

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS AMERICA, INC.

SAMSUNG ELECTRONICS CO., LTD.,

Petitioners

v.

KONINKLIJKE KPN N.V.

Patent Owner

Case IPR2025-00512

U.S. Patent 8,881,235

PATENT OWNER'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

I.	INTRODUCTION	10
II.	LEVEL OF SKILL IN THE ART	11
III.	CLAIM CONSTRUCTION	11
IV.	OVERVIEW OF PATENT	11
	A. The Problem.....	11
	B. The Solution.....	14
V.	INSTITUTION SHOULD BE DENIED.....	17
	A. Grounds 1-2 Fail Because TS-33.402 Does Not Qualify as Prior Art....	17
	1. The Invention Was Conceived Before TS-33.402.....	18
	2. The Invention Was Constructively Reduced to Practice on December 15, 2008.	24
	3. The Inventor and Prosecution Counsel Exercised Reasonably Continuous Diligence.....	25
	B. Ground 1 Fails on the Merits.....	31
	1. Claim 1[a]: “the terminal sending a service request for access to a network service;”	32
	2. Claim 1[e].....	33
	3. 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.”	43
	4. Claim 4[b]: “the terminal modifying the authentication response on the basis of the identified communications channel.”	48
	5. Claim 5[a]: “the terminal sending a service request via a predetermined communications channel to the network”	51

6.	Claim 5[c]: “determining on the basis of the expected service code an expected response.”	51
7.	Claim 6[a]-[b].....	57
8.	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
9.	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
10.	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
C.	Ground 2 Fails on the Merits.....	60
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.”	64
D.	Ground 3 Fails on the Merits.....	64
1.	Claim 1[d]: “the terminal determining a service code associated with the identified communication channel”	64
2.	Claim 1[e].....	69
3.	Claim 2	74

4.	Claim 3[a].....	76
5.	Claim 4[b]	77
6.	Claim 5[b]-[c].....	77
VI.	CONCLUSION.....	78

EXHIBIT LIST

Exhibit No.	Description
2001	Expert Declaration of Jacob Sharony, PhD.
2002	Excerpt from Microsoft Computer Dictionary (5 th Ed. 2002)
2003	3GPP Technical Specification 33.102 Version 8.0.0, “Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture” (published October 2008)
2004	U.S. Patent No. 8,165,565
2005	U.S. Patent No. 7,908,484
2006	U.S. Patent No. 8,627,092
2007	U.S. Patent No. 8,265,593
2008	U.S. Patent Application Publication No. 2006/0128362
2009	Excerpt from Webster’s New World College Dictionary (4 th Ed. 1999)
2010	Declaration of Frank Muller
2011	Declaration of Erik Visscher
2012	Oct. 8, 2008 E-mail
2013	Certified Translation of Oct. 8, 2008 E-mail
2014	Attachment “Service based authentication (8-10-2008).doc” to Oct. 8, 2008 Email from Erik Visscher (Ex. 2012)
2015	Attachment “service based auth (8-10-2008).ppt” to Oct. 8, 2008 Email from Erik Visscher (Ex. 2012)
2016	Certified Copy of European Patent Application No. EP 08021705 (“EP Application”)
2017	Nov. 6, 2008 E-mail
2018	Certified Translation of Nov. 6, 2008 E-mail

Exhibit No.	Description
2019	Nov. 18, 2008 Email
2020	Certified Translation of Nov. 18, 2008 Email
2021	Nov. 24, 2008 Email (first)
2022	Certified Translation of Nov. 24, 2008 Email (first)
2023	Nov. 24, 2008 Email (second)
2024	Certified Translation of Nov. 24 2008 Email (second)
2025	Nov. 25, 2008 Email
2026	Certified Translation of Nov. 25, 2008 Email
2027	Dec. 8, 2008 Email (first)
2028	Certified Translation of Dec. 8, 2008 Email (first)
2029	Dec. 8, 2008 Email (second)
2030	Certified Translation of Dec. 8, 2008 Email (second)
2031	Dec. 9, 2008 Email (first)
2032	Certified Translation of Dec. 9, 2008 Email (first)
2033	Dec. 9, 2008 Email (Second)
2034	Certified Translation of Dec. 9, 2008 Email (second)
2035	Dec. 9, 2008 Email (Third)
2036	Certified Translation of Dec. 9, 2008 Email (third)
2037	Dec. 10, 2008 Email (first)
2038	Certified Translation of Dec. 10, 2008 Email (first)
2039	Dec. 10, 2008 Email (second)

