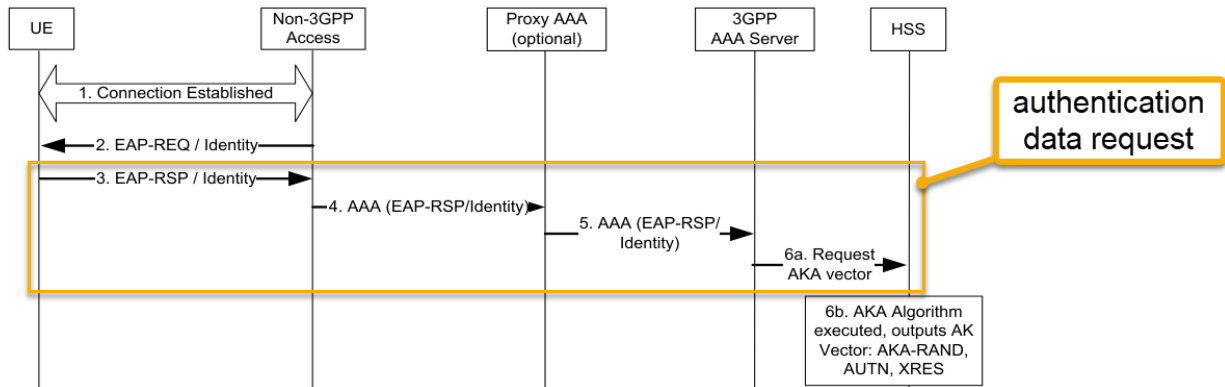
7. Claim 11

(i) 11[pre]: *A network node for service-based authentication of a terminal to a network, the network node comprising:*

139. As I discussed in limitations 1[pre] and 1[a], TS-33.402 discloses a network server that provides ***service-based authentication of a terminal to a network***.

(ii) 11[a]: *a receiver configured to receive an authentication data request;*

140. In my opinion, TS-33.402 discloses this limitation. As I discussed in limitation 1[a], the network server receives an “EAP Response/Identity message,” *i.e. an authentication data request*. Ex. 1006, 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. 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.*



(iii) 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

141. In my opinion, TS-33.402 discloses this limitation.

142. As I 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. Ex. 1006, 13. Accordingly, the 3GPP AAA Server, *i.e.* **first generator**, determines the access network identity.

(iv) 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.

143. In my opinion, TS-33.402 alone discloses, or in view of Arkko renders obvious, this limitation.

144. As I 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 $(CK', IK') = F(CK, IK, \langle \text{access network identity} \rangle)$.” Ex. 1006, 15. Because the transformation relies on the access network identity, the ***modification depends on the determined expected service code***.

8. Claim 12

(i) 12[pre]: A system for service based authentication to a network, comprising:

145. See 1[pre].

(ii) 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;

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

(iii) 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.

147. 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**). Ex. 1006, 15.

9. 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.

148. As I 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**.

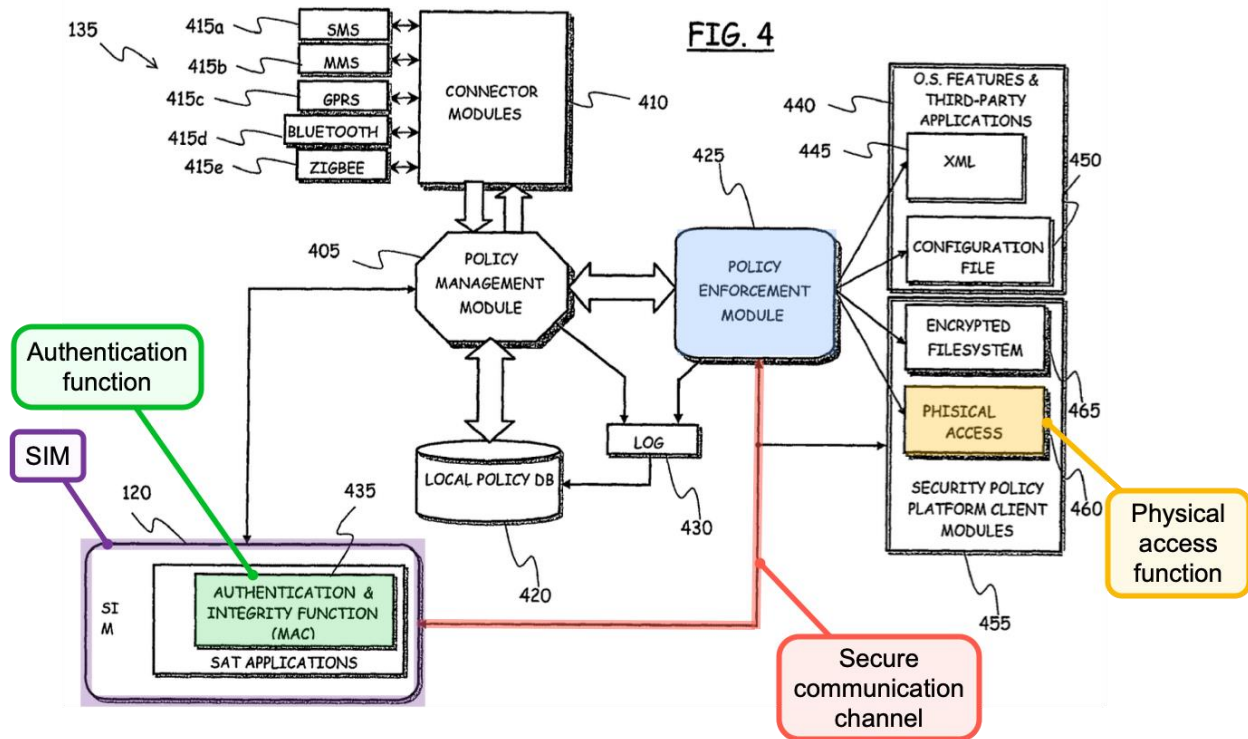
B. Ground 2: TS-33.402 (With or Without Arkko) in View of Aldera Render Obvious Claims 2, 8-10, and 13

149. 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.

1. Motivation to Combine

150. In my opinion, 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.

151. These teachings include Aldera's description of 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. Ex. 1014, 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]." Ex. 1014, 24:28-35.



