

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS AMERICA, INC.
SAMSUNG ELECTRONICS CO., LTD.,
Petitioner,

v.

KONINKLIJKE KPN N.V.,
Patent Owner

IPR2025-00512
Patent No. 8,881,235

EXPERT DECLARATION OF JACOB SHARONY, PH.D.

TABLE OF CONTENTS

I.	INTRODUCTION	5
II.	BACKGROUND AND QUALIFICATIONS	5
III.	UNDERSTANDING OF LEGAL STANDARDS.....	9
A.	Patentability	9
B.	Prior Art.....	14
C.	Inherency	15
D.	Person of Ordinary Skill In The Art.....	15
E.	Claim Construction.....	17
IV.	BASES FOR OPINIONS	18
V.	LEVEL OF ORDINARY SKILL IN THE ART	19
VI.	OPINIONS ON CLAIM CONSTRUCTION	21
VII.	OPINIONS ON CONCEPTION	22
VIII.	OPINIONS ON VALIDITY	34
A.	Ground 1	34
1.	Claim 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.”	34
1.	Claim 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.”	42
2.	Claim 4[b]: “the terminal modifying the authentication response on the basis of the identified communications channel.”	48
3.	Claim 5[c]: “determining on the basis of the expected service code an expected response.”	51
4.	Claim 6[a]: “comparing the expected response with the authentication response sent by the terminal to the network;”	57
5.	Claim 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.”	58
6.	Claim 12[a]: “...send in response to the authentication request a modified response to the network, wherein the modification depends on the determined service code;”	59
7.	Claim 12[b]: “a network node 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”	59
B.	Ground 2	59
1.	Claim 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.”	60
2.	Claim 9: “An identity module ... comprising ... a modifier for modifying the response on the basis of a predetermined mathematical function using a service code associated with the identified communication channel.”	62
3.	Claim 10[d]: “send in response to an authentication request a modified response to the network wherein the modification depends on the determined service code.”	63

C.	Ground 3.....	64
1.	Claim 1[d]: “the terminal determining a service code associated with the identified communication channel”	64
2.	Claim 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.”	69
3.	Claim 2: “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.”	72
4.	Claim 3[a]: “the terminal modifying the authentication information on the basis of the identified communications channel”	74
5.	Claim 4: “the terminal modifying the authentication response on the basis of the identified communications channel.”	75
6.	Claim 5[b]-[c]: “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 determining on the basis of the expected service code an expected response.”	75
IX.	CONCLUSION.....	76

I. INTRODUCTION

1. I have been retained as a technical expert by Koninklijke KPN N.V., (“Patent Owner”) and asked to provide my objective and unbiased opinions concerning U.S. Patent No. 8,881,235 (“the ’235 Patent”). Specifically, I have been asked to provide my opinions on the patentability of the ’235 Patent in view of certain prior art references, the state of the art at the time of the claimed invention, and the knowledge of a person of ordinary skill in the art at the time of the claimed inventions. I have also been asked to provide my opinions on the arguments set forth in a Petition for *Inter Partes* Review of the ’235 Patent in IPR2024-00512 (“Petition”), which was filed by Samsung Electronics America, Inc. and Samsung Electronics Co., Ltd (“Petitioner”).

II. BACKGROUND AND QUALIFICATIONS

2. In forming the opinions expressed in this Declaration, I have considered and relied upon my education, background, and experience. In addition, I have reviewed and relied upon additional materials in preparation of this Declaration, as described below.

3. My experience, qualifications and education are detailed in my curriculum vitae (“CV”), a copy of which is attached hereto as Appendix A. Some of my background and experience that qualifies me to offer the opinions in this Declaration are discussed further below.

4. I have over 35 years of experience working in the fields of information communication technologies (ICT), wireless networks, mobile devices and applications, and data capture and sensing, which has resulted in over 50 issued patents and numerous publications in scientific journals and conferences. I am a Life Senior Member of the Institute of Electrical and Electronic Engineers (IEEE). I have also served on various government expert panels, including for the National Science Foundation (NSF) and National Institutes of Health (NIH).

5. Since 2010, I have been an Adjunct Professor of Electrical Engineering at Columbia University, teaching graduate level courses on advanced wireless technologies including in the areas of wireless sensing and Auto ID technologies, mmWave communications, and applications for 5G wireless networks and systems.

6. I received a B.Sc. degree (1979) and M.Sc. degree (1984) in Electrical Engineering from Tel Aviv University, as well as M.Phil. (1991) and Ph.D. (1993) degrees in Electrical Engineering from Columbia University. I also have an M.B.A. degree (1989) from Tel Aviv University.

7. I have been involved with mobile and wireless networking technologies since the mid-1990s, and during my career have witnessed the change from voice-centric to data-centric networks. For nearly three decades, I have worked as a researcher, developer, and educator on wireless wide, local, and personal area

networks (WWAN, WLAN, and WPAN) infrastructure and mobile devices. I have also worked on enterprise mobility products and solutions since the late 1990s.

8. After obtaining my Ph.D., I led the advanced mobile networking group at BAE Systems, developing tactical mesh-based wireless network systems for the U.S. Department of Defense. I also conducted research and development in advanced mobile and wireless networks. My work resulted in several issued patents including U.S. Patent No. 5,652,751, titled “Architecture For Mobile Radio Networks With Dynamically Changing Topology Using Virtual Subnets,” and U.S. Patent No. 5,742,593, titled “On-line Distributed TDMA/FDMA/CDMA Link Assignment in Mobile Radio Networks With Flexible Directivity.”

9. From 1997 to 2005, I held various positions at Symbol Technologies (acquired by Motorola Solutions). While working at Symbol/Motorola, I gained substantial experience in application-specific mobile devices and wireless networking and architecture solutions in several vertical applications, *e.g.*, transportation and logistics, healthcare, warehousing, retail, and education. As Senior Director, Research and Development, I initiated and led several research and development programs in wireless LAN (local area network) technologies, including mobile device management and security. As Senior Director, Technology Strategy and Development, I was responsible for the research and development of new mobile applications for delivering multimedia-rich content to mobile devices connected

over heterogeneous networks. That work resulted in several U.S. patents, including U.S. Patent No. 7,778,649, titled “System and Method for Asset Location in Wireless Networks,” U.S. Patent No. 6,853,293, titled “Wearable Communication System,” U.S. Patent No. 7,039,358 titled “Coexistence Techniques in Wireless Networks,” U.S. Patent No. 6,925,094, titled “System and Method for Wireless Network Channel Management,” U.S. Patent No. 7,668,201 “Bandwidth management in wireless networks,” and U.S. Patent No. 7,426,383 “Wireless LAN intrusion detection based on location.”

10. In 2004, I founded Mobius Consulting, a consulting firm providing professional services in mobile wireless strategy, technologies, systems, and applications, including enterprise mobility, wireless communication networks, mobile embedded devices, device management, and mobile applications and services. In this capacity, I have worked with many companies in the mobile and wireless ecosystem including service providers and operators, equipment vendors, and semiconductor companies. Since founding Mobius Consulting, I have worked with many enterprises interested in deploying mobile and wireless solutions in order to become more productive, efficient, and cost effective. These solutions spanned numerous industry sectors and involved various mobile and wireless technologies including 3G/4G/5G Cellular, Wi-Fi, Bluetooth, ZigBee, and RFID. That work resulted in several U.S. patents, including U.S. Patent No. 9,014,702, titled

“Location Processing in Small Cells Implementing Multiple Air Interfaces,” U.S. Patent No. 9,088,923, titled “Small Cells Implementing Multiple Air Interfaces,” and U.S. Patent No. 10,080,177, titled “Unlicensed Spectrum Offload Architecture for Small-Cell Base Stations.”

III. Understanding of Legal Standards

11. I am not an attorney. For purposes of this Declaration, I have been informed about certain aspects of the law that are relevant to my opinions, as set forth below.

A. Patentability

12. I understand that for an invention claimed in a patent to be valid and patentable, it must be, among other things, new and not obvious in light of what was known and came before it. That which was known or came before the invention claimed is generally referred to as “prior art.”

13. I understand that there are two ways in which prior art may render a patent claim unpatentable. First, the prior art can be shown to “anticipate” the claim. Second, the prior art can show that the claim was obvious to a person of ordinary skill in the field of the invention at the time the invention was made.

14. I understand that, for a patent claim to be “anticipated” by the prior art, each and every element or requirement of the claim must be found, expressly or inherently, in a single prior art reference. Further, I understand that anticipation

requires that the single prior art reference must disclose the elements of the claim arranged or combined in the same way as in the claim.

15. It is my understanding that whether a claimed invention is obvious is a question of law, with underlying factual inquiries that are determined from the perspective of a person of ordinary skill in the art at the time of the claimed invention.

16. It is my understanding that a claimed invention is obvious if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art (a “POSITA”).

17. It is my understanding that obviousness requires consideration of the following underlying factual inquiries:

- determining the scope and content of the prior art
- ascertaining the differences between the claimed invention and the prior art;
- resolving the level of ordinary skill in the art; and
- evaluating objective evidence or “secondary considerations” of non-obviousness, such as commercial success, long-felt but unresolved needs, failure of others, industry praise, and unexpected results.

18. It is my understanding that a reference must be analogous art to the claimed invention in order to be properly considered for use in an obviousness

inquiry. It is my understanding that a reference is analogous art to the claimed invention if:

- the reference is from the same field of endeavor as the claimed invention (even if it addresses a different problem); or
- the reference is reasonably pertinent to the problem faced by the inventor (even if it is not in the same field of endeavor as the claimed invention).

19. It is my understanding that whether a reference is reasonably pertinent turns on how the problem faced by the inventor is reflected, either explicitly or implicitly, in the specification.

20. It is my understanding that the following are exemplary rationales that may support a conclusion of obviousness:

- Combining prior art elements according to known methods to yield predictable results;
- Simple substitution of one known element for another to obtain predictable results;
- Use of known techniques to improve a similar method or product in the same way;
- Applying a known technique to a known method or product ready for improvement to yield predictable results;
- Obvious to try – choosing from a finite number of identified,

predictable solutions, with a reasonable expectation of success;

- Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations are predictable to one of ordinary skill in the art; and
- Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

21. In addition to the above, I understand that a person of ordinary skill in the art may resort to logic, judgment and common sense available to him or her at the time of the invention to find a claim feature obvious, even if the prior art relied on does not explicitly state or teach that feature. I understand that when common sense is relied on to find a feature obvious, the reasoning for that conclusion must be articulated with sufficient clarity.

22. I also understand that a patent claim is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. An obviousness determination requires finding both that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so. I understand that it is important to be careful not to allow hindsight reconstruction of references to produce the claimed invention,

without any explanation as to how or why the references would be combined to produce the claimed invention.

23. Regarding “objective evidence” or “secondary considerations,” I understand that for such evidence to be relevant to the obviousness of a claim, there must be a causal relationship (called a “nexus”) between the claim and the evidence. I also understand that such objective evidence may include: commercial success of products covered by the patent claims; long-felt need for the invention; failed attempts by others to solve the problem addressed by the invention; copying of the invention by others in the field; unexpected results achieved by the invention; praise of the invention; the taking of licenses under the patent by others; expressions of surprise by experts and those skilled in the art at the making or use of the invention; and that the patentee proceeded contrary to the accepted wisdom of the prior art.

24. I understand that a person of ordinary skill is also a person of ordinary creativity. I further understand that the obviousness analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim, but instead can take into account “ordinary innovation” that does no more than yield predictable results, which are inferences and creative steps that a person of ordinary skill in the art would be understood to employ.

25. I understand that sometimes it will be necessary to look to interrelated teachings of multiple patents and publications; the effects of demands known to the

relevant field or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art. I understand that all these issues may be considered to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.

B. Prior Art

26. I understand that for purposes of this proceeding, prior art includes patents and printed publications in or outside the United States before the effective filing date of the claimed invention. I also understand that prior art includes U.S. patents, published U.S. patent applications, and published international applications (pursuant to the Patent Cooperation Treaty) that themselves have an effective filing date before the effective filing date of the claimed invention, as long as they name another inventor.

27. I also understand that prior art may include any public disclosure, including any products in public use, on sale, or otherwise available to the public, before the effective filing date of the claimed invention. I understand that information that constitutes prior art generally must be information that was publicly disclosed before the effective filing date of the claimed invention. I understand that there may be exceptions to what is prior art but have been instructed that they are not relevant for purposes of my opinions here.

C. Inherency

28. I understand that if a prior art reference does not expressly set forth a particular claim element, the prior art may still disclose that element if it is “inherent” in its disclosure. To establish inherency, it is my understanding that evidence must make clear that the missing descriptive matter is necessarily present in the thing described in the reference. It is my understanding that inherency may not be established by probabilities or possibilities. In other words, it is my understanding that the mere fact that a certain thing may result from a given set of circumstances is not sufficient to establish inherency.

29. I understand that under the principles of inherency, if a prior art device, in its normal and usual operation, would necessarily perform a claimed method, then the method will be considered to be anticipated by the prior art device. I also understand that when the prior art device is the same as a device described in the specification for carrying out the claimed method, it can be assumed the device will inherently perform the claimed process.

D. Person of Ordinary Skill In The Art

30. I understand that “a person of ordinary skill in the art” or POSITA is a hypothetical person who is presumed to have known the relevant art at the time of the invention. I understand that the term “person having ordinary skill in the art” or POSITA is sometimes used synonymously. Such a person would necessarily have

the capability of understanding any scientific and engineering principles applicable to the pertinent art.

31. I understand that factors that may be considered in determining the level of ordinary skill in the art include, but are not limited to, the following:

- a. the educational level of the inventor;
- b. the type of problems encountered in the art;
- c. prior art solutions to those problems;
- d. the rapidity with which innovations are made;
- e. the sophistication of the technology; and
- f. the educational level of active workers in the field.

32. I understand that a person of ordinary skill in the art is not a real person, but rather is a hypothetical individual having the qualities reflected by the factors above. This hypothetical person has knowledge of all prior art in the relevant field as if it were arranged on a workshop wall and takes from each reference what it would teach to a person of ordinary skill in the art.

33. I understand that a person of ordinary skill in the art is a person of ordinary creativity, not an automaton. In many cases a person of ordinary skill will be able to fit the teachings of multiple prior art references together like pieces of a puzzle.

34. I understand that a person of ordinary skill in the art can collaborate with one or more other persons of ordinary skill in the art for one or more aspects with which the other person may have superior expertise, experience, and/or knowledge.

E. Claim Construction

35. It is my understanding that claim construction, or the interpretation of the claims of a patent, is ultimately a question of law. I have been informed that claim terms are generally presumed to carry their ordinary and customary meaning. However, I understand that a patent applicant is his own lexicographer and is entitled to provide alternate definitions of words in common usage, but if the patent applicant uses a term that is in common usage without providing an alternate definition, then that term should generally be understood as having its common meaning.

36. I understand that a person of ordinary skill in the art is deemed to read a claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent specification and the “file history” of the patent developed during examination by the Patent Office.

37. I understand that the claims, the specification, and the file history are referred to as “intrinsic evidence,” and are to be read as a person of ordinary skill in the art at the time of the invention would have done at the time of the alleged invention.

38. In addition to the intrinsic evidence, I understand that the court or tribunal may also consider other relevant evidence, which is called “extrinsic evidence,” concerning relevant scientific principles, the meaning of technical terms, and the state of the art. Such evidence includes the testimony of expert witnesses. Although extrinsic evidence may be used to resolve ambiguities that may exist after reviewing the intrinsic evidence, I understand that extrinsic evidence cannot be used to contradict a claim construction that is clear from the intrinsic evidence.