152. Note that the policy enforcement module communicates with a SIM (*i.e. an identity module*) via a secure communication channel.

153. In my opinion, a POSITA would have found it obvious to combine TS-33.402 (alone or in view of Arkko) 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." Ex. 1006, 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.* Yet a POSITA would understand that hardware is a necessary component. 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.

154. Aldera also provides disclosures which a POSITA would find motivating. For example, Aldera states that the "policy management module" is desirable for "implementing and ensuring the enforcement of desired security

policies on the mobile communications devices.” Ex. 1014, 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. Increased security is, of course, a desirable and motivating feature to have. Thus, these teachings provide further motivation to incorporate Aldera’s teachings.

155. In my opinion, a POSITA would have had a reasonable expectation of success in the combination. Aldera provides significant detail regarding the implementation of its hardware components, which a POSITA would have no issue understanding. TS-33.402 also provides implementation details regarding its methods. Thus, implementation of TS-33.402 using Aldera’s components would therefore have been straightforward and within the skill of an ordinary artisan.

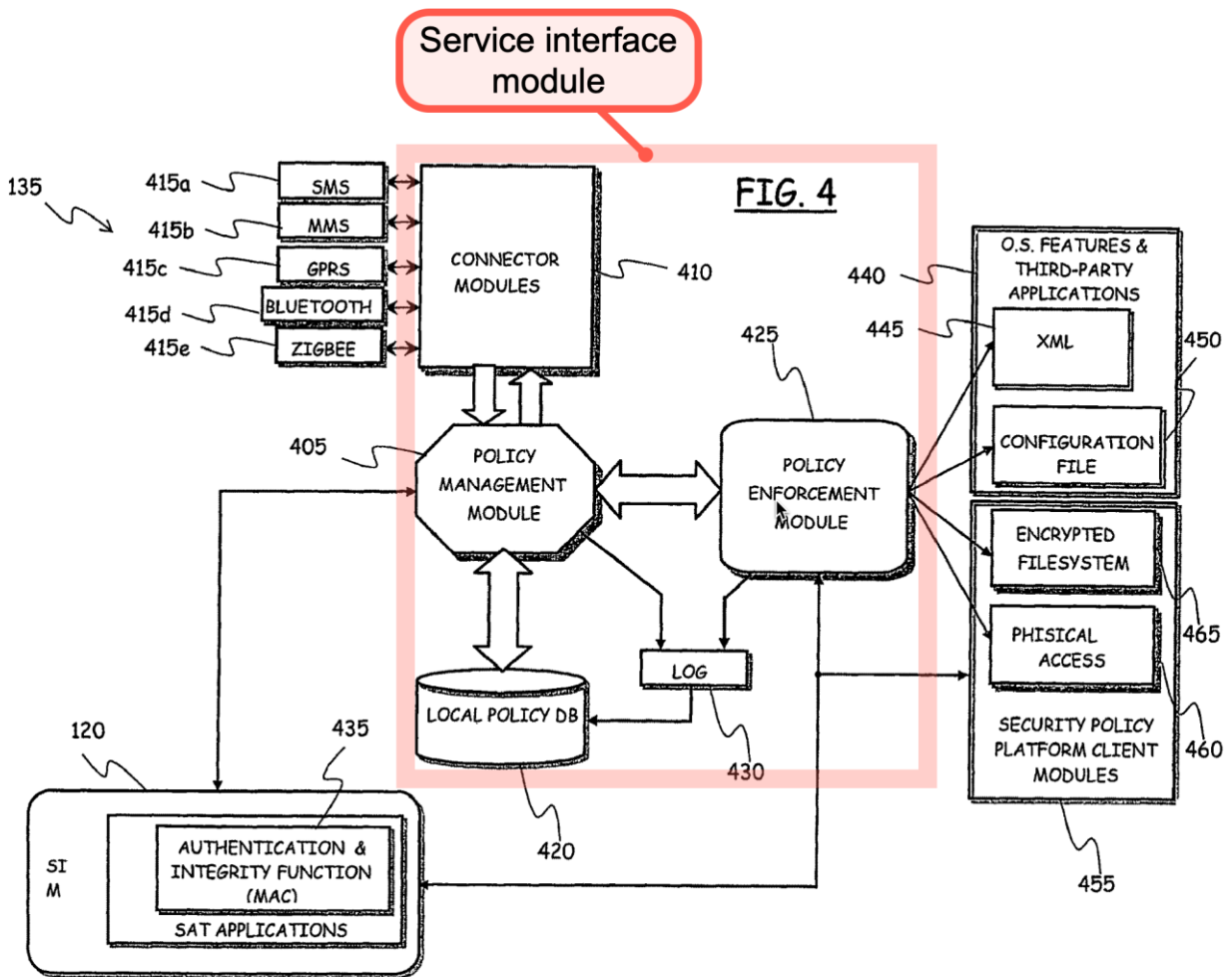
156. It is also my opinion that TS-33.402, Aldera and the ’235 patent are directed to the same field of endeavor, namely, authentication within a cellular network. Ex. 1001, Abstract (“A method and a system for service-based authentication of a terminal to a network is described.”); Ex. 1006, 6 (“The present document specifies the security architecture, i.e., the security feature groups and the security mechanisms performed during inter working between non-3GPP accesses and the Evolved Packet System (EPS).”); Ex. 1014, Abstract (“A system for enforcing security policies on mobile communications devices”).

2. Claim 8

- (i) *8[pre]: Service interface module for use in a terminal, the service interface module comprising:*

157. In my opinion, TS-33.402 in view of Aldera renders obvious this limitation, to the extent it is limiting.

158. 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.” Ex. 1014, 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**. Ex. 1014, 8:43-44. A schematic of the platform client (*i.e.*, **service interface module**) is shown below in Figure 4. Ex. 1014, 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. Ex. 1014, 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.



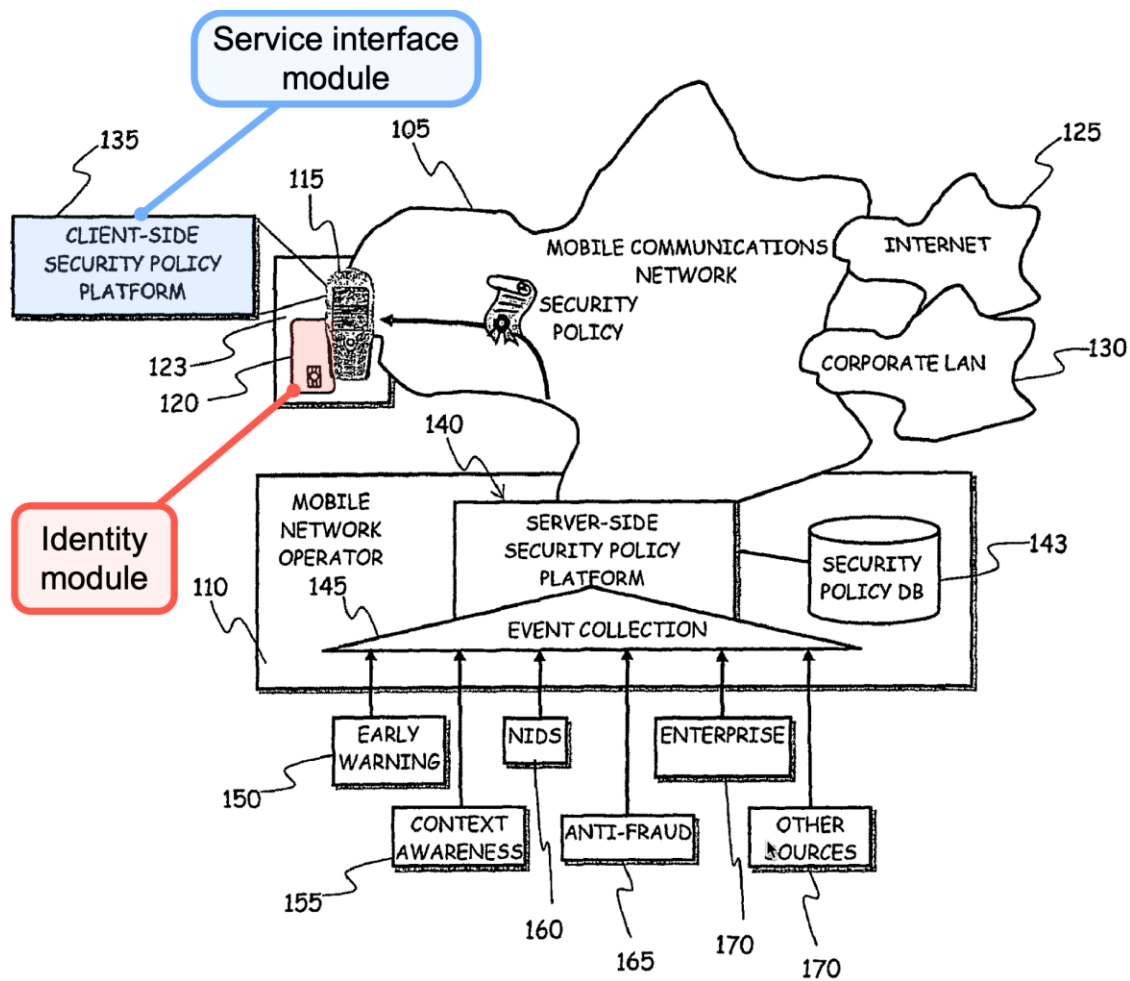


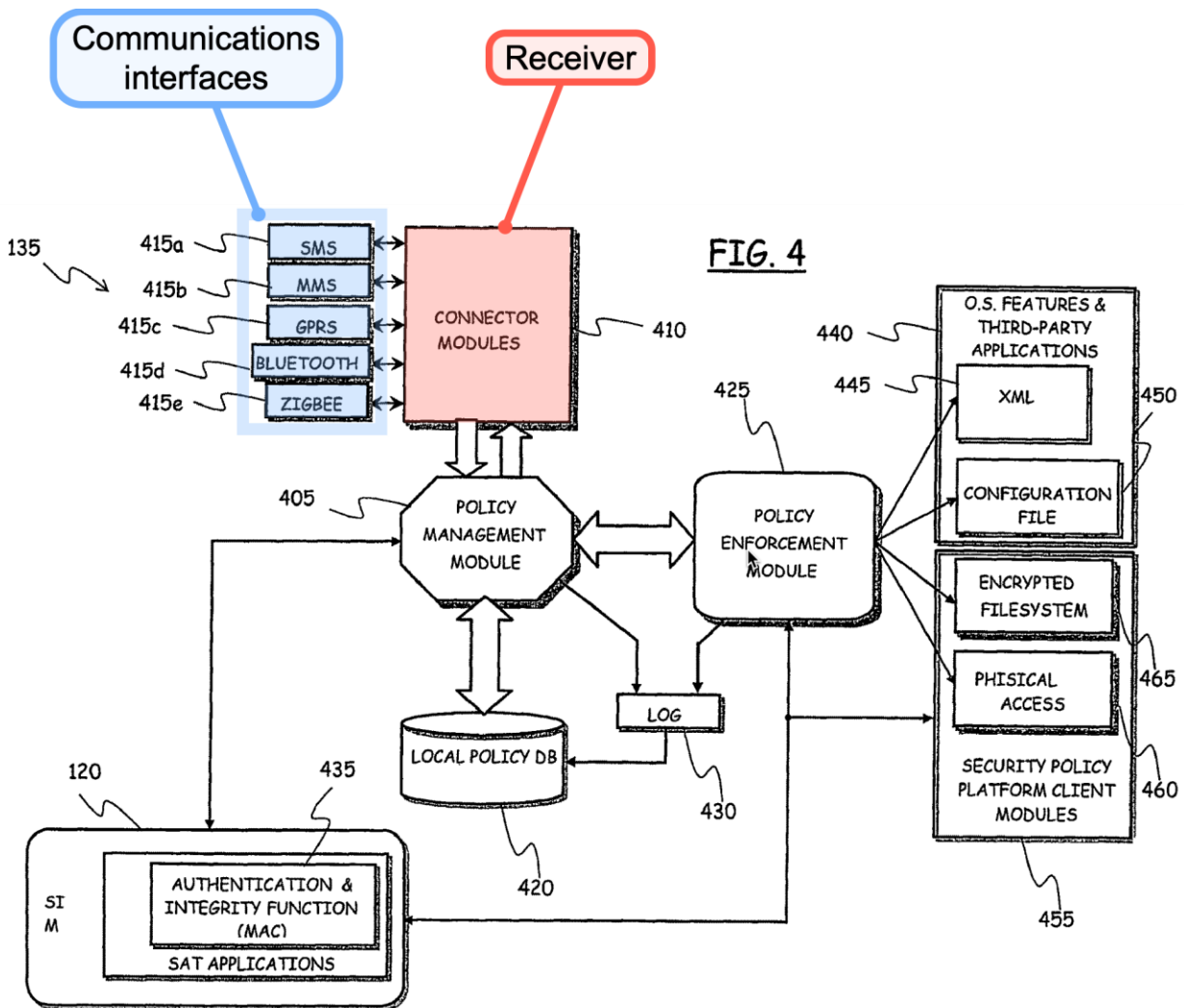
FIG. 1

159. As I noted above, in my opinion, “service interface module” should be given its plain meaning. However, if “service interface module” is construed as invoking §112(6), as I discussed above, it is my opinion its recited function is “to identify the communications channel through which the authentication request was received” and its corresponding structure is 5:56-6:7, 7:45-54, or their equivalents. Such structure includes a receiver and multiple interfaces. Aldera’s platform client has the same structures as I noted above.

- (ii) 8[a]: a receiver configured to receive an authentication signal from the network via one of the communications interfaces of the terminal;

160. In my opinion, TS-33.402 in view of Aldera renders obvious this limitation.

161. Aldera discloses a “connectors module 410 [*i.e.* **receiver**] to multiple **communication interfaces** 415a-415e **of the** mobile communication device [*i.e.*, **terminal**].” Ex. 1014, 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**. Ex. 1014, 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. Ex. 1014, 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. Ex. 1014, Fig. 4.



(iii) 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;

162. In my opinion, TS-33.402 in view of Aldera renders obvious this limitation.

163. As I 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.

164. And as I 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.

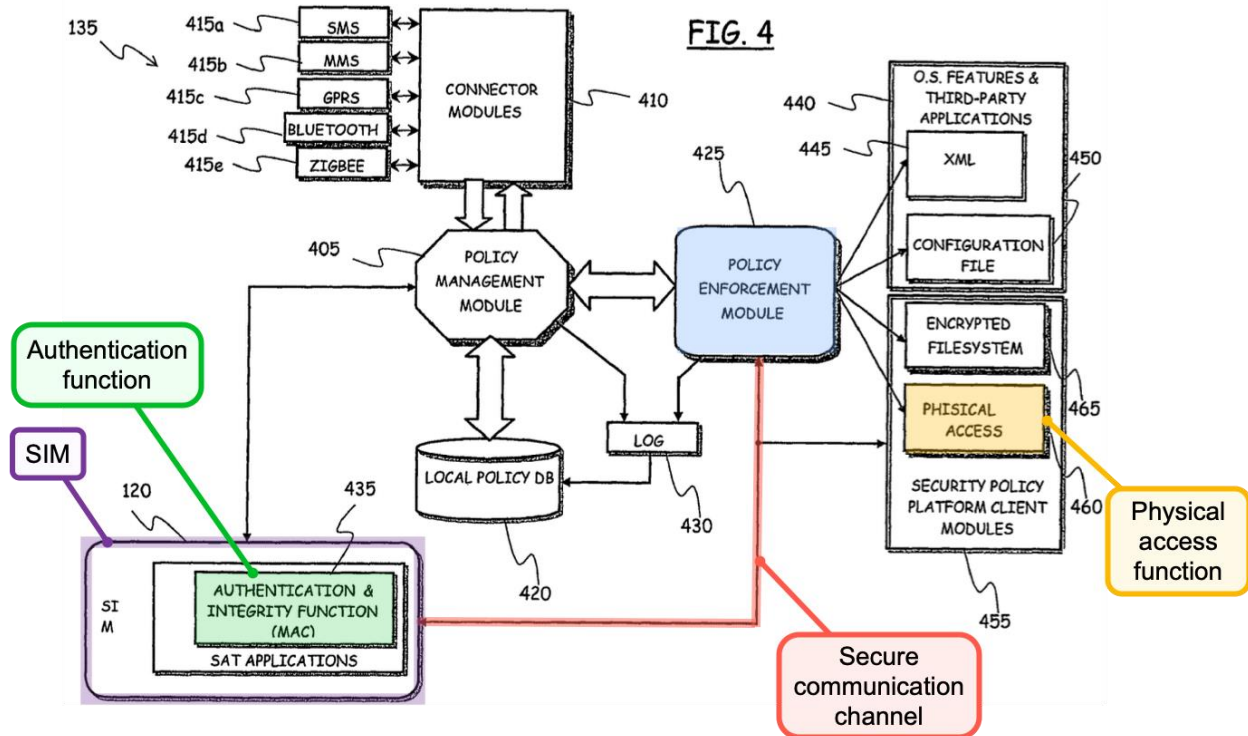
(iv) 8[c]: *a channel interface configured to establish a secure communication channel between the module and an identity module of the terminal; and*

165. In my opinion, TS-33.402 in view of Aldera renders obvious this limitation.

166. 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**].” Ex. 1014, 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].” Ex. 1014, 24:31-35. The

policy enforcement module is illustrated in Figure 4, shown below. Ex. 1014, Fig. 4.

167. 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**.” Ex. 1014, 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.” Ex. 1014, 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).



(v) 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.

168. In my opinion, TS-33.402 in view of Aldera renders obvious this limitation.

169. As I 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].” Ex. 1014, 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.” Ex. 1014, 24:66-25:8.

170. In addition, as I 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. As also discussed above, it would have been obvious to perform this function using Aldera’s encryption function 465 (i.e., *modifier*).

3. **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.**

171. In my opinion, TS-33.402 in view of Aldera renders obvious this limitation.

172. With respect to the limitation “*An identity module for establishing a safe communication channel with a service interface module as claimed in claim 8,*” as I 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.