39. I understand that some claims are independent, and that those independent claims are complete by themselves. Other claims refer to these independent claims, or other dependent claims, and are “dependent” on those claims. The dependent claims include all of the limitations of the claims on which they depend.

IV. BASES FOR OPINIONS

40. The opinions set forth in this Declaration are my own. In forming the opinions herein, I have considered the exhibits to the Petition for *Inter Partes Review* filed against the ’235 Patent, as well as the additional materials cited in this

Declaration (including exhibits to the Patent Owner's Preliminary Response cited herein), and my education, training, and experience.¹

41. My analysis of the materials relating to this matter is ongoing and I will continue to review any new material that is provided to me. This Declaration represents certain opinions that I have formed to date and the bases for those opinions. I reserve the right to revise, supplement, and/or amend my opinions based on new information presented to me and on my continuing analysis of the materials cited herein or later provided to me.

V. LEVEL OF ORDINARY SKILL IN THE ART

42. I have not been asked to provide an opinion on the level of ordinary skill in the art at the time of the invention. For purposes of this Declaration only, I

¹ Exhibit 2003 referenced in my declaration is a copy of 3GPP TS 33.102 V8.0.0 (2008-10), Release 8, October 23, 2008. This exhibit is a true and correct copy of that document as published by ETSI at https://www.etsi.org/deliver/etsi_ts/133100_133199/133102/08.00.00_60/ts_133102v080000p.pdf. Further, an expert in my field would reasonably rely on the facts or data set forth in this document in forming the opinions provided here. I am not aware of any information or reason to doubt the accuracy or truth of the contents of this document.

have instead been asked by Patent Owner to apply the definition of a person having ordinary skill in the art (“POSITA”) proposed by Petitioner:

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

Petitioners’ expert exceeded this definition by the priority date....

Petition, 6.

43. My experience and qualifications meet and/or exceed that of a POSITA as described in Section II above. My education combined with my substantial experience designing, developing, and/or testing telecommunication systems, and my familiarity with wireless standards and protocols related to data transmission and network management, qualifies me to provide an expert opinion as to the understanding of a POSITA.

44. All references to a POSITA here are made pursuant to the definition above. However, my application of that definition is not a reflection of my agreement or disagreement with it. I reserve the right to provide my own opinion on the level of ordinary skill should a trial be instituted in this proceeding. Moreover, my opinions herein would not change if the level of ordinary skill in the art was

determined as of December 15, 2008, which is the earliest priority date listed on the '235 Patent.

VI. OPINIONS ON CLAIM CONSTRUCTION

45. I understand that a district court previously construed the claimed “service code” to be a “code that identifies a communication channel” and “expected service code” to be an “expected code that identifies a communication channel.” Ex. 1015, 64. I also understand that Petitioner proposes that no terms require construction for purposes of these proceedings and purports to apply the “plain and ordinary meaning” as understood by a POSITA at the time of the invention. Pet., 10-15.

46. As the express construction of the claims terms is not necessary to address the assertions made in the Petition based on the information I have at this time, I do not currently provide any opinion at this time on whether Petitioner’s proposed constructions, or the prior construction of the district court, are accurate. My references to Petitioner’s constructions should not be taken as endorsements of those constructions. I reserve the right to provide constructions of any of the claim terms should a trial be instituted.

47. Here, I have been asked to apply the plain and ordinary meaning of the claim terms as understood by a POSITA.

VII. OPINIONS ON CONCEPTION

48. I have been asked to review an October 8, 2008 draft of the European Patent Application No. 08021705 (“EP Application”), which the ‘235 Patent claims priority to on the cover page. Ex. 1001, 1. Specifically, I have been asked to review the text of the written description of the draft EP Application (Exhibit 2014) and the figures of the draft EP Application (Exhibit 2015) to determine whether a POSITA would understand the draft EP Application to provide support for the challenged claims of the ‘235 Patent. It is my opinion that the draft EP Application provides support for all challenged claims, as reflected in my analysis below showing where and how each claim limitation corresponds to the disclosures of the draft EP Application. I use the same claim nomenclature as set forth in Petitioner’s list of challenged claims (PDF pages 13-18 of Petition).

'235 Patent		Conception Evidence
Claim	Limitation	
1[pre]	Method for service-based authentication of a terminal to a network, the terminal comprising one or more communications interfaces for setting-up a communication channel with the network, the method comprising:	“a method for service-based authentication of a terminal to a network wherein the terminal comprises a number of communications interfaces, each communications interface allowing the terminal to set-up a predetermined communication channel with the network.” Ex. 2014, 2:15-20.

1[a]	the terminal sending a service request for access to a network service;	“sending a service request for access to a network service;” <i>Id.</i> , 2:20-21.
1[b]	the terminal receiving in response to the service request an authentication request from the network;	“receiving in response to the service request an authentication request from the network;” <i>Id.</i> , 2:21-23.
1[c]	the terminal identifying the communication channel through which the authentication request was received;	“identifying the communication channel through which the authentication request was received;” <i>Id.</i> , 2:23-24.
1[d]	the terminal determining a service code associated with the identified communication channel; and	“determining a service code associated with the identified communication channel;” <i>Id.</i> , 2:34-36.
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.	“sending an authentication response RES to the network, wherein the authentication response depends on the identified communication channel.” <i>Id.</i> , 2:24-27. “calculating the response RES on the basis of the information in the authentication request and the service code, thereby encrypting information regarding identity of the communication channel through which the authentication request was received into the response.” <i>Id.</i> , 2:36-3:2.
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	“the terminal comprises an identity module ... and a radio module comprising a number of communications interfaces and configured to identify the communications channel

	channel through which the authentication request was received.	through which the authentication request was received. ... Preferably, the radio module comprises one or more trusted module allowing the service code to be sent to the identity module, e.g. a (U)SIM, in a secure way.” <i>Id.</i>, 3:8-20. While the draft EP Application does not use the term “service interface (SI) module,” the term “radio module” (including the “trusted module”) in the passage above is characterized in the same manner as the service interface module in the specification of the ’235 Patent. <i>See</i> Ex. 1001, 2:39-44 (“In another embodiment the terminal used in the method comprises an identity module and a service interface (SI) module, the SI preferably implemented as a trusted hardware module...”). In other words, the ’235 Patent teaches that SI module may be a “trusted hardware module.” A POSITA would thus understand that the “radio module” in the passage above qualifies or includes a “service interface (SI) module” as claimed, at least because the radio module comprises a trusted hardware module for allowing for “secure” communication with the U(SIM).
--	---	--

3[pre]	Method according to claim 1, wherein the authentication request comprises authentication information the method further comprising the steps of:	“the authentication request comprises authentication information, preferably a random challenge RAND” Ex. 2014, 3:28-30.
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.	“modifying the authentication information one [<i>sic</i>] the basis of the identified communications channel; generating ... an authentication response RES on the basis of the modified authentication information.” <i>Id.</i> , 3:31-36.
4[pre]	Method according to claim 1, wherein the authentication request comprises authentication information, the method further comprising:	“the authentication request comprises authentication information, preferably a random challenge RAND....” <i>Id.</i> , 3:36-38.
4[a]	the terminal generating the authentication response;	“generating ... an authentication response RES;” <i>Id.</i> , 4:1-4.
4[b]	the terminal modifying the authentication response on the basis of the identified communications channel.	“modifying the authentication parameter RES on the basis the identified communications channel.” <i>Id.</i> , 4:4-6.
5[pre]	Method according to claim 1, the method further comprising:	
5[a]	the terminal sending a service request via a predetermined communications channel to the network;	“the terminal comprises a number of communications interfaces, each communications interface allowing the terminal to set-up a predetermined communication channel with the network. The method comprises the steps of: sending a service request for access to a network service;” <i>Id.</i> , 22:1-10; <i>see also id.</i> , 4:19-22, 17:6-8.

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	“In response, the AuC/HLR generates a UMTS authentication vector AV and determines through which service interface (UMTS, GSM, WiFi, Bluetooth, etc.) contact was established with the terminal.... The identified service interface information is forwarded to the SIU, which determines on the basis of the information on the identified service interface an expected service code XSC (step 304). The SIU may determine XSC by retrieving the service code associated with the identified service interface (in this case a UMTS service) from a look-up table – substantially identical to the one used in the terminal – which is stored in a secure memory of the AuC/HLR.” <i>Id.</i> , 13:11-23; <i>see also id.</i> 5:29-35, 18:30-32.
5[c]	determining on the basis of the expected service code an expected response.	“determining on the basis of expected service code XSC an expected response XRES” <i>Id.</i> , 4:15-16; <i>see also id.</i> , 14:6-15, 18:33-34.
6[pre]	Method according to claim 5, the method further comprising:	
6[a]	comparing the expected response with the authentication response sent by the terminal to the network; and	“the network node comprises: ... means for comparing the response RES with the modified expected response XRES”” <i>Id.</i> , 6:3-6; <i>see also id.</i> , 14:15-21, 18:35-36.

6[b]	determining the terminal to be in an un-trusted state if the authentication response is not equal to the expected response.	“determining the terminal to be in an un-trusted state if RES is not equal to XRES” <i>Id.</i> , 4:18-20; <i>see also id.</i> , 14:22-28; <i>see also id.</i> , 18:37-38.
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.	“the terminal comprises a 2G or 3G type radio interface, a Bluetooth radio interface, a wireless LAN interface, a digital enhanced cordless (DECT) radio interface or a data bus interface.” <i>Id.</i> , 4:29-32. “[T]he radio module may comprise e.g. an Ethernet interface....” <i>Id.</i> , 8:22-24.
8[pre]	Service interface module for use in a terminal, the service interface module comprising:	See Claim 2 above (identifying “radio module” as service interface module).
8[a]	a receiver configured to receive an authentication signal from the network via one of the communications interfaces of the terminal;	“The radio module 118 ... includes an RF interface comprising an RF receiver The RF interface of the radio module is capable of receiving and/or transmitting RF signals in accordance with various wireless technologies....” <i>Id.</i> , 8:11-21. “Preferably, the radio module is implemented in the form of one or more trusted hardware components . The hardware of the terminal is preferably configured in such a way that all incoming authentication requests for a network service will be routed via the radio card....” <i>Id.</i> , 11:14-23. Although the EP Application

		does not use the term “authentication signal,” a POSITA would understand the “authentication requests” from the network are transmitted as signals and thus qualify as “authentication signals.”
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;	“the terminal comprises an identity module, preferably a removable identity module, and a radio module comprising a number of communications interfaces and configured to identify the communications channel through which the authentication request was received. The method further comprises the step of: the radio module sending an service code SC to the identity module, wherein the service code identifies the communications channel through which the authentication request was received.” Ex. 2014, 3:8-19; <i>see also id.</i> at 5:1-7. “the AC manager in the radio module 118 is configured to generate a service code (SC) identifying the specific service interface for setting up a wired or a wireless communication channel....” <i>Id.</i>, 11:5-13.
8[c]	a channel interface configured to establish a secure communication channel between the module and an identity module of the terminal; and	“Preferably, the radio module comprises one or more trusted module allowing the service code to be sent to the identity module, e.g. a (U)SIM, in a

		secure way. In one embodiment, the hardware of the terminal is configured in such a way that all incoming authentication requests for a network service will be routed via the radio card, so that the identity module receives for each incoming authentication request a service code.” <i>Id.</i>, 3:16-27; <i>see also id.</i>, 5:8-13, 11:14-24. A POSITA would understand that the trusted module(s) are channel interface(s) for establishing a secure communication channel, otherwise the service code could not be sent to the SIM “in a secure way” as described in the above text.
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.	“means for modifying the response RES on the basis of a predetermined mathematical function using the service code as an input parameter;” Ex. 2014, 5:22-24; <i>see also id.</i> at 12:5-10, 12:21-23.
9	[i] An identity module for establishing a safe communication channel with a service interface module as claimed in claim 8, the identity module comprising: [ii] a calculator for calculating a response upon receipt of an authentication request; and [iii] a modifier for modifying the response on the basis of a predetermined mathematical	[i] “In another embodiment, the terminal comprises an identity module ... and a radio module Preferably, the radio module comprises one or more trusted module allowing the service code to be sent to the identity module, e.g. a (U)SIM, in a secure way. In one embodiment, the

	function using a service code associated with the identified communication channel.	hardware of the terminal is configured in such a way that all incoming authentication requests for a network service will be routed via the radio card, so that the identity module receives for each incoming authentication request a service code.” <i>Id.</i>, 3:8-27. [ii] “The identity module may comprise a processor, one or more memory components e.g. ROM, RAM and/or EEPROM and I/O circuitry. For authentication purposes the UICC comprises a secret service-subscriber authentication key K and one or more algorithms for calculating a response comprising one or more authentication parameters upon the reception of a random challenge.” Ex. 2014, 9:20-27. [iii] “the (U)SIM may modify the calculated response RES on the basis of the service code” <i>Id.</i> at 12:9-10; <i>see also</i> 12:21-25. A POSITA would understand that the “processor” of the (U)SIM (see [ii]) is a modifier because it executes the algorithms that perform the “modifying” (see [iii]).
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	(i) “Operating System (OS) 126 of the terminal comprises ... memory for storing program instructions” Ex. 2014, 8:33-37.

	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:	(ii) <i>See</i> Claim 2 (discussing radio module)
10[a]	receive an authentication request from the network;	<i>See</i> Claim 1[b]
10[b]	determine the communication channel through which the authentication request is received;	<i>See</i> Claim 1[c]
10[c]	determine a service code associated with the identified communication channel via which the authentication request was received by the terminal; and	<i>See</i> Claim 1[d]
10[d]	send in response to an authentication request a modified response to the network wherein the modification depends on the determined service code.	“a terminal configured to send in response to an authentication request a modified response RES’ to the network wherein the modification depends on the type of communication channel the authentication request was received by the terminal” Ex. 2014, 6:8-12.
11[pre]	A network node for service-based authentication of a terminal to a network, the network node comprising:	“Network node for service based authentication to a network, the network node comprising:” <i>Id.</i> , 20:10-11.
11[a]	a receiver configured to receive an authentication data request;	“the network node comprising ... means for receiving an authentication data request from a terminal;” <i>Id.</i> , 20:10-13; <i>see also id.</i> , 13:5-11; Ex. 2015, Fig. 4 (showing network receiving authentication data request from

		terminal). While the draft EP Application does not explicitly use the word “receiver,” a POSITA would understand the network node to necessarily have a receiver because it receives the authentication data request signals.
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	“means for generating an expected service code XSC on the basis the type of communication channel the authentication data request was sent to the network;” Ex. 2014, 20:14-16; <i>see also id.</i>, 4:12-15.
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.	“a network node configured to generate in response to the receipt of an authentication data request a modified expected response XRES’ and configured to compare RES’ with XRES’, wherein the modification of the expected response XRES depends on the type of communication channel the authentication data response was sent to the network.” <i>Id.</i>, 6:12-15; <i>see also id.</i>, 20:37-21:2. “the network node comprises: ... means for modifying the expected response XRES on the basis of a predetermined mathematical function using the expected service code XSC as an input parameter.” <i>Id.</i>, 5:29-6:2.