173. With respect to the limitation ***“a calculator for calculating a response upon receipt of an authentication request,”*** as I 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.

174. With respect to the limitation ***“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. The keyed hash algorithm is the HMAC-SHA-256-128 algorithm, *i.e. a predetermined mathematical function*. Ex. 1008, 12.

4. Claim 10

- (i) *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:*

175. In my opinion, TS-33.402 in view of Aldera renders obvious this limitation.

176. With respect to the limitation “*[a] terminal for accessing network services,*” as I discussed above in connection with claim 8, Aldera discloses a terminal for accessing network services.

177. With respect to the limitation “*the 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. Ex. 1014, 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**].”).

178. With respect to the limitation “*the terminal comprising ... (ii) a service interface module configured to identify a communication channel through which*

an authentication request is received,” as I discussed above in connection with claim 8, TS-33.402 in view of Aldera renders obvious a terminal comprising a service interface module configured to identify a communication channel through which an authentication request is received.

(ii) *10[a]: receive an authentication request from the network;*

179. As discussed above in connection with limitation 8[a], TS-33.402 in view of Aldera renders obvious a terminal capable of receiving an authentication request from the communication network.

(iii) *10[b]: determine the communication channel through which the authentication request is received;*

180. As discussed above in connection with limitation 8[b], TS-33.402 in view of Aldera renders obvious a terminal capable of determining the communication channel through which the authentication request is received.

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

181. As discussed above in connection with limitation 8[c], TS-33.402 (alone or in view of Arkko) in further view of Aldera renders obvious a terminal capable of determining a service code associated with the communication channel through which the authentication request was received.

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

182. As discussed above in connection with limitation 8[d], TS-33.402 (alone or in view of Arkko) in further view of Aldera renders obvious a terminal capable of sending a response to an authentication request that depends on the determined service code.

5. 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.

183. In my opinion, TS-33.402 in view of Aldera renders obvious this limitation.

184. 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*].” Ex. 1014, 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.

6. 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.

185. As discussed in limitations 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.*

C. **Ground 3: Naslund Renders Obvious Claims 1-7**

186. 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.

1. **Claim 1**

(i) *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:*

187. In my opinion, to the extent the preamble is limiting, Naslund discloses this limitation.

188. With respect to the limitation “*[m]ethod for service-based authentication of a terminal to a network,*” 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.” Ex. 1005, 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*].” Ex. 1005, 21:2-3.

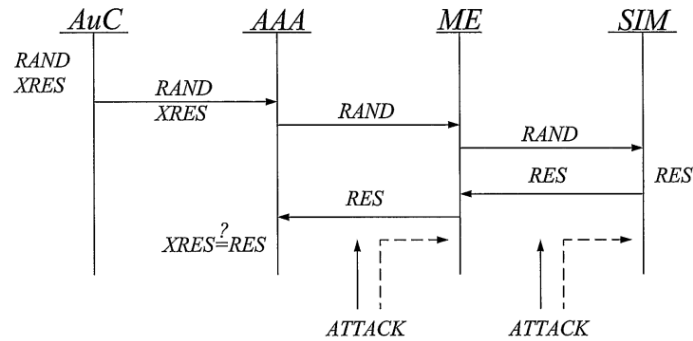
Thus, Naslund teaches that a terminal processes authentication requests based on the “network/operator identity,” *i.e.* ***based on a service.***

189. With respect to the limitation “***terminal 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.” Ex. 1005, 19:23-25. This “network interface” sets up a communication channel with a, for example, “GSM” or “UMTS” network. *Id.*, 19:9-10.

(ii) 1[a]: *the terminal sending a service request for access to a network service;*

190. Naslund discloses or renders obvious that the AKA authentication protocol is for “authenticat[ing] [a terminal] to ... ***services*** [such as] ***network access.***” Ex. 1005, 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.*** 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.

191. Figure 1 of Naslund depicts a typical AKA authentication protocol. Naslund uses protocol, but provides a version with additional steps to enhance security. Ex. 1005, 25:7-27. As Naslund explains (and as is well understood), 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." Ex. 1005, 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, because it is required for authenticating that user—the secret key can otherwise be used by a malicious actor to mimic the user. Ex. 1005, 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.



(Prior Art)

Fig. 1

192. 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. The network would not otherwise know that the user’s terminal needs to be authenticated.

193. I note that during prosecution, the applicant did not dispute that Naslund discloses this limitation. Ex. 1002, 99.

194. It is also my opinion that 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. 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. 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. 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.

(iii) 1[b]: *the terminal receiving in response to the service request an authentication request from the network;*

195. In my opinion, Naslund discloses this limitation

196. 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.” Ex. 1005, 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**. Ex. 1005, Fig. 11.

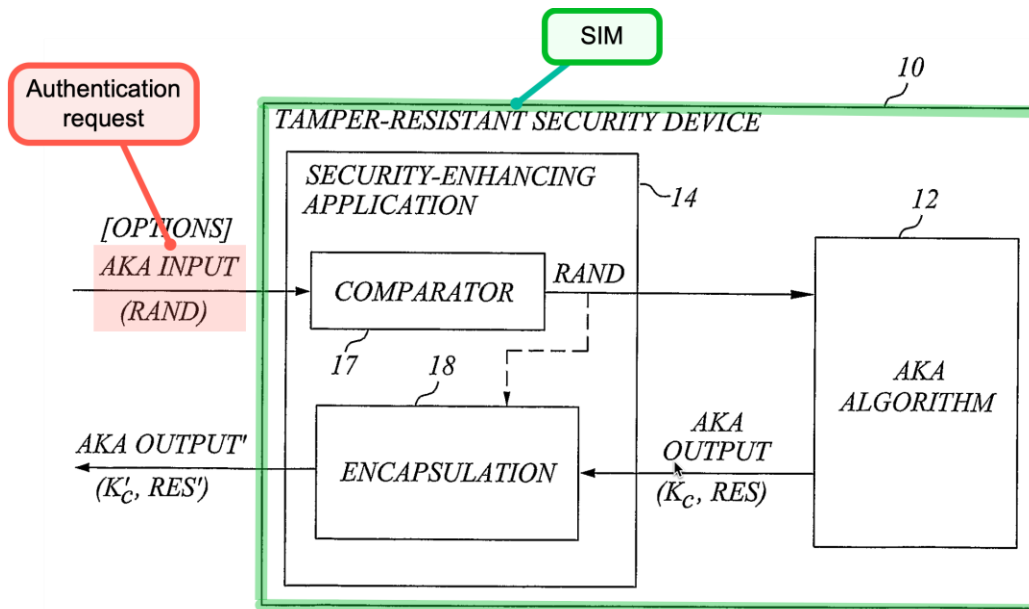


Fig. 11

- (iv) 1[c]: the terminal identifying the communication channel through which the authentication request was received;

197. In my opinion, Naslund discloses this limitation.

198. 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.).” Ex. 1005, 19:23-29.