12[pre]	A system for service based authentication to a network, comprising:	
12[a]	[i] a terminal configured to receive an authentication request from the network, [ii] to determine a service code associated with the type of communication channel via which the authentication request was received by the terminal, and [iii] to send in response to the authentication request a modified response to the network, wherein the modification depends on the determined service code;	[i] See Claim 1[b] [ii] See Claims 1[c]-[d] [iii] See Claim 10[d].
12[b]	[i] 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 [ii] 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 [iii] configured to compare the modified response with the modified expected response.	[i] See Claims 11[a]-[b] [ii] See Claim 11[c] [iii] See Claim 6[a]
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.	“computer program product comprising software code portions configured for, when run in the memory of a mobile device, executing the method steps as described above.” Ex. 2014, 6:19-22.

VIII. OPINIONS ON VALIDITY

A. Ground 1

49. Petitioner contends that Claims 1, 3-7 and 11-13 of the '235 Patent are obvious based on 3GPP Technical Specification 33.402 version 8.1.1 ("TS-33.402") alone, or in view of J. Arkko, et al., "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)," RFC 5448 Draft version 9 (published October 24, 2008) (available at <https://datatracker.ietf.org/doc/html/draft-arkkoeap-aka-kdf-09>) ("Arkko").

50. It is my opinion that neither TS-33.402 nor the combination of TS-33.402 and Arkko teach or suggest all limitations of any claim. The basis for my opinion is provided in detail below.

1. **Claim 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."**

51. Neither TS-33.402 nor Arkko discloses or suggests the language underlined above. Specifically, as discussed in detail below, a POSITA would not understand the combination to teach or suggest an authentication response that

depends on the identified communication channel or that is *calculated on the basis of a service code*.

52. I begin first with Petitioner’s invalidity theory. Petitioner identifies the AKA Response/AKA-Challenge message of TS-33.402 as the alleged “authentication response” and contends that the underlined limitation is satisfied because the MAC value is part of that message and is calculated based on the “access network identity” (alleged “service code”). Pet., 27-29. Specifically, Petitioner contends that in TS-33.402 the authentication response depends on the identified communications channel and is based on the service code because (1) a new MAC value is calculated using the access network identity (alleged “service code”) and (2) that MAC value then “cover[s] *the EAP [response] message* with the new keying material.” Pet., 28 (alteration in original, emphasis added). However, Petitioner’s MAC value theory is erroneous because it is premised on incorrectly identifying the entire *EAP-RSP/AKA-Challenge message* as the “authentication response,” rather than correctly identifying RES as the “authentication response” as understood by those of skill in the art.

53. As I explained in greater detail below, “RES” is explicitly defined as the “user **authentication response**” in the 3GPP standard, and both the ’235 specification and numerous other references use “authentication response” consistently to refer to RES—not the entire AKA-Challenge message—as the

authentication response. The authentication response RES in TS-33.402 is not calculated or in any way based upon the “access network identity” (alleged “service code”). Instead, RES is calculated based on $RES = f2_K(RAND)$, where RAND is the Random Challenge from the network and f2 is the Message authentication function used to compute RES and XRES. Ex. 2003, 11, 24. Consequently, a POSITA would not understand TS-33.402 to teach or suggest this claim limitation.

54. A POSITA would understand that in TS-33.402 the MAC value and authentication response (RES) are contained as separate values within the EAP Response/AKA-Challenge message. As TS-33.402 teaches, the “[t]he UE calculates a new MAC value covering the EAP message with the new keying material. UE sends EAP Response/AKA-Challenge containing [1] *calculated RES* and [2] *the new calculated MAC* value to the authenticator in the access network.” Ex. 1006, 15 (alterations and emphasis added). “RES” is the authentication response and is contained within the EAP-Response/AKA-Challenge message separately from the MAC value. Stated another way, the EAP-Response/AKA-Challenge is the message conveying both the authentication response (RES) and new calculated MAC back to the network. The network then compares the authentication response (RES) with the “expected authentication response” (XRES). *Id.* (“18. The 3GPP AAA Server checks the received MAC and compares XRES to the received RES.”). It is worth emphasizing that the expected authentication response XRES is compared to RES—

not to the entire EAP message. This is because only RES is the “authentication response,” not the entire EAP message.

55. A POSITA would have understood “RES”—which is defined as the “user authentication response” by the standard—to be the authentication response in the AKA-Challenge process of TS-33.402. Specifically, TS-133.102 provides a conceptual illustration of the AKA-Challenge process:

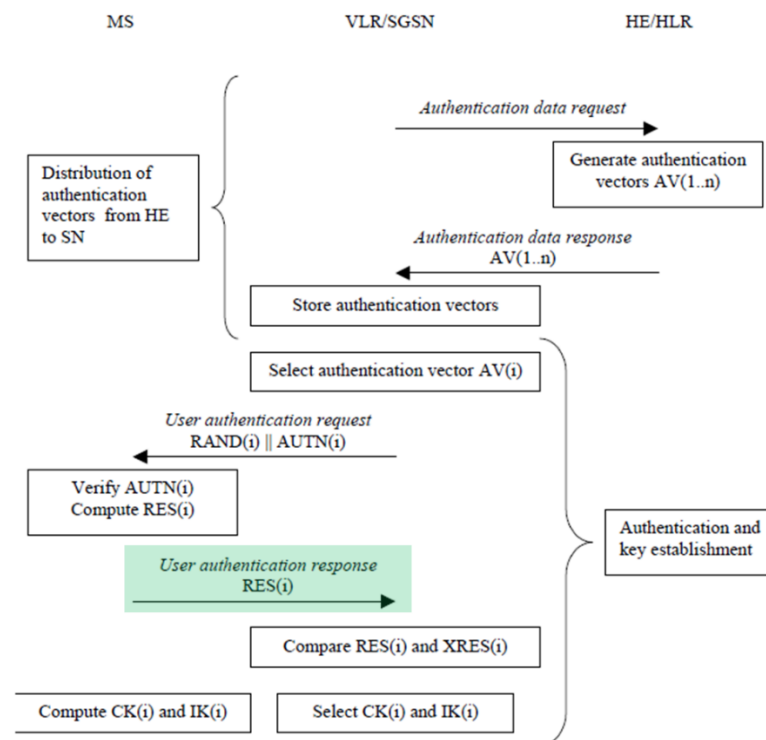


Figure 5: Authentication and key agreement

Ex. 2003, 19 (annotated). RES is explicitly referred to as the “user authentication response” in the figure and described as such throughout the text. *Id.* at 28 (“The authentication response (RES) shall have a variable length of 4-16 octets.”). Indeed, it is abbreviated “RES” because it is the authentication **RESPONSE**. And the

authentication response is compared to the expected authentication response XRES, not the entire EAP/AKA-Challenge message.

56. This understanding is further reflected in by Figure 8 of TS-133.102:

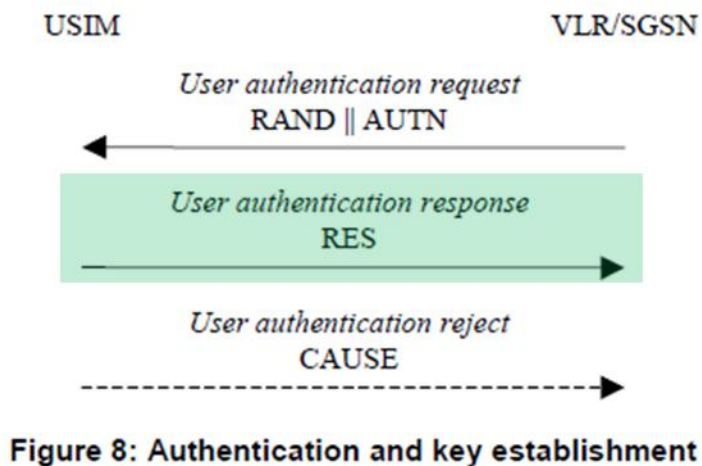


Figure 8: Authentication and key establishment

Id. at 22. As shown, “User authentication response” corresponds to **RES**, which is the same **RES** that is included alongside the MAC value in the entire EAP-RSP/AKA-Challenge message in TS-33.402. Moreover, the MAC is not depicted or illustrated as being the “User authentication response.”

57. An abundance of other references also supports that a POSITA would have understood RES to be the authentication response in the AKA-Challenge of TS-33.402. *See e.g.*, Ex. 2004, 1:65-2:5 (patent assigned to British Telecommunications plc explaining that in UMTS networks the USIM of the terminal “calculates an authentication response **RES** using a fixed algorithm based on RAND and the shared key K” and that the “response **RES**” is transmitted back” to the network); Ex. 2005, 1:60 (patent assigned to Nokia providing list of

abbreviations relating to 3GPP, including “**RES** Authentication Response generated by ISIM”). A patent assigned to LG Electronics Inc. provides a schematic drawing similar to those reproduced above showing that RES is considered the authentication response in UMTS networks:

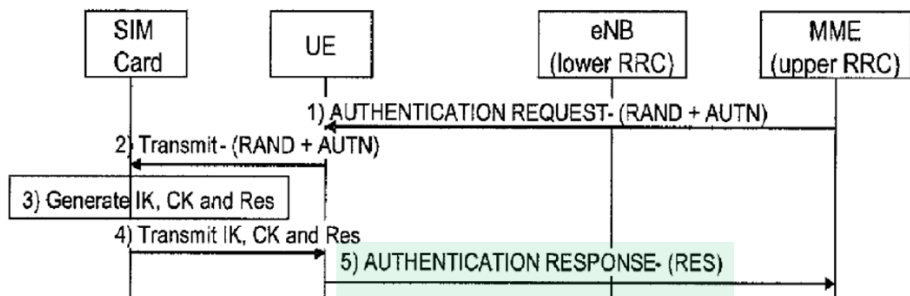
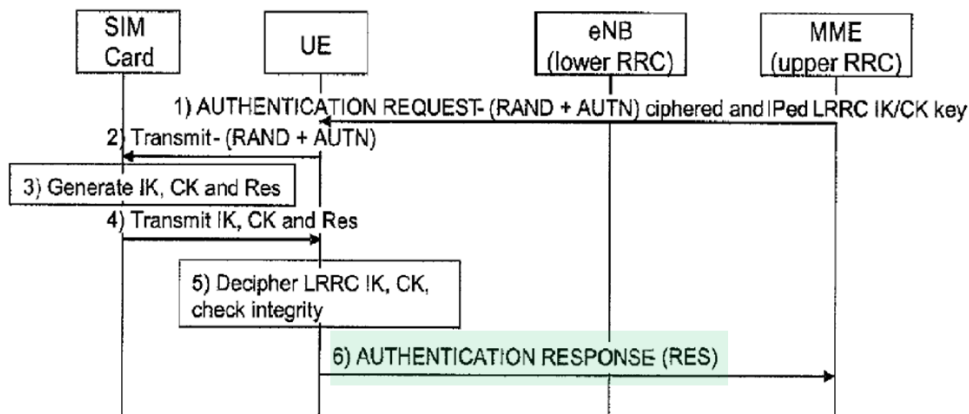


Fig. 12



Ex. 2006, 9:45-49 (“the UE responsively generates an authentication response RES”).

58. The evidence above is consistent with repeated and exclusive teachings from the specification of the '235 Patent that “RES” is the authentication response in the AKA-Challenge process. See *e.g.*, Ex. 1001, 7:1-3 (explaining that the terminal, “returns a calculated response **RES** back to the MSC”), 7:30-33 (“...the

USIM calculates—amongst others—a response **RES**....”), 8:20 (“...then returns a response **RES** back to the SI module”), 9:16-20 (“the digital signal comprising RAND and AUTN is forwarded to the USIM (step 414), which calculates the response **RES**.... Then the USIM sends the response **RES** back to the SI module (step 416)”), 9:67-10:3 (“In another variant, the SIM first calculates the **response RES** on the basis of the RAND....”), 10:39-43 (“In that case, the (U)SIM responds to the request by calculating a correct response **RES**....”). Notably as well, Petitioner appears to acknowledge that “RES” is the known-abbreviation for the “authentication response” and further that TS-33.402 uses RES consistent with that understanding. See Pet., 62-63.

59. In view of the above, a POSITA would have understood that the authentication response in an EAP-Response/AKA-Challenge is RES, which is not calculated based on the “access network identity.” This is not only because the ’235 Patent repeatedly and exclusively uses the term “authentication response” synonymously with RES, but also because a POSITA understood (as shown by the evidence above) that the authentication response of an AKA agreement was specifically defined and referred to as RES—not the entire EAP-RSP/AKA-Challenge message. A POSITA would have thus understood that the authentication response (i.e., RES) in TS-33.402 is distinct from the MAC value, and that both the RES and MAC are contained with the EAP-Response/AKA-Challenge message.

RES is not calculated or based in any way on the access network identity (alleged “service code”) and thus a POSITA would not understand TS-33.402 to teach or suggest Claim 1[e].

60. Petitioner further contends that the EAP-Response/AKA-Challenge (alleged “authentication response”) is calculated on the basis of the received MAC and AUTN values (alleged “information in the authentication request”). Pet., 27-28. Petitioner’s reliance on these values is erroneous.

61. A POSITA would understand that the authentication response RES is not calculated by the UE based on AUTN and the received MAC. Petitioner contends that this limitation is satisfied based on AUTN and the received MAC because “the response (‘RES’) is not generated unless ‘AUTN is correct,’” and the UE “check[s] the received MAC with the new derived keying material,” respectively. Pet., 28. However, TS-33.402 only teaches that whether AUTN and the received MAC value are correct dictates *whether calculations are performed* to compute RES, IK and CK—those calculations are not *based on* AUTN. Specifically, TS-33.402 teaches:

If AUTN is incorrect, the terminal rejects the authentication (not shown in this example).... If AUTN is correct, the USIM application computes RES, IK and CK.”). The UE then computes $(CK', IK') = F(CK, IK, \langle \text{access network identity} \rangle)$ in the same way as the HSS. The UE derives required additional new keying material, including the key MSK, according to RFC 4187 EAP-AKA [7] from the new computed CK', IK' and checks the received MAC with the new derived keying material.

Ex. 1006, 15. A POSITA would thus understand that whether AUTN and the received MAC (i.e., alleged “information in the authentication request”) are correct merely dictates *whether* the RES calculations are performed—those values are not used to calculate the authentication response RES. This is true even under Petitioner’s identification of the entire EAP-Response/AKA-Challenge message as the alleged “authentication request,” because whether AUTN and the received MAC are correct also only dictates whether the EAP-Response/AKA-Challenge message is generated—it is not used in any calculation to prepare that message. *Id.*

1. Claim 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.”

62. Petitioner contends that this limitation is taught by TS-33.402. I have reproduced Petitioner’s arguments on this point below:

As discussed in limitation 1[c] and 1[d], TS-33.402 discloses that the encryption keys CK’ and IK’ are derived from the access network identity, *i.e.* ***identified communications channel***. TS-33.402 further discloses that the CK’ and IK’ are used to derive “new keying material, including the key MSK” which is in turn used to “check[] the received MAC.” EX1006, 15. A POSITA would understand that the MAC is a keyed hash of the authentication request. EX1008, 12 (“The MAC algorithm is HMAC-SHA-256-128, a keyed hash value.”). Thus, checking the MAC involves the terminal using the MAC algorithm (specifically HMAC-SHA-256-128) and the new keying material to

modify the authentication request, i.e. **authentication information**, to generate the keyed hash in order to match its value with the received MAC. EX1003, ¶¶120-21.

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

Pet., 29-30. There are several reasons that Petitioner is mistaken.

63. Petitioner is incorrect that that the authentication request is “modified” to check the received MAC (see underlined portion of passage above). The received MAC is only used as an input to a (keyed hash) calculation, to **verify** that the MAC is correct. Ex. 1016, 63, (“The MAC algorithm is HMAC-SHA1-128 [RFC2104] keyed hash value.”). As Petitioner correctly acknowledges in the passage above, the MAC is merely used to “check” for a match—the message itself is not **modified**; it is delivered to the terminal “as is” if there is a match. A POSITA would understand

this to be fundamentally different than modifying the authentication information as claimed.

64. As an example of “modifying” as claimed, the ’235 specification teaches:

In one embodiment the (U)SIM may ***modify the authentication information*** in the authentication request, e.g. a random challenge RAND, on the basis of the service code SC and subsequently calculate a response RES on the basis of an authentication and key agreement (AKA) of a telecommunications standard. For example, in the case of a GSM service the SIM may perform the steps: $RAND' = f(RAND, SC)$ and $RES' = A3(RAND', K_C)$.

Ex. 1001, 9:60-67. The RAND (“authentication information”) of the authentication request is thus “modified” by the terminal to generate RAND', which is a function of both RAND and SC. A POSITA would not understand the act of using an input to verify a hash value to qualify as “modifying” as claimed, but instead would understand “modifying” consistent with the examples provided in the specification.

65. Second, Petitioner is incorrect that TS-33.402 teaches “generating the authentication response on the basis of the modified authentication information.” Petitioner acknowledges that whether the MAC value is correct simply affects ***whether*** the EAP Response/AKA-Challenge message (including the authentication response RES contained within the message) is calculated. If the MAC value is incorrect, the message is not calculated. Ex. 1006, 15 (“The UE derives required

additional new keying material, including the key MSK, according to RFC 4187 EAP-AKA [7] from the new computed CK', IK' and ***checks the received MAC with the new derived keying material.***") If the MAC value is correct, the message is calculated, but the MAC value forms ***no basis*** of the calculation. *Id.* Consequently, the value of the message (including the authentication response RES contained within the message) is entirely independent of the incoming MAC value. A POSITA would thus understand that neither the EAP Response/AKA-Challenge message (the alleged "authentication response") nor the actual authentication response (RES) is generated "on the basis of" the MAC value (alleged "modified authentication information").

66. I also note that Petitioner's invalidity theory on Claim 3[a] is also inconsistent with the specification of the '235 Patent. The phrase "on the basis of" is uniformly used by the specification to refer to generating a value based on a particular input parameter. *See e.g.*, Ex. 1001, 9:60-66 ("the (U)SIM may modify the authentication in the authentication request, e.g., a random challenge RAND, ***on the basis of*** the service code SC For example, ... the SIM may perform the steps: $RAND' = f(RAND, SC) \dots$ "), 9:67-7:3 ("In another variant, the SIM first calculates the response RES on the basis of the RAND and then modifies RES ***on the basis of*** SC: $RES' = A_3(RAND, K_C)$ and $RES' = f(RES, SC)$ "); 8:64-66 ("***On the basis of*** the identified service interface information an expected service code XSC is determined

(step 404).”), 9:28-30 (“The expected response XRES' may be determined by the SIU using the one-way function f with the expected response XRES determined **on the basis of** the UMTS AKA and the SC as the input parameters: $XRES'=f(XRES,SC)$.”); 10:9-11 (“determining the expected response XRES' **on the basis** [of] the UMTS AKA using RAND' as one of the input parameters”); 10:52-55 (“the network 510 will determine an expected service code XSC **on the basis of** the request of the attacker”). In fact, the phrase “on the basis of” is used in the specification 21 times, and always to refer to the value of something (e.g., modified authentication response RES', modified authentication information RAND') being determined by something else (e.g., the service code SC).

67. A POSITA would also understand that Petitioner’s interpretation of Claim 3[a] is inconsistent with the embodiments described in the specification. A POSITA would understand that the purpose of the terminal “generating the authentication response on the basis of the modified authentication information” is so that **the network** can verify/authenticate the authentication response by confirming that the terminal identified the correct communications channel, which ensures that it was received from the terminal and not a “man-in-the-middle.” Ex. 1001, 2:33-38. To accomplish this, the authentication response must be generated using the modified authentication information as an input parameter, as the modified information is what is (1) associated with the identified channel (pursuant to the

claim language “modifying the authentication information on the basis of the identified communications channel”) and (2) used as a function input by both the terminal and network so that the results can be compared to authenticate.

68. As one example, specification teaches that the SIM of a terminal may perform the step of $RAND' = f(RAND, SC)$, which associates the **service code SC** with the RAND (i.e., authentication information” from the authentication request) to generate modified RAND' (i.e., authentication information modified “on the basis of the identified communications channel”). Ex. 1001, 9:65-67. A response RES' is then generated on the basis of RAND' via the step $RES' = A3(RAND', K_C)$. *Id.* RES' is thus associated with the **service code SC** because RES' relies on RAND', which itself relied on the **service code SC** as an input parameter. The network “comprises the mathematical function f used by the USIM in the terminal” and independently determines RAND' using the equation $RAND' = f(RAND, XSC)$, which is then used as an input parameter to generate XRES' for comparison to RES'. *Id.* at 10:6-16. A POSITA would understand that the network is therefore able to authenticate the terminal and prevent a “man-in-the-middle-attack” because both the terminal and network use the same function inputs (***including modified authentication information RAND'***) to generate RES' and XRES', respectively.

69. A POSITA with this understand would recognize that Petitioner’s proposed understanding of the claim phrase “the terminal generating the

authentication response on the basis of the modified authentication information” is simply erroneous. Under Petitioner’s understanding, “the modified authentication information” dictates **whether** the alleged authentication response is created. But if that were the case in the example above, RAND’ could not be used as an input function, and there would be no purpose in modifying RAND to create RAND’ in the first place. Indeed, the network would not be able to authenticate the terminal if the terminal does not use RAND’ to generate its authentication response. For this and the other reasons discussed above, a POSITA would not understand TS-33.402 to teach or suggest limitation 3[a], which is fundamentally different than the disclosed MAC check process of TS-33.402.

2. Claim 4[b]: “the terminal modifying the authentication response on the basis of the identified communications channel.”

70. Petitioner contends that TS-33.402 teaches this limitation because it allegedly teaches that “the terminal ‘calculates the new MAC value covering the EAP message [*i.e.*, **authentication response**] with new keying material” and the new keying material is derived from access network identity (*i.e.*, the alleged identified communications channel). Pet. 31-32 (emphasis in original).² It is my opinion that Petitioner is mistaken for at least two reasons.

² I note that the MAC is a cryptographic checksum used to verify both the integrity and authenticity of a message. When a message is sent with a MAC, the recipient

71. First, Petitioner’s invalidity theory is premised on incorrectly mapping “the authentication response” to the EAP-Response/AKA-Challenge message. But as I explained with respect to Claim 1[e], that AKA-Challenge message is not the authentication response. Rather, the AKA-Challenge message *includes* the authentication response, which is expressly defined and understood to be **RES** (as evidenced by numerous objective references). TS-33.402 does not teach or suggest modifying **RES** on the basis of the identified communications channel. Quite the opposite—TS-33.402 expressly teaches that the authentication response is not modified, but rather is transmitted back to the network in its original form so that it can be used for authentication. *See* Ex. 2006, 15 (“UE sends EAP Response/AKA-Challenge ***containing calculated RES*** and the new calculated MAC value to the authenticator in the access network.”).

72. Second, even if one was to assume that a POSITA would have understood the EAP-Response/AKA-Challenge message to be the “authentication response” (a POSITA would not), this limitation would still not be disclosed by TS-33.402. Petitioner acknowledges that TS-33.402 teaches that “[t]he UE calculates a new MAC value ***covering*** the EAP message with the new keying material.” Pet., 31 (citing Ex. 1006, 15). A POSITA would understand that “covering” refers to the fact

can verify that: 1) the message was not altered (integrity), and 2) it was generated by someone with access to the secret key (authenticity).

that the MAC value is similar to *a signature on* the EAP message to *prevent* modification of the message. Ex. 1016, 10 (“The EAP-Request/AKA-Challenge message MAY optionally contain encrypted data, which is used for identity privacy and fast re-authentication support, as described in Section 4.1. **The AT_MAC attribute contains a message authentication code covering the EAP packet. The encrypted data is not shown in the figures of this section.**”).

73. A POSITA would understand that there is a fundamental difference between *covering/signing* the EAP message with the MAC and *modifying* the message. When the MAC is applied it is simply *appended to* the EAP message as a signature—the content (e.g., the authentication response RES) of the EAP message itself remains the same. Ex. 2002, 4 (defining “signature” as a “sequence of data used for identification, such as text *appended to* an e-mail message or fax”); Ex. 2009, 4 (defining “append” as “to *attach* or *affix*”). A POSITA would understand that the content of the EAP message before and after covering with the MAC remains the same. The “covering” referenced in TS-33.402 does nothing to change the content but simply adds a signature. Indeed, “MAC” stands for “*message authentication code*” and the “message” that the MAC authenticates is the EAP Response/AKA-Challenge message, meaning the MAC does not form part of the message content that is being authenticated. An apt analogy would be email signature. Specifically, the MAC is similar to a digital signature used for email

authentication, which verifies the authenticity of an email but does not modify or affect its underlying content. In this analogy, the email is RES and the MAC is the signature.³

74. A POSITA would understand that “covering” with a MAC is fundamentally different than what is claimed and described in the ’235 Patent. The specification uniformly describes “modifying” information (e.g., RES, RAND) as altering the content of information to form “modified” information (e.g., RES', RAND'). See *e.g.*, Ex. 1001, 9:21-24, 9:60-10:6, 10:57-60. Under Petitioner’s very broad understanding of “modifying,” simply transmitting a message over a network necessarily means it is “modified” because all messages transmitted over a network undergo some form of encapsulation (e.g., broken into packets to be transmitted via the IP protocol). A POSITA would not understand “modify” as used in the specification and claims to have such an expansive meaning.

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

75. The Petition contends that “the network server calculates an authentication vector containing XRES (*i.e.* ***expected response***) using the expected access network identity, which is the identity of the communications channel the

³ EAP-response/AKA-challenge message = {RES, MAC}. The MAC is calculated on RES.

service request was sent to the network.” Pet., 32-33. The Petition thus initially alleges that XRES is the “expected response.” *See also id.* at 34-35 (relying on XRES as “the expected response” for Claim 6). However, the Petition then appears to change its identification of the alleged “expected response” by asserting that the “new authentication vector” is “the expected response.” *Id.* at 32-33 (“Thus, the authentication vector is an **expected response**, and it is determined on the basis of the **expected service code**.”). A POSITA would not understand either the “new authentication vector” nor “XRES” of TS-33.402 to satisfy Claim 5[c].

76. The new authentication vector is not an “expected response—“XRES” is the expected response. Indeed, Petitioner earlier acknowledged that “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.” Pet., 7 (emphasis added). As Petitioner further acknowledges, it is XRES and RES that are compared—the authentication vector is never compared to anything by the server. *Id.* at 8 (“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.”). This is precisely why it is referred to as XRES—it is the “expected” (X) authentication response (RES) and must match the authentication RES to authenticate the terminal. Indeed, TS-33.402 does not teach that the new authentication vector is compared to

RES, because the new authentication vector is not the expected authentication response.

77. That a POSITA would understand the XRES of TS-33.402 to be the “expected authentication response” is supported by the teachings from the specification of the ’235 Patent, which uniformly uses “XRES” to refer to the expected authentication response. *See e.g.*, Ex. 1001, 3:17-18 (“determining on the basis of expected service code XSC an **expected response XRES**”), 3:20-21 (“comparing the expected response XRES with the authentication response RES”), 4:46-50 (“wherein the modification of the **expected response XRES** depends on the type of communication channel”), 4:27-29 (“a generator for generating an **expected response XRES** or a receiver for receiving from another network node an **expected response XRES**”), 4:30-31 (“a modifier the **expected response XRES**”), 6:63-65 (“which generate an **expected response XRES**”), 7:17-21 (“These four parameters are fed into the ... functions f1-f5, resulting in five new parameters: ... the **Expected Response (XRES)**”), 9:28-32 (“the SIU using the one-way function f with the **expected response XRES**”).

78. That a POSITA would understand XRES to be the expected response in the AKA-Challenge of TS-33.402 is further shown by numerous other references describing the AKA-Challenge process. For example, TS-133.102 explicitly defines “XRES” to mean “Expected Response.” Ex. 2003, 12. TS-133.102 also provides the

formula for computing “expected response $XRES = f2_K (RAND)$ where $f2$ is a (possibly truncated) message authentication function.” *Id.* at 22. Thus, RES and XRES are both computed using $f2$ with RAND and the secret key K as an inputs. TS-133.102 also provides a schematic diagram showing how the expected response XRES is compared to the authentication response RES:

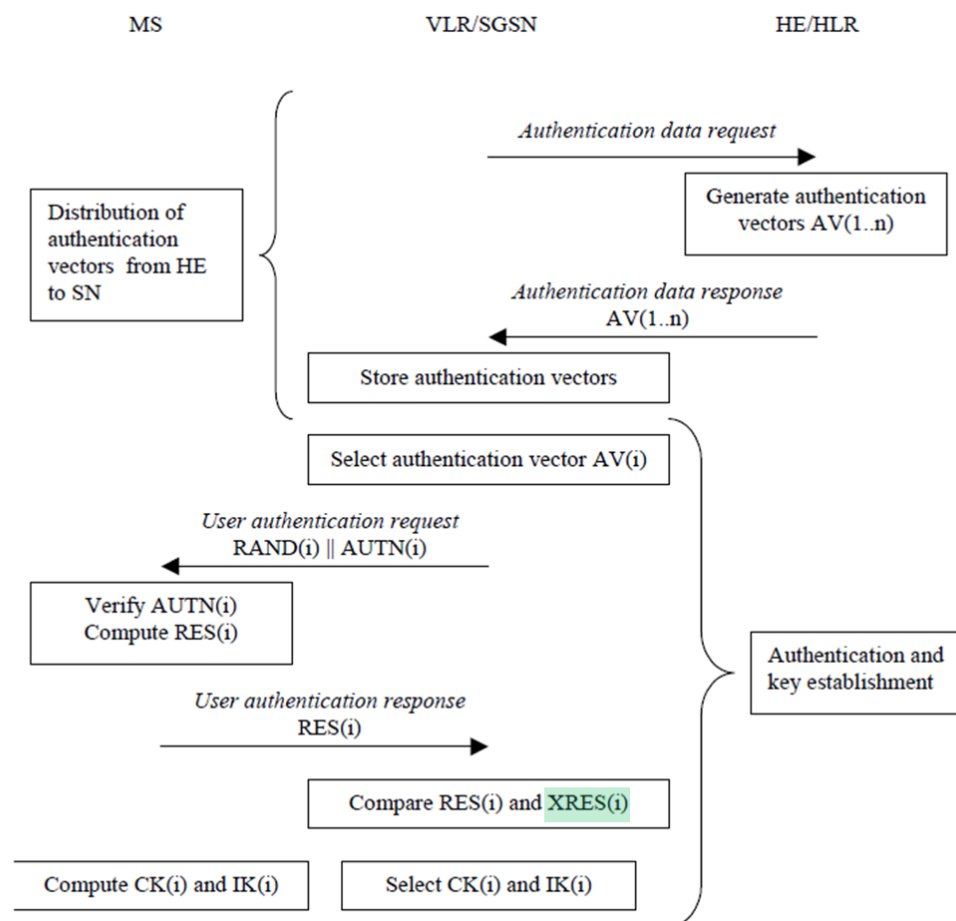


Figure 5: Authentication and key agreement

Ex. 2003, 19-20 (“Each authentication vector consists of the following components: a random number RAND, an expected response XRES.... The VLR/SGSN compares the received RES with XRES.”). Indeed, it would have been part of the

background knowledge of a POSITA that in an AKA-Challenge the authentication response is defined as RES and the expected authentication response is defined as XRES, as reflected by TS-133.102.