(v) *1[d]: the terminal determining a service code associated with the identified communication channel; and*

199. In my opinion, Naslund discloses this limitation.

200. 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*.

201. 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.” Ex. 1005, 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**.

202. 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**. Ex. 1005, Table 1. Thus, in determining the sub application for processing, Naslund's system **determines a service code associated with the identified communication channel**. As can be seen, these codes **identify the communication channel** for the particular network/operator. 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

203. As I discussed above, the examiner overlooked these disclosures in Naslund. Although 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.” Ex. 1002, 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.”

204. It is my opinion that the examiner erred 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. 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. 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.”

- (vi) *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.

205. In my opinion, Naslund discloses this limitation. In sum, 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.

206. With respect to the limitation ***“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.” Ex. 1005, 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.

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

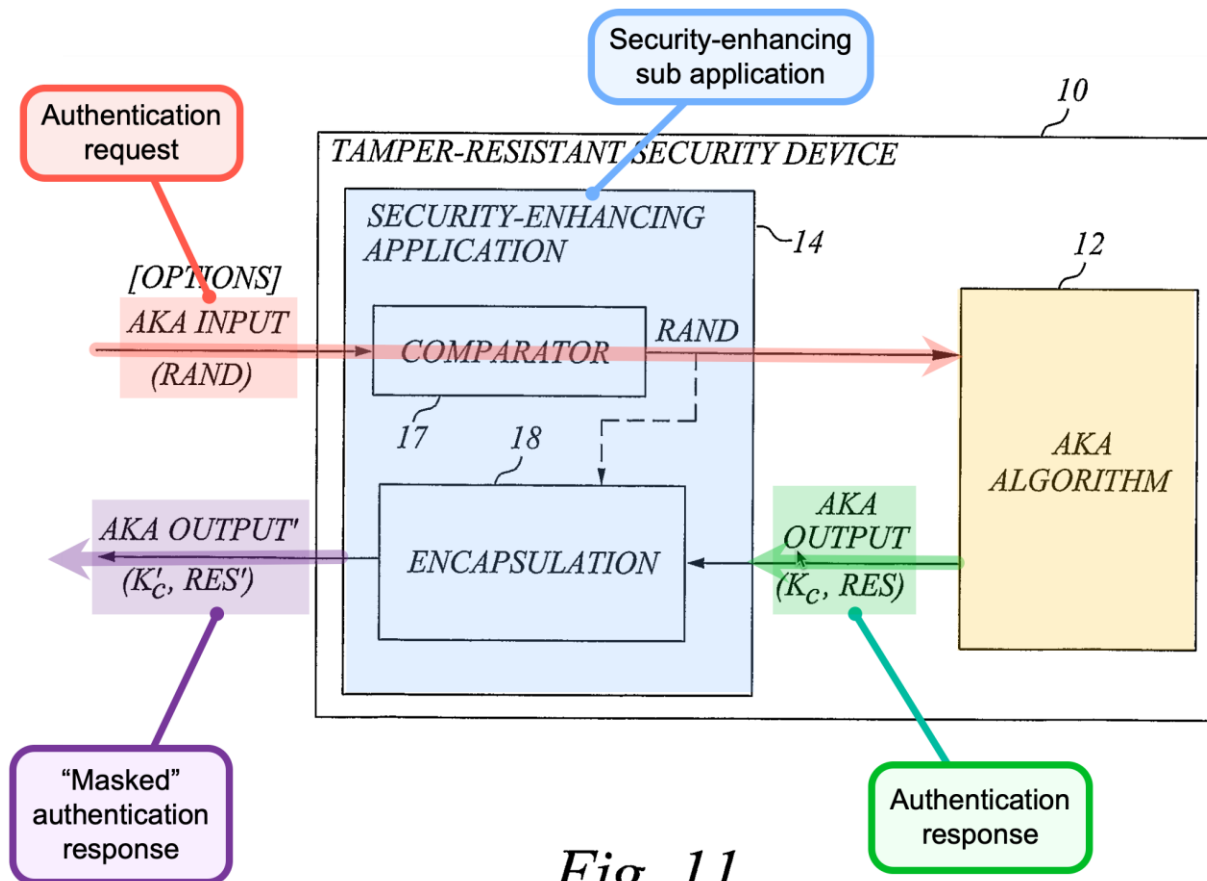


Fig. 11

208. With respect to the limitation *“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*. 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).” Ex. 1005, 14:26-28. As discussed in limitation 1[b], the challenge RAND is the **authentication request**.

209. 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.” Ex. 1005, 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.

210. With respect to the limitation “*thereby securely including information regarding the identified communication channel through which the authentication request was received into the response,*” Naslund discloses it. 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'. 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.

2. **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.

211. In my opinion, Naslund discloses or renders obvious this limitation.

212. 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). Ex. 1001, 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[.]" Ex. 1005, 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]." Ex. 1005, 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. Ex. 1005, 20:25-26; Ex. 1001, 6:32-48.

213. 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). Ex. 1001, 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.” Ex. 1001, 8:1-3.

214. 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**). Ex. 1005, Fig. 4.