79. Additional references also reflect that a POSITA would have understood XRES to be the expected response in TS-33.402. *See e.g.*, Ex. 2004, 6:5-12 (patent assigned to British Telecommunications plc explaining that in UMTS networks the “authentication vector AV is generated by the HSS 102 and includes a random number RAND, an **expected response** XRES_{HSS} ... **expected response** XRES_{HSS} is derived by the HSS”); Ex. 2011, 1:36-44 (Alcatel Lucent patent explaining that “[c]onventional 3G CDMA security protocols are based on an authentication key agreement (AKA).... The well-known AKA security protocols used in 3G CDMA are based on quintuplets. Quintuplets include a random number RAND, **expected response** XRES....”), 2:33-36 (“The serving system of the network then compares the **expected response** XRES with the response RES to authenticate the mobile equipment....”). Notably as well, one of Samsung’s own patent applications teaches, with respect to the AKA-Challenge process, “[e]ach of the AVs includes a random number RAND, an authentication token AUTN, a cipher key CK, an integrity key IK, and an **expected response** XRES.” Ex. 208 ¶[0009].

80. For the reasons discussed above, a POSITA would have understood that the expected response in the EAP-AKA Challenge of TS-33.402 is XRES, not the

“new authentication vector” as alleged by Petitioner. This is an important fact because XRES is not determined based on the access network identity (alleged “service code”). As reflected in the annotated figure from TS-133.102, XRES (green) is determined exclusively based on the message authentication function f2 and RAND (orange), specifically $XRES = f2(RAND, K)$:

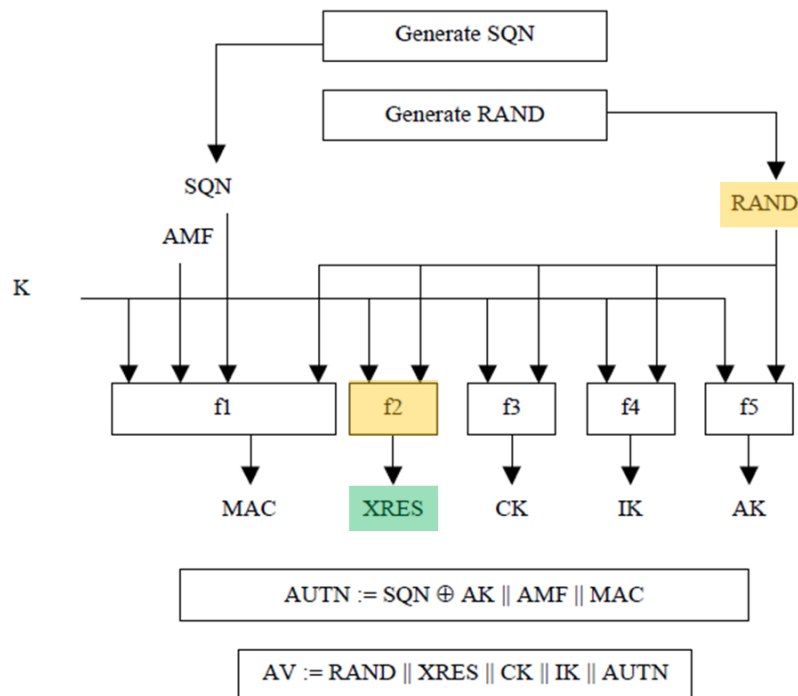


Figure 7: Generation of authentication vectors

Ex. 2003, 21-22. Because the expected response XRES of TS-33.402 is in no way calculated based on or determined by the access network identity (alleged “service code”), a POSITA would not understand TS-33.402 to teach Claim 5[c].

4. Claim 6[a]: “comparing the expected response with the authentication response sent by the terminal to the network;”

81. Claim 6[a] recites “*comparing* the expected response with the authentication response sent by the terminal to the network” and 6[b] recites “determining the terminal to be in an un-trusted state *if the authentication response is not equal to the expected response.*” As explained with respect to Claim 5[c], Petitioner initially identifies XRES as the “expected response” in TS-33.402, but then changes its theory to allege that “new authentication vector” is the “expected response.” Pet., 34-35.

82. If the “new authentication vector” is considered to be the “expected response” of the claim (as Petitioner alleges in Claim 5[c]), TS-33.402 does not teach or suggest comparing the new authentication vector to the EAP-Response/AKA-Challenge message (alleged “authentication response”) or the actual authentication response RES. Ex. 1006, 13. In fact, TS-33.402 does not teach comparing the new authentication vector to *anything*.

83. Petitioner alleges that TS-33.402 teaches that Claim 6[a] is satisfied because it teaches “3GPP Server 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” Ex. 1006, 15 (cited by Pet., 34-35). In other words, Petitioner points to XRES in TS-33.402 as the “expected response” that is compared as claimed. Although XRES would be understood to be

an expected response in TS-33.402, XRES is *not* calculated or determined based on the access network identity. *See* Ex. 2003, 22 (“expected response $XRES = f2_K(RAND)$ where $f2$ is a (possibly truncated) message authentication function”). Consequently, if XRES is the alleged “authentication response” Claim 5 would not be taught by TS-33.402 and thus Claim 6 necessarily cannot be taught. But if the “new authentication vector” is considered the “expected response,” then Claim 6 cannot be invalid because the vector is not “compared” as claimed.

5. Claim 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.”

84. Petitioner contends that the “new authentication vector” is a “modified expected response” because transformation of the vector relies on the access network identity (alleged “service code”). Pet., 37. Petitioner’s theory here is incorrect for the reasons discussed with respect to Claim 5[c]. Specifically, the authentication vector would not be understood to be an “expected response” and would thus also not be understood to be a “modified expected response.” Instead, a POSITA would understand that XRES is the expected response in TS-33.402, which is never modified—i.e., there is no XRES’ in TS-33.402. XRES is instead compared to the received authentication response RES “as is.” Ex. 1006, 15 (“The 3GPP AAA Server checks the received MAC and compares XRES to the received RES.”). Because the

expected response XRES is not modified in TS-33.402, there is no “modified expected response” as claimed.

6. Claim 12[a]: “...send in response to the authentication request a modified response to the network, wherein the modification depends on the determined service code;”

85. Petitioner relies on its discussion of limitation 4[b] for this limitation. Pet., 37. However, TS-33.402 does not teach or suggest that the terminal generates or transmits a modified response that is based on a determined service code as explained with respect to Claim 4[b] above.

7. Claim 12[b]: “a network node 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”

86. For this limitation, Petitioner relies on its analysis with respect to limitation 11[c]. Pet., 38. TS-33.402 fails to teach or suggest this limitation for the same reason discussed with respect to Claim 11[c].

B. Ground 2

87. Petitioner contends that Claims 2, 8-10 and 13 as obvious based on TS-33.402 (with or without Arkko) in view of U.S. Patent No. 8,413,209 (“Aldera”). Pet., 4-5.

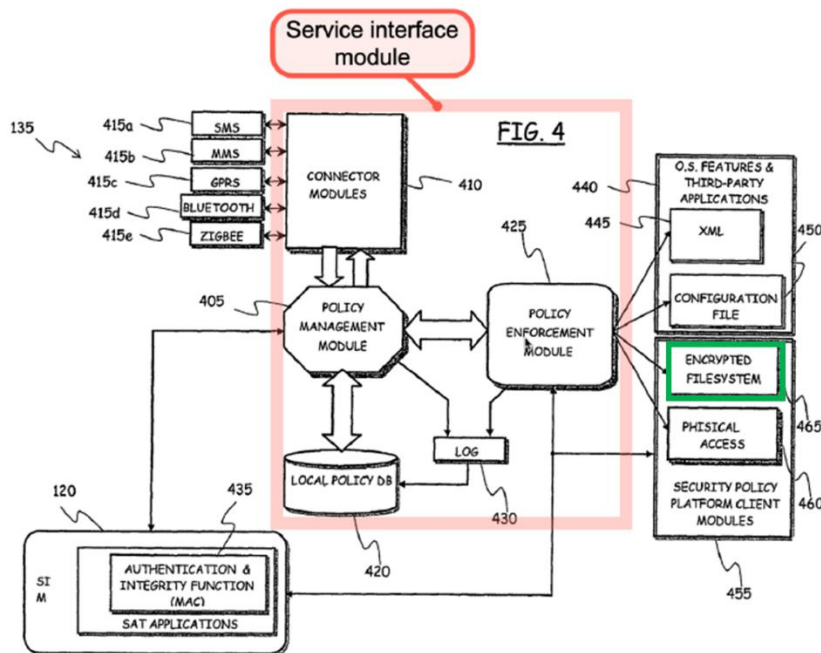
88. It is my opinion that the combination of TS-33.402, Arkko and Aldera do not teach or suggest all limitations of any claim and further that it would not have

been obvious to combine those references as proposed by Petitioner. The basis for my opinion is provided in detail below.

1. Claim 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.”

89. Petitioner relies on Aldera for the “modifier” *structure*, but relies exclusively on TS-33.402 for the *function* “modify an authentication response of the identity module on the basis of the service code associated with the identified communication channel.” Pet., 48-49. However, as I explained with respect to Claim 4[b], TS-33.402 does not teach or suggest that function. As such, the combination of TS-33.402, Arkko and Aldera does not teach or suggest this limitation.

90. Petitioner identifies the “encryption function” 465 as the alleged “modifier.” Pet., 49. However, pursuant to Petitioner’s own identifications (shown below), the encryption function 465 (green box, added by Patent Owner) is not part of the alleged “service interface module” (red box, added by Petitioner).



Pet. 43. Indeed, the encryption function 465 resides outside of the alleged “service interface module.” A POSITA would understand that the “modifier” of Claim 8[d] must be part of the “service interface module” because the claim recites “the service interface module **comprising**: ... a modifier....” Because the alleged “service interface module” does not “comprise” the alleged “modifier” (encryption function 465), a POSITA would not understand the Aldera to satisfy this limitation pursuant to Petitioner’s own mappings.

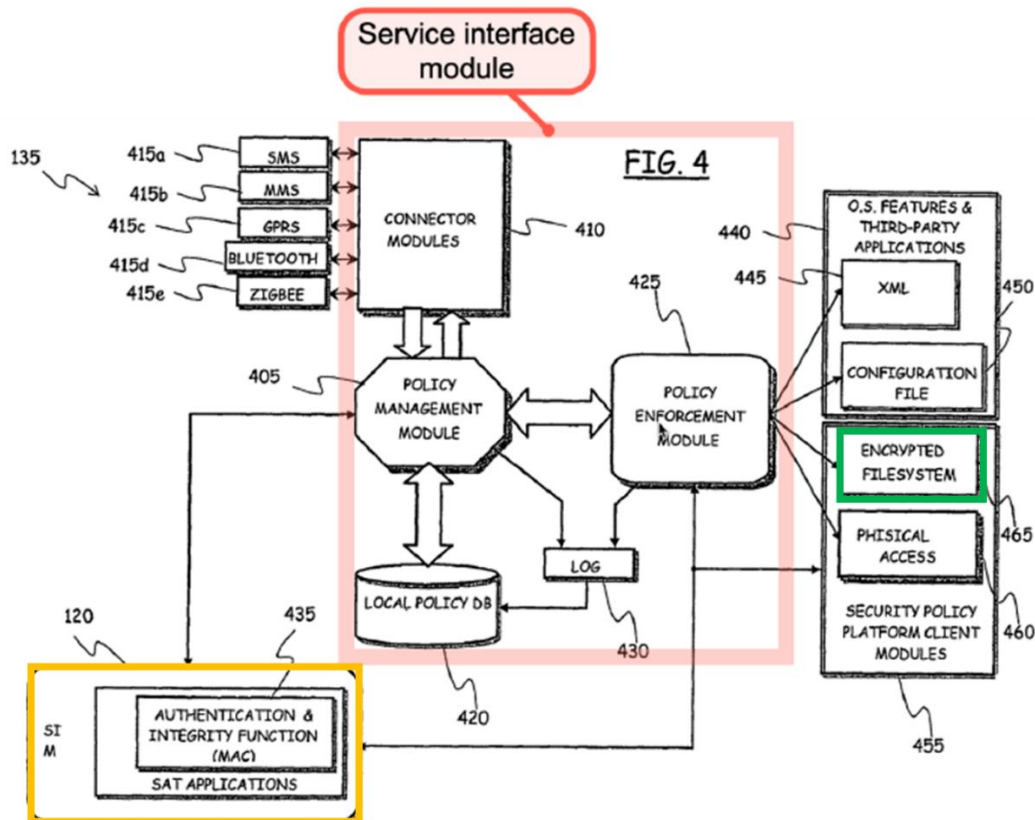
91. Additionally, TS-33.402 teaches that “the UE runs AKA algorithms **on the USIM application on UICC.**” Ex. 1006, 15. However, Petitioner contends that it would have been obvious to have the “encryption function 465” perform the alleged “modifying.” Petitioner does not explain why a POSITA would be

motivated to have the encryption function 465 (**outside of** the SIM 120 of Aldera) perform the alleged “modification,” given the teaching from TS-33.402 that the AKA algorithms are performed on the USIM application.

2. Claim 9: “An identity module ... comprising ... a modifier for modifying the response on the basis of a predetermined mathematical function using a service code associated with the identified communication channel.”

92. As with Claim 8[d], Petitioner here relies on Aldera for the “modifier” **structure**, but relies exclusively on TS-33.402 for the “modifying” **functionality**. Pet., 50. As explained with respect to Claim 4[b], TS-33.402 does not teach or suggest “modifying” the response on the basis of a predetermined mathematical function using a service code associated with the identification communication channel. Consequently, the combination of TS-33.402, Arkko and Aldera fails for the same reason that TS-33.402 alone fails to satisfy this limitation. *Supra* Section XX.

93. It is also my opinion that Petitioner’s contention that Aldera’s alleged “identity module” (i.e., SIM 120) comprises the “modifier” of Claim 9 is irreconcilable with Petitioner’s theory on Claim 8. Specifically, in reference to the annotated figure below, for Claim 8 Petitioner contends that the “encryption function” 465 (green box, added by me) is the “modifier” of the alleged “**service interface module**” (red box, Pet. 43).



However, for Claim 9, Petitioner is contending that the “modifier” is part of the alleged “*identity module*” (SIM 120, orange box added by me) because the claim requires the modifier to be part of the identity module. The Petition does not explain or address why it would be obvious to place the “modifier” in the identity module rather than the service interface module as alleged for Claim 8.

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

94. Petitioner relies exclusively on TS-33.402 for this limitation. Pet., 52. However, TS-33.402 does not teach or suggest that limitation for the reasons

discussed with respect to Claim 4[b]. As such, the combination of TS-33.402, Arkko and Aldera does not teach or suggest this limitation.

C. Ground 3

95. Petitioner contends that Claims 1-7 and 13 are obvious based on Naslund alone. Pet., 4-5. Naslund do not teach or suggest all limitations of any of those claims. The basis for my opinion is provided in detail below.

1. Claim 1[d]: “the terminal determining a service code associated with the identified communication channel”

96. Petitioner alleges that Naslund discloses this limitation because it discloses a “security policy table” with policies that include one or more “Security-enhancing sub application” codes (e.g., 01, 04, 05), where each policy includes an “Interface” parameter (e.g., Normal, Bluetooth, WLAN). Pet., 59-61. Petitioner annotates the security policy table (Table I) as follows to support its position:

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

97. A POSITA would not understand Naslund to teach or suggest a service code associated with the identification communication channel. As determined by the district court, the plain and ordinary meaning of “service code” is a “code *that identifies* a communication channel.” Ex. 1015, 64 (discussed by Pet., 11). Pursuant to Claim 8[b], the claimed “service code” must identify “the communication channel *through which the authentication signal was received.*” As I explain below, the “Security-enhancing sub application” codes cannot satisfy this requirement.

98. A POSITA would instead understand that each code (e.g., 01 through 07) represents a particular “Security-enhancing sub application.” Indeed, this is why the codes are listed in the column “Security-enhancing sub application” (green). The codes are thus associated with security-enhancing sub applications, not an identified communication channel as claimed. A POSITA would understand that the codes for

the security-enhancing sub applications are only included in the same table as “Interface” because “Security-enhancing sub application” and “Interface” are parameters of each security policy. See Ex. 1005, 21:7-9 (“For illustrative purposes, an example of a security policy table for implementation in a tamper-resistant security device according to the invention is presented below.”).

99. The fact that the same codes are used in policies having **different** “Interface” parameters confirms that the codes cannot identify the channel upon which the authentication request was received. For instance, as shown in the further annotated version of Table I, in row two code “01” is included in a policy listing “Normal” interface, but in row ten the same code “01” is included with a policy listing the “WLAN” interface:

Table I

Security conditions			Security mode	
Environment	Network/Operator	Interface	Normal AKA	Security-enhancing sub application
1 Mobile	Home	Normal	Enabled	-
*2 PC	Home	Normal	Disabled	01
3 Mobile	Home	Bluetooth	Disabled	02
4 Mobile	Home	IR	Disabled	03
5 Mobile	Home	WLAN	Disabled	04
6 Mobile	Visited	Normal	-	05 (negotiation)
7 Mobile	Operator A	Normal	Disabled	06
8 Mobile	Operator B	Normal	Disabled	07
9 ...				...
*10 PC	Visited	WLAN	Disabled	01,04,05

A POSITA would understand that the “Security-enhancing sub application” code cannot be associated with the identified communication channel, as each code can

be included in policies involving *different* “Interface” parameters. The codes are instead associated with the security-enhancing sub applications. The fact that the codes for the “Security-enhancing sub application” and “Interface” are included in the same row is merely because they are both part of the same security policy, not because the codes are associated with any particular “Interface” parameter.

100. The fact that different codes may be part of different security policies that include the same “Interface” parameter further confirms that the codes do not identify a communication channel as claimed. For example, as shown above, the policies of rows 2, 6, 7 and 8 include “Normal” as the “Interface” parameter but have different “Security-enhancing sub application” codes. Thus, the codes are part of security policies having different “Interface” parameters (but same codes as exemplified by rows 2 and 10) and security policies having the same “Interface” parameter but *different* codes (as exemplified by rows 2, 6, 7 and 8).

101. A POSITA would understand Petitioner’s interpretation of the claim to be inconsistent with context of the claim as a whole. Specifically, the claimed service code is determined based on the identified communication channel so that it can then be used to calculate the authentication response (claim 1[d]), which allows the network to authenticate the authentication response because the network also knows the identity of the communication channel upon which the authentication request was transmitted. The service codes of Naslund cannot plausibly accomplish this,

because the same code can be included in multiple security policies involving *different* “Interface” parameters (i.e., alleged “identified communication channel”). Under Petitioner’s theory on Naslund, the service codes would identify *multiple* possible communication channels, making it impossible for the network to authenticate the authentication response and/or prevent man-in-the-middle attacks.

102. A POSITA would understand that the fundamental reason that the claimed invention requires that the service code identify the channel that the authentication request was received over is to prevent “man-in-the-middle” attacks. This is accomplished by essentially “binding” the channel to the authentication response, thereby ensuring that if the man-in-the-middle communicates with the victim UE using a communication channel (e.g., Bluetooth) that is different than the established communication channel (e.g., 3G radio) with the network, the network knows to deny authentication. Petitioner’s interpretation of Naslund is inconsistent with this premise, because the “Security-enhancing sub application” codes of Naslund can be associated with *multiple* interfaces (e.g., Bluetooth *and* 3G radio)—they would not prevent man-in-the-middle attacks because the man-in-the-middle could use a different interface than the terminal (e.g., Bluetooth rather than 3G) and still be authenticated.

2. Claim 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.”

103. Petitioner states that in Naslund the authentication response RES' “is calculated using the RAND value from the authentication request.” Pet., 63. Petitioner further argues that “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.***” Pet., 64 (emphasis in original). The only support for this statement is the following argument:

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

Id. Petitioner is mistaken.

104. Even assuming that the AKA processing by the terminal of Naslund differs depending on the selected security-enhancing sub application, that still would not teach or suggest that the authentication response RES' is “***calculated on the basis***

of the determined service code.” Although Naslund does disclose functions for calculating authentication responses RES and RES' (which Petitioner does not cite or discuss), none of those functions involve using any of the alleged service codes (e.g., code “01” in Table I) as part of those calculations. Indeed, Naslund does not teach or suggest that any of the “Security-enhancing sub application” codes are used in any function or calculation to generate authentication response RES'. This is in stark contrast to RAND, which actually is used to calculate the authentication response RES. See Ex. 2003, 24 (“the USIM computes $RES = f_{2K}(RAND)$ ”). I note that Naslund teaches “**comput[ing]** a response and/or one or more keys ***based on*** the challenge RAND (and the stored security key),” which evidences to a POSITA that Naslund likewise understood “computing” (or calculating) a response “based on” a particular parameter (e.g., RAND) to involve using that parameter in the calculation. Ex. 1005, 14:26-28. A POSITA would not understand the alleged authentication response of Naslund to be “calculated on the basis of the determined service code,” because Naslund does not use the “Security-enhancing sub application” code (alleged “service code”) as part of any calculation.

105. Petitioner contends that the “selected security-enhancing sub application is dependent on the service code, and therefore RES' is, by extension, calculated based on the service code.” Pet., 64. But even assuming that the AKA process changes based on the selected sub application code, that would not mean

that RES' is “**calculated** based on the service code.” As discussed above, the sub application code forms no part of the calculation of RES'. Indeed, simply “selecting among” different “customized security-enhancing modules or sub application” (Ex. 1005, 17:5-8) to perform AKA operations does not teach or suggest calculating RES' based on the code.

106. Additionally, Claim 1[e] requires that “the authentication response **depends on the identified communication channel** in that the response is calculated on the basis of ... the determined service code.” However, the alleged service code of Naslund does not depend on the identified communication channel as explained with respect to Claim 1[d]. To the contrary, the same code can be used in multiple security policies having **different** “Interface” parameters (e.g., Normal, WLAN) and different codes can be used in different security policies having the **same** “Interface” parameter. Thus, while the security-enhancing sub application is dependent on its corresponding code, the code is not dependent on any identified communication channel.

107. Further, the plain language of Claim 1[e] requires that the authentication response is calculated on the basis of **both** “information in the authentication request and the determined service code.” While Naslund discloses that RES' is calculated on the basis of the challenge RAND (alleged “information in the authentication request”), RES' is not calculated on the basis of the alleged service

code as discussed above. A POSITA would thus understand that Naslund does not teach the latter half of this limitation.

3. Claim 2: “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.”

108. Petitioner identifies the SIM 10 (red) of Naslund as the alleged “identity module” and the network communication unit(s) 25 (blue) as the alleged “service interface (SI) module”:

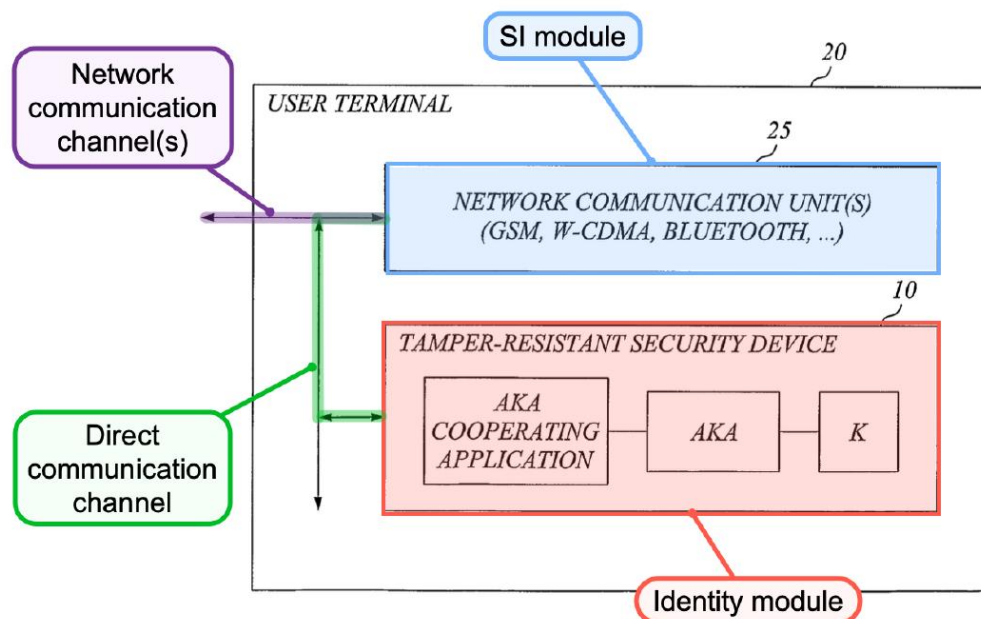


Fig. 4

Pet., 65-66.

109. Naslund does not teach that the alleged SI module is “configured to *securely* communicate with the identity module.” Naslund teaches only that the

terminal “generally has some form of communication capabilities”—Naslund is silent as to whether the communication channel (green above) between the alleged SI module and identity module is in anyway secured by the SI module. This is different than the ‘235 Patent, which teaches that the SI module “is implemented in the form one or more trusted hardware components” to “provide a secure communication channel.” Ex. 1001, 8:1-5. The Petition does not identify a comparable teaching in Naslund.

110. Naslund also does not teach that the alleged SI module is “configured to ... ***to identify*** the communications channel through which the authentication request was received.” Naslund is silent as to which component of the terminal performs the interface identification, and instead only generally states that “the terminal (mobile)” determines the interface. See Ex. 1005, 19:23-29. Although Naslund is silent on this issue, it strongly suggests to a POSITA that the interface identification would be performed by the SIM. *Id.* at 23:21-23 (“[A]ll AKA related processing takes place on the SIM, including the security enhancing step.”). In contrast, the ’235 Patent teaches that the SI module may be “configured to ***generate a service code (SC) identifying the specific service interface*** used to setup a wired or a wireless communication channel” and may rely on a look-up table for that purpose. Ex. 1001, 7:52-60.

4. Claim 3[a]: “the terminal modifying the authentication information on the basis of the identified communications channel”

111. Petitioner alleges that Naslund teaches that its terminal modifies the alleged authentication information (i.e., “the authentication request” received from the network) “on the basis of the identified communication channel” because “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.” Pet., 67.

112. Naslund does not teach or suggest that the identified channel, or even the service code for that matter, serves as the basis for the alleged modified authentication request, as explained with respect to Claim 1[e]. Indeed, the same code (i.e., security-enhancing sub application) can be used for *different* “Interface” parameters (e.g., Normal, WLAN) and different codes can be used in different security policies having the *same* “Interface” parameter. A POSITA would thus understand that the identified channel cannot serve as “the basis” of those modifications. Naslund does not rely on or use the identified channel as part of any of its disclosed mathematical functions, including the alleged function for “modifying” the authentication response. In contrast, the ’235 Patent teaches modifying authentication information on the basis of an identified channel by using the service code (SC) and RAND (i.e., “authentication information”) as part of a function to generate RAND’. Ex. 1001, 9:60-66.

5. Claim 4: “the terminal modifying the authentication response on the basis of the identified communications channel.”

113. Petitioner alleges that Naslund discloses “the terminal modifying the authentication response on the basis of the identified communications channel,” because 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. Pet., 69-70 (emphasis added). This is essentially the same theory applied to Claim 3[a] and is incorrect for the same reasons discussed there.

6. Claim 5[b]-[c]: “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 determining on the basis of the expected service code an expected response.”

114. Petitioner asserts that the alleged “expected service code” is “generated on the basis of *the type of communication channel* the service request was sent to the network.” However, this assertion is premised on the same logic offered by Petitioner with respect to Claims 1[d] and 1[e]. Specifically, Petitioner again incorrectly asserts that the alleged service code of Naslund is associated with the identified communication channel and that the authentication response is calculated on the basis of the alleged service code. Pet., 71-72. For Claim 5, Petitioner argues that Naslund’s network must necessarily follow this same process “to carry out their cryptographic algorithms” by generating the expected service code and expected

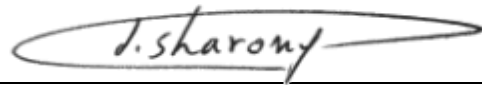
response. *Id.* Consequently, Naslund does not teach or suggest this limitation for the same reasons discussed with respect to Claims 1[d] and 1[e] above.

IX. CONCLUSION

115. In addition to the opinions and evidence expressed herein, I reserve the right to rebut any arguments made or evidence presented in response to this report. I also reserve the right to supplement this report based on further investigation or analysis.

116. I declare that all statements made herein of my knowledge are true, and that all statements made on information and belief are believed to be true, and 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 Title 18 of the United States Code. I further declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Dated: May 27, 2025

A handwritten signature in cursive script, reading "J. Sharony", is written over a horizontal line.

Jacob Sharony, Ph.D.

APPENDIX A

Seasoned professional with over 35 years experience and expertise in information communications technologies (ICT), wireless networks, mobile devices/applications, data capture and sensing; visionary, creative and innovative with strong technology and business skills.

EXPERIENCE

MOBIUS CONSULTING, Huntington Station, NY

2004 –

Founder, Principal Consultant

- Professional consulting services in mobile wireless strategy, technologies, systems and applications.
- “Trusted Advisor” role facing large clients in telecom, vertical enterprises and government, building trust and relationships.
- Expertise includes WiFi, 4G LTE and 5G, WiMAX, picocell/femtocell, DAS, mesh networking, Internet of Things (IoT), M2M, RFID, RTLS, smart antennas, MIMO/beamforming, cloud computing, mobile crowd sourcing/sensing, enterprise mobility, security protocols, mobile embedded devices, device management, mobile applications/services, LBS, VoIP, video streaming, Zigbee, Bluetooth, sensor networks, RTLS, smart grid, m-health, m-learning, smart home networking.
- System and network protocol analysis, modeling and simulations of wireless systems (e.g., WiFi, LTE) for network performance assessment and optimization.
- Participated in a lead role in several medium-large projects in various vertical, enterprise and government/military markets, e.g., smart grid, mobile health, WiFi and 4G deployments.
- Selected consulting engagements are listed below: Lattice Semiconductor, SiBEAM, Powerwave Technologies, Time Warner Cable, and Corning-MobileAccess.

COLUMBIA UNIVERSITY, New York, NY

2010 –

Adjunct Professor

- Professor of Electrical Engineering. Teaching graduate courses on advanced wireless technologies: mmWave Wireless Communications and Applications for 5G/6G, Wireless Sensing (RFID, RTLS, M2M communications, smart grid/energy, smart infrastructure, intelligent transportation, m-health).