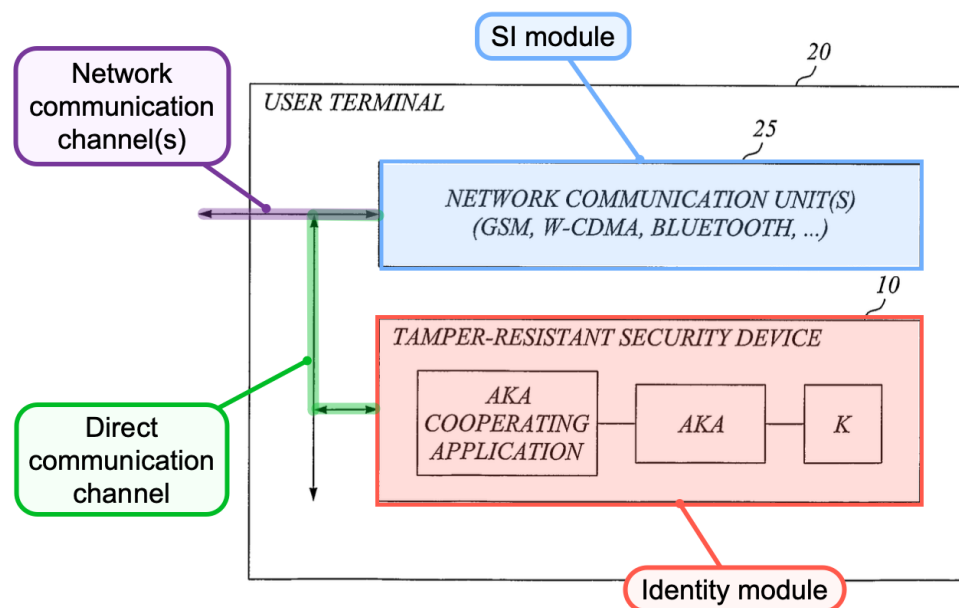


Fig. 4

3. Claim 3

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

215. In my opinion, Naslund discloses this limitation.

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

(ii) *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.*

217. 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.**” Ex. 1005, 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).

218. Separately, Naslund also teaches that “[t]he enhanced security processing may involve **manipulation of** output parameters and/or **input** parameters

of the AKA process.” Ex. 1005, 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*). Ex. 1005, Fig. 10. 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). Ex. 1005, Fig. 10.

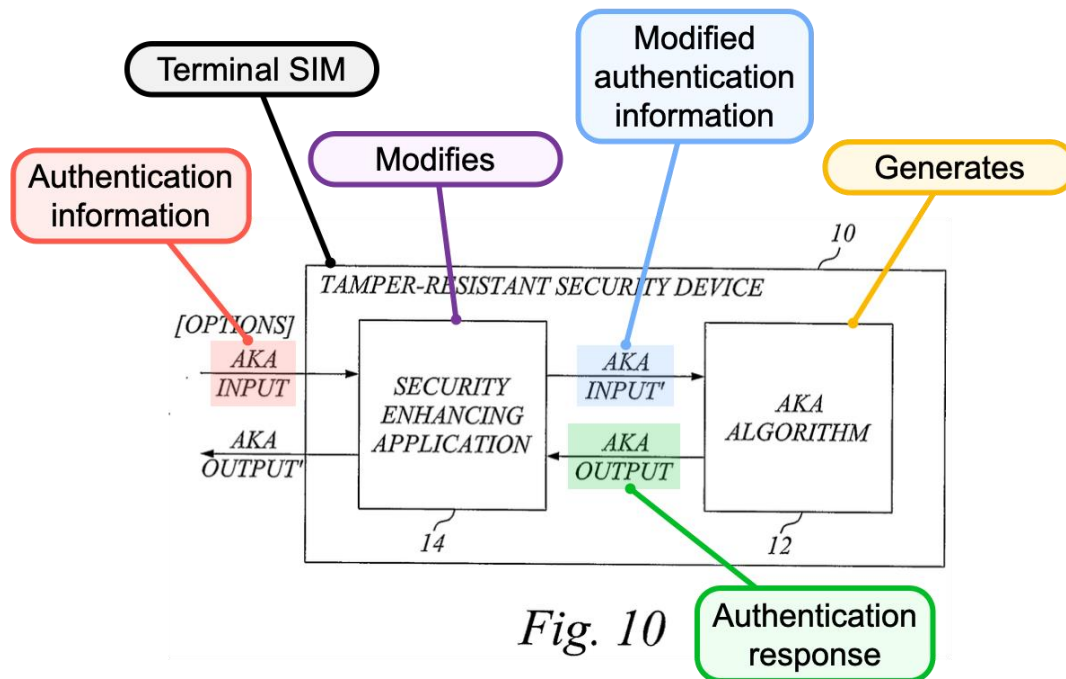


Fig. 10

4. Claim 4

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

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

- (ii) *4[a]: the terminal generating the authentication response;*

220. As discussed above in connection with limitation 3[a] (Section VII.C.3(ii)), Naslund discloses a terminal generating the authentication response.

- (iii) *4[b]: the terminal modifying the authentication response on the basis of the identified communications channel.*

221. 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**.” Ex. 1005, 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’. Ex. 1005, Fig. 10. 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'. Ex. 1005, Fig. 10.