LATTICE SEMICONDUCTOR, Sunnyvale, CA

2014 – 2016

CTO Office Senior Advisor

Developing 5G solutions using mmWave and Phased Array Antenna technologies. Applications include ‘wireless fiber’ backhaul/front-haul, connected cars, in-home connectivity.

SIBEAM, Silicon Valley

2014 – 2016

Technology Strategy Senior Consultant

Developing intelligent millimeter wave (60 GHz) technologies for wireless communications (802.11ad) and fixed access solutions for 5G.

POWERWAVE TECHNOLOGIES, Santa Ana, CA

2011 – 2013

CTO Office Senior Principal Consultant / VP Innovation

- Leading innovation, strategy and development of HetNets, DAS and small cells (picocell) solutions using 4G LTE and WiFi technologies to enhance coverage and capacity of wireless network infrastructure.

CENTER OF EXCELLENCE IN WIRELESS & IT, SUNY, Stony Brook, NY

2006 – 2010

Director, Network Technologies Research Division

- Leading network technologies research, development and commercialization efforts
- Industry liaison, working on smart energy, wireless healthcare and intelligent transportation solutions.
- Deployed mobile WiMAX pico/femto solution as part of the 4G-campus initiative.
- Key contributor to the Long Island Broadband Wireless Access Initiative using WiFi and 4G.

- TIME WARNER CABLE**, Stamford, CT **2007 – 2008**
Wireless Strategy & Development Senior Consultant
- Worked on a large wireless project involving WiFi, WiMAX and 3G with advanced mobile devices.
 - Developed concept and product requirements documents, architecture and RF design, and test plans.
 - Supported the business development group on femtocells models, MVNO's models and services, etc.
- MOBILE-ACCESS (Acquired by Corning)**, Vienna, VA **2006 – 2008**
CTO Office DAS Strategy & Development Senior Consultant
- Worked with the CTO and senior engineers to develop WiFi DAS systems.
 - Developed detailed analysis and novel method to support MIMO (802.11n) in DAS systems.
- MOTOROLA (formerly Symbol Technologies)**, Holtsville, NY **1997 – 2005**
Senior Director, Technology Strategy and Development **2003 – 2005**
- Served as “the eyes of the company” – Charter was to identify and evaluate emerging/disruptive technologies, and conduct technology/business due diligence of possible partners/acquisitions. Team leader.
 - Guided the company technology roadmap by generating Technology Position Statements (TPS). Selected topics include: 802.11a/b/g migration strategy, 802.11e (QoS), Broadband Wireless Access - 802.16d/e fixed and mobile WiMAX, mesh networks, RFID, RTLS, and MIMO. These TPS were fact based and relied on results obtained through modeling, analysis and simulations.
 - Explored a new family of products based on multi-point MIMO architecture in mesh wireless networks.
 - Investigated VoIP capacity in 802.11a/b/g networks and initiated work on admission control algorithms/policies.
 - Researched and developed new mobile applications delivering multimedia-rich content to heterogeneous networked mobile devices.
 - Developed strategic alliances and led technology initiatives with technology/business partners.
 - Participated actively in IEEE 802.11, 802.15 and 802.16 standards meetings.
 - Awarded several patents.
- Senior Director, Research and Development** **1997 – 2003**
- Initiated and led several R&D programs in wireless LAN technologies: intelligent access point, reliable multicast video streaming, mobile device management/security and spatial wireless switching.
 - Conceived, investigated and developed a novel wireless switching architecture based on MIMO technology.
 - Conducted innovative research in WLAN QoS, Bluetooth interference mitigation, multicast video streaming, mobile security, RFID, RTLS - location tracking (RSSI/TDOA), VoIP and smart antennas.
 - Participated in strategic planning and impacted the technology/business direction of the company.
 - Awarded several patents.
- BAE SYSTEMS**, Greenlawn, NY **1994 – 1997**
Research Scientist
- Led the advanced mobile networking group.
 - Developed tactical mesh-based wireless network systems for DoD.
 - Worked on advanced antenna techniques including beam steering/switching.
 - Awarded several patents.
- NEC RESEARCH INSTITUTE**, Princeton, NJ **1992 – 1994**
Research Fellow
- Worked on optical interconnects for parallel processing.
 - Investigated multi-dimensional switches using wavelength, space and time.
 - Designed a wavelength router/switch using free-space optics.
- IBM RESEARCH CENTER**, Hawthorne, NY **1990 – 1992**
Research Associate
- Developed and prototyped a gigabit switch.
 - Built a testbed of multi-wavelength optical network.
 - Developed algorithms for WDMA using AO tunable filters.

Head of Fiber-optics Systems Engineering

- Pioneered security products using fiber optic sensors.
- Conducted research & development in fiber optic sensors.
- Co-developed and deployed a large fiber optic data communications network.

EDUCATION

COLUMBIA UNIVERSITY, New York, NY

- Ph.D., Electrical Engineering, 1993.
- M.Phil, Electrical Engineering, 1991.

TEL AVIV UNIVERSITY, Tel Aviv, Israel

- MBA, Recanati Business School, 1989.
- MSc., Electrical Engineering, 1984.
- BSc., magna cum laude, Electrical Engineering, 1979.

PUBLICATIONS / PATENTS / OTHER

- Numerous publications in proceedings and conference papers.
- Numerous US and international patents issued.
- Served on several government agencies expert panels (NSF, NIH).
- IEEE Life Senior Member.
- Featured speaker on several industry sponsored webinars.
- Served as an expert witness/consultant in District Court, IPR, PGR, ITC, FRAND, PCA, AAA cases.

COURSES TAUGHT

- Introduction to Auto ID and Data Capture (AIDC) Technologies (State University NY, Stony Brook)
- Wireless Sensing Networks (Columbia University)
- mmWave Communications and Applications for 5G/6G (Columbia University)

RECENT EXPERT WITNESS CONSULTING¹

- 2025: Samsung Electronics v. KPN (IPR)
- 2025: Pegasus Wireless v. Verizon Wireless et al. (Litigation)
- 2024: Cisco Systems Inc. v. Video Solutions (IPR)
- 2024: S.M.R Innovations LTD and Y.M.R Tech LTD v. Apple (Litigation)
- 2024: Zebra Technologies v. OnAsset Intelligence (Litigation)
- 2023: Varia Holdings v. Apple (Litigation)
- 2023: Maxell Ltd. v. Samsung Electronics (Litigation)
- 2023: Ericsson Inc. and Oracle Corporation v. Telecom Network Solutions (IPR)
- 2023: OZMO Licensing v. Dell Technologies (Litigation/IPR)
- 2022: Howlink Global v. AT&T (Litigation)
- 2022: Cleveland Medical Devices v. ResMed Corp (Litigation/IPR)
- 2022: Lone Star Systems v. Zebra Technologies (Litigation/IPR)
- 2022: Telecom Network Solutions v. AT&T, Verizon, and T-Mobile (Litigation/IPR)
- 2021: BillJCo v. Apple (Litigation/IPR)
- 2021: BillJCo v. Cisco Systems et al. (Litigation)
- 2021: Zebra Technologies v. OnAsset Intelligence (ITC)
- 2021: CellSpin Soft v. Under Armour (Litigation)
- 2021: CellSpin Soft v. Nike (Litigation)
- 2021: Intellectual Ventures v. Hewlett Packard Enterprise (Litigation/IPR)

¹ Represented parties are underlined.

- 2021: AEGIS v. Hisense (Litigation)
- 2020: Soter Technologies v. IP Video Corp. et al (Litigation)
- 2020: Intellectual Tech v. Zebra Technologies (Litigation)
- 2020: Uniloc v. Apple (Litigation)
- 2020: American Patents v. Juniper Networks (Litigation)
- 2020: Proxicom Wireless v. Target Corporation (Litigation)
- 2020: Sol IP v. AT&T et al. (Litigation)
- 2019: Cellular Evolution v. AT&T et al. (Litigation)
- 2019: Philips v. HTC (Litigation, UK)
- 2019: Ericsson v. Tishman Interiors (AAA Arbitration)
- 2019: Uniloc v. Samsung, Huawei (Litigation)
- 2018: Intel et al. v. Hera Wireless (IPR)
- 2018: Deutsche Telecom v. The Republic of India (UNCITRAL Arbitration, Paris Tribunal)
- 2017: Devas v. The Republic of India (UNCITRAL Arbitration, The Hague Tribunal)
- 2017: RPX Corp. et al. v. Iridescent Networks (IPR)
- 2017: Intellectual Ventures v. FedEx (Litigation)
- 2017: FedEx v. Intellectual Ventures (IPR)

PREVIOUS TESTIMONY

- *Deutsche Telekom AG v. The Republic of India*, PCA Case No. 2014-10 (UNCITRAL) Expert Reports + Arbitration Hearing.
- *Devas (Mauritius) Ltd. et al v. The Republic of India*, PCA Case No. 2013-09 (UNCITRAL) Expert Reports + Arbitration Hearing.
- *Philips v. HTC*, Claim HP-2015-000063 (UK) Expert Report.
- *Ruckus Wireless, Inc. et al v. Hera Wireless S.A.*, Case IPR2018-01419 (PTAB) Expert Declaration.
- *Ruckus Wireless, Inc. et al v. Hera Wireless S.A.*, Case IPR2018-01736 (PTAB) Expert Declaration.
- *Intel Corporation v. Hera Wireless S.A.*, Case IPR2018-01702 (PTAB) Expert Declaration.
- *Ruckus Wireless, Inc. et al v. Hera Wireless S.A.*, Case IPR2018-01418 (PTAB) Expert Declaration.
- *Ruckus Wireless, Inc. et al v. Hera Wireless S.A.*, Case IPR2018-01739 (PTAB) Expert Declaration.
- *Intel Corporation et al v. Hera Wireless S.A.*, Case IPR2018-01700 (PTAB) Expert Declaration.
- *Intel Corporation et al v. Hera Wireless S.A.*, Case IPR2018-01701 (PTAB) Expert Declaration.
- *Ruckus Wireless, Inc. et al v. Hera Wireless S.A.*, Case IPR2018-01732 (PTAB) Expert Declaration.
- *Ruckus Wireless, Inc. et al v. Hera Wireless S.A.*, Case IPR2018-01737 (PTAB) Expert Declaration.
- *Intel Corporation et al v. Hera Wireless S.A.*, Case IPR2018-01686 (PTAB) Expert Declaration.
- *Ruckus Wireless, Inc. et al v. Hera Wireless S.A.*, Case IPR2018-01420 (PTAB) Expert Declaration.
- *Intel Corporation et al v. Hera Wireless S.A.*, Case IPR2018-01687 (PTAB) Expert Declaration.
- *Ruckus Wireless, Inc. et al v. Hera Wireless S.A.*, Case IPR2018-01738 (PTAB) Expert Declaration.
- *RPX Corporation et al v. Iridescent Networks, Inc. (McEwen, Kathy, inventor)*, Case IPR2018-00254 (PTAB) Expert Declaration.
- *RPX Corporation et al v. Iridescent Networks, Inc. (McEwen, Kathy, inventor)*, Case IPR2017-01661 (PTAB) Expert Declaration.
- *RPX Corporation et al v. Iridescent Networks, Inc.*, Case IPR2017-01662 (PTAB) Expert Declaration.
- *Intellectual Ventures II LLC v. FedEx Corp.*, (2:16-cv-00980), Expert Report + Deposition + Trial (Texas Eastern District Court).
- *FedEx Corp. v. Intellectual Ventures II LLC*, Case IPR2017-00729 (PTAB) Expert Declaration.
- *FedEx Corp. v. Intellectual Ventures II LLC*, Case IPR2017-02030 (PTAB) Expert Declaration.
- *FedEx Corp. v. Intellectual Ventures II LLC*, Case IPR2017-00741 (PTAB) Expert Declaration.
- *Uniloc USA, Inc., Uniloc Luxembourg, S.A., and Uniloc 2017 LLC (Uniloc) v. Samsung*, (2:18-cv-00042) Expert Report + Deposition.
- *Uniloc USA, Inc., Uniloc Luxembourg, S.A., and Uniloc 2017 LLC (Uniloc) v. Samsung*, (2:18-cv-00044) Expert Report + Deposition.
- *SoL IP v. AT&T et al.*, (2:18-cv-00526), Expert Report + Deposition.
- *Juniper Networks v. American Patents*, Case IPR2020-01114 (PTAB) Expert Declaration.

- *Juniper Networks v. American Patents*, Case IPR2020-01115 (PTAB) Expert Declaration.
- *Intellectual Tech v. Zebra Technologies*, (6:19-cv-00628) Expert Declaration.
- *Aegis 11 S.A. v. Belkin Int'l, Inc.*, Civ. Nos. 19-1161-RGA, -1162-RGA, and 1163-RGA Expert Declaration.
- *Aegis 11 S.A. v. TTE Tech., Inc.*, Civ. No. 19-1165-RGA Expert Declaration
- *Aegis 11 S.A. v. Funai Electric Co.*, Civ. No. 20-03890
- *AEGIS v. Hisense*, (1:20-cv-03891) Expert Declaration.
- *Soter Technologies, LLC v. IP Video Corp. et al*, SDNY 20-cv-05007(LJL) Expert Declaration.
- *Soter Technologies, LLC v. IP Video Corp. et al*, EDNY 2:20-cv-02989(GRB)(AKT) Expert Declaration + Deposition.
- *Cellspin Soft, Inc. v. Nike, Inc.*, NDCA 4:17-cv-05931YGR Expert Report.
- *Cellspin Soft, Inc. v. Under Armour, Inc.*, NDCA 4:17-cv-05932YGR Expert Report.
- *BillJCo, LLC v. Cisco Systems, Inc. et al.*, EDTX 2:21-cv-181, 183-JRG Expert Reports + Deposition.
- *BillJCo, LLC v. Apple, Inc.*, WDTX 6:21-cv-528-ADA Expert Declaration.
- *Zebra Technologies v. OnAsset Intelligence, Inc.*, ITC Washington DC, Investigation No. 337-TA-1278 Expert Reports on Infringement & Validity + Deposition + Trial/Hearing.
- *Intellectual Tech LLC v. Zebra Technologies*, WDTX 6:19-cv-00628-ADA Expert Report.
- *Hewlett Packard Enterprise v. Intellectual Ventures II LLC*, Case IPR2021-01377 (PTAB) Expert Declaration + Deposition.
- *Hewlett Packard Enterprise v. Intellectual Ventures II LLC*, Case IPR2022-00096 (PTAB) Expert Declaration + Deposition.
- *Ericsson Inc. and Oracle Corporation v. Telecom Network Solutions LLC*, Case IPR2022-1572 (PTAB) Expert Declaration.
- *Ericsson Inc. and Oracle Corporation v. Telecom Network Solutions LLC*, Case IPR2022-1573 (PTAB) Expert Declaration.
- *Zebra Technologies v. Lone Star Systems*, Case IPR2022-01374-01377 (PTAB) Expert Declarations + Deposition.
- *Howlink Global v. AT&T*, EDTX 2:22-cv-00040-JRG, Expert Report + Deposition.
- *Unified Patents LLC v. OZMO Licensing LLC*, Case IPR2023-02060 (PTAB) Expert Declaration.
- *Cisco Systems Inc. v. Video Solutions PTE LTD.*, Case IPR2024-00194 (PTAB) Expert Declarations + Deposition.
- *Varia Holdings v. Apple*, EDNY 1:23-cv-07477-RPK-VMS, Expert Declarations + Depositions.
- *Unified Patents v. BSD Crown*, Ex Parte Reexamination of U.S. Patent No. 6,389,473, Expert Declaration.
- *Zebra Technologies v. OnAsset Intelligence*, NDTX 3:21-cv-00055-K Inc., Expert Report + Deposition.
- *ResMed Corp v. Cleveland Medical Devices*, Case IPR2023-00565 (PTAB) Expert Declaration + Deposition.
- *Cleveland Medical Devices v. ResMed Corp*, DE 1:22-cv-00794-GBW, Expert Declaration.
- *S.M.R Innovations LTD and Y.M.R Tech LTD v. Apple*, WDTX 6:23-cv-479-ADA, Expert Declaration.
- *Samsung Electronics, LTD v. Maxell, LTD*, Case IPR2024-00735/00777 (PTAB) Expert Declarations
- *Cisco Systems, Inc. v. Video Solutions PTE. LTD*, Case IPR2024-00194 (PTAB) Expert Declaration.

ADDENDUM

Publications

- J. Sharony, "Understanding Het-Nets, Antennas and other Advanced Techniques in LTE-Advanced; Advanced Systems and Techniques," LTE-Advanced: Understanding 3GPP Release 10 and Beyond – Workshop presented by 4G Americas, Marina del Rey, CA, October 2012.
- J. Sharony, V. Ramanna, "Self Learning Real Time Location Tracking in Wireless Sensor Networks," Accepted to WiCOM, The 5th International Conference on Wireless Communications, Networking and Mobile Computing, China, 2009.
- J. Sharony, "Introduction to Wireless MIMO – Theory and Applications", IEEE LI, November 2006.
- J. Sharony, M. Sen, "Bandwidth management in 802.11 wireless LANs," ICC 2004 - IEEE International Conference on Communications, vol. 27, no. 1, Paris, France, June 2004 pp. 3837-3843.
- L-T.Cheok, J.Sharony and A.Eleftheriadis, "A SMIL-enabled Mobile Shopping Mall Application," SMILEurope Conference, Paris, France, February 2003.
- L-T.Cheok, J.Sharony and A.Eleftheriadis, "Symshop: A Mobile Shopping Mall Application," International Conference on Mobile and Ubiquitous Multimedia (MUM), Oulu, Finland, December 2002.
- J. Sharony, "Effective Throughput of 802.11 Wireless LAN with Interference from Nearby Cells," Proc. of Mobile Multimedia Communications (MoMuC), 7th International Workshop, Tokyo, Japan, 2000.
- J. Sharony, "An Architecture for Mobile Radio Networks With Dynamically Changing Topology Using Virtual Subnets," Mobile Networks & Applications, vol. 1, no. 1, 1996 pp. 75-86.
- J. Sharony, "A Multi-Star Optical Backbone Network Suitable for Distributed Microcellular Wireless Systems," Proc. of IEEE GLOBECOM'96, London, UK, November, 1996.
- J. Sharony, A. C. Sevdinoglou, "On-line distributed TDMA/FDMA/CDMA Link Assignment in Mobile Radio Networks with Flexible Directivity," Hazeltine Technical Bulletin, 1996.
- Y. Li, T. Wang, Z. G. Pan, J. Sharony, "Minimum-Complexity Free-Space Optical Nonblocking Networks for Multicast Interconnect Applications," Optical Letters, vol. 19, no. 8, April 1994 pp. 515-517.
- Y. Li, T. Wang, Z. G. Pan, J. Sharony, "Complexity-Minimized Optical Non-Blocking Interconnects for Multicast Computer Communications," Proceedings of the SPIE - Advances in Optical Information Processing VI 2240:192-204, 1994.
- Y. Li, T. Wang, J. Sharony, "Free-Space Optical Interconnects Using Connectivity-Enhanced Mesh-Based Networks," Optical Engineering, vol. 33, no. 5, 1994 pp. 1532-1542.
- Y. Li, T. Wang, Z. G. Pan, J. Sharony, "Free-Space Optical Implementations of Connectivity-Enhanced Mesh-Based Networks," Proceedings of the SPIE - International Society for Optical Engineering Optoelectronic Interconnects II, vol. 2153 pp. 57-68, 1994.
- J. Sharony, T. Stern, Y. Li, "The universality of multidimensional switching networks," IEEE/ACM Transactions on Networking, vol. 2, no. 6, December 1994 pp. 602-612.
- J. Sharony, "Broadcast and switch – A new class of WDM networks for high switching-speed, high connectivity applications," in Photonics in Switching Topical Meeting'93 Digest, Palm Springs, CA, Mar. 1993.
- J. Sharony, K. W. Cheung, T. E. Stern, "The Wavelength Dilation Concept in Lightwave Networks – Implementation and System Considerations," Journal of Lightwave Technology, vol. 11, no. 5/6, May/June 1993 pp. 900-907.
- J. Sharony, "Architectures of Dynamically Reconfigurable Wavelength Routing/Switching Networks," Ph.D. Thesis, Columbia University, May 1993.
- J. Sharony, K. W. Cheung, T. E. Stern, "Wavelength Dilated Switches (WDS) – A New Class of Suppressed Crosstalk, Dynamic Wavelength-Routing Crossconnects," OFC'92, paper TuO3, San Jose, CA, Feb 1992.
- J. Sharony, C. Georgiou, "Wavelength Selective Optical Crossconnect," IBM Technical Disclosure Bulletin, vol. 34, no. 10A, March 1992.
- J. Sharony, S. Jiang, T. Stern, K. Cheung, "Wavelength Rearrangeable and Strictly Non-Blocking Networks," Electronics Letters, vol. 28, no. 2, March 1992 pp. 536-537.
- J. Sharony, K. W. Cheung, T. E. Stern, "The Wavelength Dilation Concept – Implementation and System Considerations," Proc. ICC'92, paper 330.3, Chicago, IL, June 1992.
- J. Sharony, K. W. Cheung, T. E. Stern, "Wavelength Dilated Switches (WDS) – A New Class of High Density, Suppressed Crosstalk, Dynamic Wavelength-Routing Crossconnects," IEEE Photonics Technology Letters, vol. 4, no. 8, August 1992 pp. 933-935.

- Y. Li, T. Jiang, J. Sharony, "Massively Parallel Free-Space Optical Clos Network Using Wavelength-Division Multiple Access," Electronics Letters, vol. 28, no.21, October 1992 pp. 2001-2002.
- J. Sharony, T. E. Stern, K. W. Cheung, "Extension of Classical Rearrangeable and Non-Blocking Networks to the Wavelength Dimension," Proc. of IEEE GLOBECOM'92, December, 1992.
- J. Sharony, "Bounds on Threshold Effects in Frequency Estimation," Master Thesis, Tel Aviv University, April 1984.

Issued U.S. Patents

- 10,200,924 - Small-cell gateway configured for multiple air interfaces
- 10,080,177 - Unlicensed spectrum offload architecture for small-cell base stations
- 10,028,188 - Location processing in small cells implementing multiple air interfaces
- 9,854,489 - Location processing in small cells implementing multiple air interfaces
- 9,807,657 - Small-cell gateway configured for multiple air interfaces
- 9,474,500 - Method and system for transfer of cardiac medical image data files
- 9,161,273 - Small cells implementing multiple air interfaces
- 9,148,835 - Small cells implementing multiple air interfaces
- 9,143,996 - Small cells implementing multiple air interfaces
- 9,125,121 - Small cells implementing multiple air interfaces
- 9,088,923 - Small cells implementing multiple air interfaces
- 9,014,702 - Wireless location processing in small cells implementing multiple air interfaces
- 7,827,610 - Wireless LAN intrusion detection based on location
- 7,778,649 - System and method for asset location in wireless networks
- 7,706,809 - RF tracking system and method
- 7,668,201 - Bandwidth management in wireless networks
- 7,596,388 - Sectorized wireless communication network operating under 802.11 specifications
- 7,426,383 - Wireless LAN intrusion detection based on location
- 7,373,154 - System and method for asset location in wireless networks
- 7,174,172 - System and method for asset location in wireless networks
- 7,164,929 - Method and apparatus for location tracking in a multi-path environment
- 7,069,024 - System and method for determining location of rogue wireless access point
- 7,039,358 - Coexistence techniques in wireless networks
- 7,019,663 - RF tracking system and method
- 6,990,587 - Cryptographic architecture for secure, private biometric identification
- 6,925,094 - System and method for wireless network channel management
- 6,853,293 - Wearable communication system
- 6,735,445 - System and method for medium access control in a wireless network
- 6,577,609 - Local addressing of mobile units in a WLAN with multicast packet addressing
- 6,411,608 - Method and apparatus for variable power control in wireless communications systems
- 5,953,143 - Multidimensional switching networks
- 5,742,593 - On-line distributed TDMA/FDMA/CDMA link assignment in mobile radio networks with flexible directivity
- 5,652,751 - Architecture for mobile radio networks with dynamically changing topology using virtual subnets
- 5,495,356 - Multidimensional switching networks
- 4,867,820 - Preparation of laminated structure containing an optical fiber
- 4,847,596 - Wallpaper comprising an optical fibre

Issued International Patents

- EP2974520 - Unlicensed spectrum offload architecture for small-cell base stations
- EP1906294 - Wearable communication system
- EP1851978 - System and method for asset location in wireless networks
- EP1678960 - System and method for determining location of rogue wireless access point
- EP0886981 - An architecture for mobile radio networks with dynamically changing topology using virtual subnets
- EP1552632 - Apparatus and method for wireless network channel management

- EP1207654 - Coexistence techniques in a gateway between Bluetooth and WLAN wireless networks
- CA2599012 - Sectorized wireless communication network operating under 802.11 specifications
- AU2011202551 - Sectorized wireless communication network operating under 802.11 specifications
- CA2599406 - System and method for asset location in wireless networks
- AU783921 - Coexistence techniques in wireless networks

Published U.S. Patent Applications

- 20180220347 - SMALL-CELL GATEWAY CONFIGURED FOR MULTIPLE AIR INTERFACES
- 20170150412 - LOCATION PROCESSING IN SMALL CELLS IMPLEMENTING MULTIPLE AIR INTERFACES
- 20150382272 - UNLICENSED SPECTRUM OFFLOAD ARCHITECTURE FOR SMALL-CELL BASE STATIONS
- 20150365861 - SMALL-CELLS GATEWAY CONFIGURED FOR MULTIPLE AIR INTERFACES
- 20150257077 - LOCATION PROCESSING IN SMALL CELLS IMPLEMENTING MULTIPLE AIR INTERFACES
- 20130090119 - LOCATION PROCESSING IN SMALL CELLS IMPLEMENTING MULTIPLE AIR INTERFACES
- 20130089077 - SMALL CELLS IMPLEMENTING MULTIPLE AIR INTERFACES
- 20130089072 - SMALL CELLS IMPLEMENTING MULTIPLE AIR INTERFACES
- 20130089071 - SMALL CELLS IMPLEMENTING MULTIPLE AIR INTERFACES
- 20130089070 - SMALL CELLS IMPLEMENTING MULTIPLE AIR INTERFACES
- 20130089069 - SMALL CELLS IMPLEMENTING MULTIPLE AIR INTERFACES
- 20130084873 - SMALL CELLS IMPLEMENTING MULTIPLE AIR INTERFACES
- 20080201377 - Wireless LAN Intrusion Detection Based on Location
- 20080182593 - System and Method for Asset Location in Wireless Networks
- 20070105566 - System and method for asset location in wireless networks
- 20060221928 - Wireless device and method for wireless multiple access
- 20060221904 - Access point and method for wireless multiple access
- 20060221873 - System and method for wireless multiple access
- 20060211372 - Coexistence techniques in wireless networks
- 20060194616 - Sectorized wireless communication network operating under 802.11 specifications
- 20060194587 - System and method for asset location in wireless networks
- 20060194568 - System and method for determining location of rogue wireless access point
- 20060172756 - System and method for clustering mobile devices in a wireless network
- 20060125631 - RF tracking system and method
- 20050153713 - Method and apparatus for location tracking in a multi-path environment
- 20050136891 - Wireless lan intrusion detection based on location
- 20050135321 - Spatial wireless local area network
- 20050113090 - System and method for determining location of rogue wireless access point
- 20050096091 - Method and system for wireless communications using multiple frequency band capabilities of wireless devices
- 20050047343 - Bandwidth management in wireless networks
- 20040157604 - System and method for medium access control in a wireless network
- 20040057459 - System and method for wireless network channel management
- 20040038695 - SYSTEM AND METHOD FOR MEDIUM ACCESS CONTROL IN A WIRELESS NETWORK
- 20040027251 - RF tracking system and method
- 20030020629 - Wearable communication system
- 20020152391 - Cryptographic architecture for secure, private biometric identification
- 20020150098 - Local addressing of mobile units in a WLAN with multicast packet addressing
- 20020018451 - Method and apparatus for variable power control in wireless communications systems

Published International Patent Applications

- WO2013036487 - Small cells implementing multiple air interfaces

- WO0227989 - Logical addressing of mobile units in a wlan with multicast packet addressing
- WO2005046256 - Method and system for wireless communication using multiple frequency band capabilities of wireless devices
- WO2009146082 - Rfid monitoring of drug regimen compliance
- WO2004019539 - System and method for medium access control in a wireless network
- WO2005060172 - Wlan with a plurality of antennas in both access point and mobile unit
- WO2006093884 - Sectorized wireless communication network operating under 802.11 specifications
- WO2014140877 - Unlicensed spectrum offload architecture for small-cell base stations
- WO2006107538 - System and method for wireless multiple access
- WO2004028054 - System and method for wireless network channel management
- WO0205578 - Method and apparatus for variable power control in wireless communications systems
- WO2005072000 - Method and apparatus for location tracking in a multi-path environment
- WO2006093710 - System and method for asset location in wireless networks
- WO2005046254 - System and method for determining location of rogue wireless access point
- WO2006083535 - System and method for clustering mobile devices in a wireless network
- WO2006107537 - Wireless device and method for wireless multiple access
- WO2006107535 - Access point and method for wireless multiple access
- WO9736444 - An architecture for mobile radio networks with dynamically changing topology using virtual subnets
- JP2017225127 - Small cells implementing multiple air interfaces
- JP2002185476 - Coexistence technique in wireless network
- CA2495618 - System and method for wireless network channel management
- CA2602569 - System and method for wireless multiple access
- CA2543459 - Method and system for wireless communication using multiple frequency band capabilities of wireless devices
- CA2602399 - Wireless device and method for wireless multiple access
- CA2602572 - Access point and method for wireless multiple access
- EP2752051 - Small cells implementing multiple air interfaces
- EP1232594 - Logical addressing of mobile units in a wlan with multicast packet addressing
- EP1678836 - Method and system for wireless communication using multiple frequency band capabilities of wireless devices
- EP1702491 - Method and apparatus for location tracking in a multi-path environment
- EP1864396 - System and method for wireless multiple access
- EP1733511 - Wlan with a plurality of antennas in both access point and mobile unit
- EP1300029 - Method and apparatus for variable power control in wireless communications systems
- EP1844615 - System and method for clustering mobile devices in a wireless network
- EP1864404 - Wireless device and method for wireless multiple access
- EP1864516 - Access point and method for wireless multiple access
- EP0886981 - An architecture for mobile radio networks with dynamically changing topology using virtual subnets
- EP1906294 - Wearable communication system
- AU9483001 - Logical addressing of mobile units in a wlan with multicast packet addressing
- AU2003272648 - System and method for wireless network channel management
- AU2006218786 - Sectorized wireless communication network operating under 802.11 specifications
- AU2003265675 - System and method for medium access control in a wireless network
- AU2001294830 - Logical addressing of mobile units in a wlan with multicast packet addressing
- GB2319439 - Network Architecture for Linking Base Stations