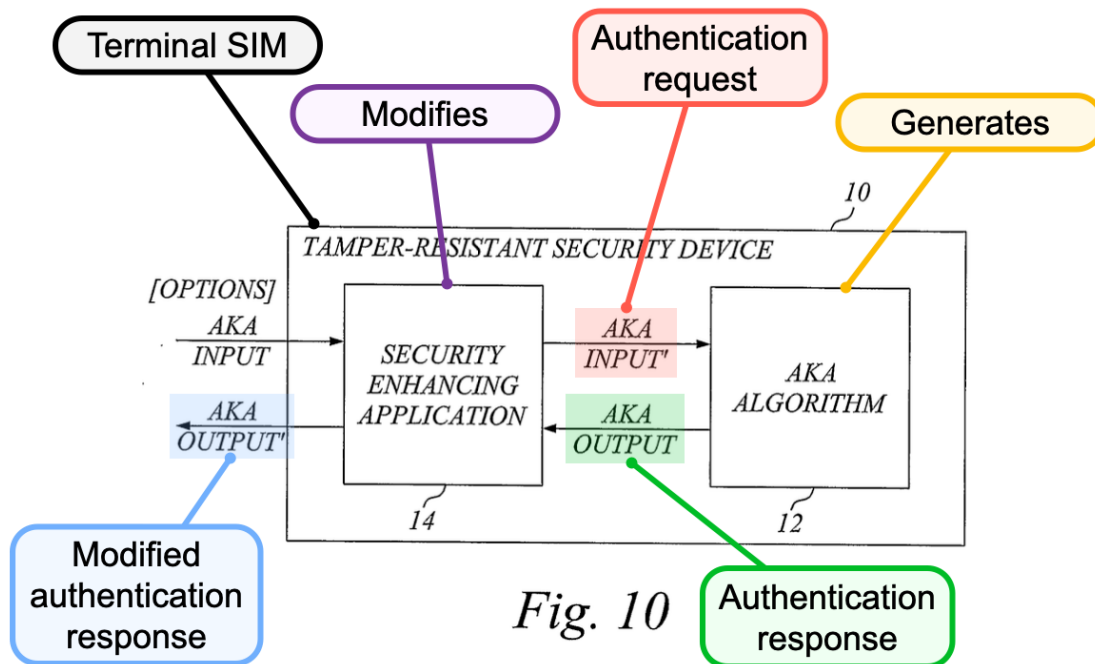


Fig. 10

5. Claim 5

- (i) 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;

222. In my opinion, Naslund discloses or renders obvious this limitation.

223. As discussed above in connection with 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].” Ex. 1005, 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. 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.

(ii) *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*

224. In my opinion, Naslund discloses or renders obvious this limitation.

225. 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].” Ex. 1005, 15:28-29. The network server and its components are illustrated below in Figure 6. Ex. 1005, Fig. 6.

226. 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. As discussed

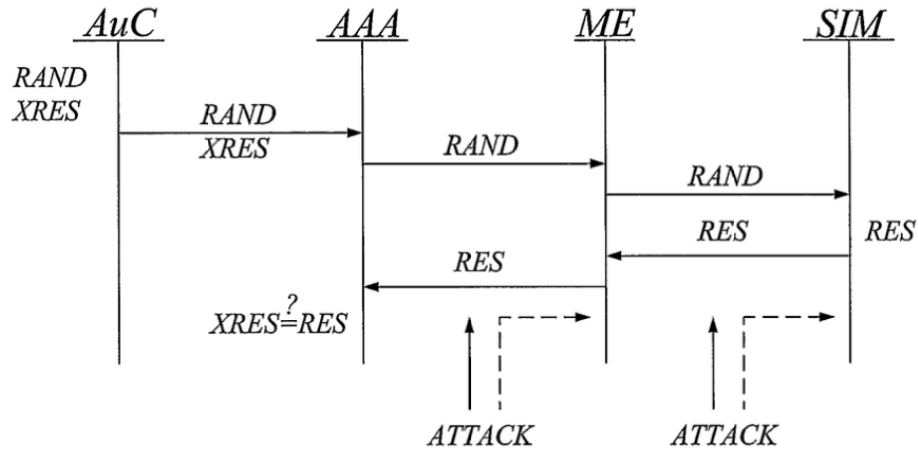
above in connection with limitations 1[d] and 1[e], Naslund discloses a terminal that (i) determines a service code associated with the specific communication channel through which an authentication request was received, and (ii) transmits to the network an authentication response that was calculated 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. 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. 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.

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

227. In my opinion, Naslund discloses or renders obvious this limitation.

228. 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. Ex. 1005, 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. Ex. 1005, 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.

229. Separately, Naslund also teaches the “encapsulation of sensitive parameters by manipulating AKA output parameters” to “produce a resulting higher-security response *RES'* [=] $h(\text{key}, \text{RES}(1), \dots, \text{RES}(n))$ ” where “the *n* responses are combined to a single response [*i.e.*, *RES'*] by a keyed function [*h*].” Ex. 1005, 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.



(Prior Art)

Fig. 1

6. Claim 6

- (i) 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

230. As I 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.

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

231. In my opinion, Naslund discloses this limitation.

232. 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.” Ex. 1005, 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***. 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. Ex. 1005, 1:10-13.

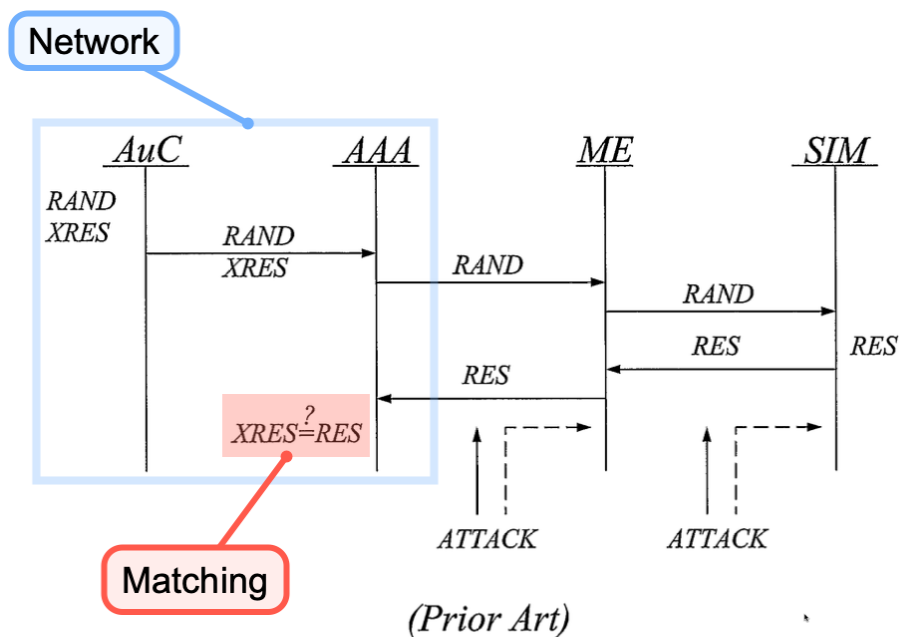


Fig. 1

7. **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.

233. 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. 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.

8. 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.

234. 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*.

VIII. CONCLUSION

235. I hereby declare that all statements made of my own knowledge are true and that all statements made on information and belief are believed to be true. I further declare that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both,

under Section 1001 of the Title 18 of the United States Code and that such willful false statements may jeopardize the validity of this proceeding.

Executed on this January 18, 2025 by:



Kevin C. Almeroth, Ph. D.