Exhibit No.	Description
2040	Certified Translation of Dec. 10, 2008 Email (second)
2041	Computer-Generated Hourly Billing Report for Erik Visscher for August 1, 2008 to December 31, 2008
2042	Attachment “Service based authentication (8-10-2008) Review FM.doc” to Nov. 10, 2008 Email from Frank Muller in email chain of Ex. 2025
2043	Attachment “service based auth (8-10-2008) Review FM.ppt” Nov. 10, 2008 Email from Frank Muller in email chain of Ex. 2025
2044	Attachment “Service based authentication (10-12-2008) final.doc” to Dec. 10, 2008 Email from Erik Visscher of Ex. 2039
2045	Attachment “Figures service based auth (10-12-2008) final.ppt” to Dec. 10, 2008 Email from Frank Muller of Ex. 2039
2046	Travel Itinerary for Frank Muller
2047	Certified Translation of Travel Itinerary for Frank Muller
2048	October 20, 2008 Email
2049	Certified Translation of October 20, 2008 Email
2050	Photographs from October 2008 Vacation of Frank Muller
2051 - 2100	RESERVED
2101	KPN’s Original Petition and Request for Disclosure in <i>Koninklijke KPN N.V. v. Samsung Elecs. Co.</i> , No. 25-0237 (71st Dist. Ct. Harrison Cty. Tex., Mar. 3, 2025).
2102	2016 Settlement, License and Non-Assertion Agreement between Koninklijke KPN N.V. and Samsung Electronics Co., Ltd. (“Financial Conditions” Redacted)
2103	Ericsson’s Nov. 16, 2021 Invalidity Contentions in <i>Koninklijke KPN N.V. v. Telefonaktiebolaget LM Ericsson et al.</i> , No. 2:21-CV-00113-JRG

Exhibit No.	Description
2104	Signed Jury Verdict Form (Dkt. 245) in <i>Koninklijke KPN N.V. v. Telefonaktiebolaget LM Ericsson et al.</i> , No. 2:21-CV-00113-JRG (Aug. 26, 2022)
2105	Amended Final Judgment (Dkt. 325) in <i>Koninklijke KPN N.V. v. Telefonaktiebolaget LM Ericsson et al.</i> , No. 2:21-CV-00113-JRG (Aug. 9, 2023)
2106	KPN's Original Petition and Request for Disclosure in <i>Koninklijke KPN N.V. v. Samsung Elecs. Co.</i> , No. 22-0762 (71st Dist. Ct. Harrison Cty. Tex., Sept. 28, 2022) (redacted)
2107	Signed Jury Verdict Form in <i>Koninklijke KPN N.V. v. Samsung Elecs. Co.</i> , No. 22-0762 (71st Dist. Ct. Harrison Cty. Tex., Feb. 23, 2024) (redacted)
2108	Final Judgment, <i>Koninklijke KPN N.V. v. Samsung Elecs. Co.</i> , No. 22-0762 (71st Dist. Ct. Harrison Cty. Tex., May 2, 2024) (redacted)
2109	Samsung's Complaint for Declaratory Judgment of Non-Infringement (Dkt. 2) in <i>Samsung Electronics Co., Ltd. v. Koninklijke KPN N.V.</i> , No. 24-cv-01433-CFC (Dec. 31, 2024) (redacted)
2110	Samsung's Complaint for Declaratory Judgment of Non-Infringement in <i>Samsung Electronics Co., Ltd. v. Koninklijke KPN N.V.</i> (Dkt. 2) (redacted), No. 25-cv-00001-CFC (Jan. 1, 2025) (redacted)
2111	Opening Brief in Support of Motion to Dismiss First Amended Complaint (Dkt. 30) in <i>Samsung Electronics Co., Ltd. v. Koninklijke KPN N.V.</i> , No. 24-cv-01433-CFC (Apr. 7, 2025) (redacted)
2112	Opening Brief in Support of Motion to Dismiss First Amended Complaint (Dkt. 31) in <i>Samsung Electronics Co., Ltd. v. Koninklijke KPN N.V.</i> , No. 25-cv-00001-CFC (Apr. 7, 2025) (redacted)

Exhibit No.	Description
2113	Amended Complaint (Dkt. 26) in <i>Koninklijke KPN N.V. v. Telefonaktiebolaget LM Ericsson et al.</i> , No. 2:22-CV-00282-JRG (Nov. 15, 2022) (redacted)
2114	Order of Dismissal (Dkt. 236) in <i>Koninklijke KPN N.V. v. Telefonaktiebolaget LM Ericsson et al.</i> , No. 2:22-CV-00282-JRG (Jan. 17, 2024)
2115	Docket Navigator Search Results for All IPR or PGR Petitions Filed Between Jan. 1, 2025 and April 17, 2025
2116	Docket Navigator Search Results for IPR or PGR Petitions Filed by Samsung Between Jan. 1, 2025 and April 17, 2025

I. INTRODUCTION

Institution should be denied because the Petition fails to demonstrate a reasonable likelihood that at least one claim is unpatentable.

Petitioner cannot carry its burden on Grounds 1 or 2 because the primary reference—TS-33.402—does not qualify as prior art. The claimed invention was conceived before the publication date of TS-33.402 as evidenced by a draft of the '235 Patent's foreign priority application. *Infra* Section V.A.1. Moreover, the inventors and prosecution counsel exercised reasonably continuous diligence toward constructively reducing to practice, as evidenced by numerous emails and revised draft applications. *Infra* Section V.A.2-3. Even if TS-33.402 could qualify as prior art (it cannot), the combination of references nonetheless fails to disclose at least one independent claim limitation, including “calculating” or “modifying” an “authentication response” on the basis of a determined “service code” that identifies the communication channel upon which an “authentication request” was received. *Infra* Sections V.B-C.

Ground 3 challenges only a subset of claims but is fundamentally flawed nonetheless. Petitioner acknowledges that Naslund was before the Office during examination, and that the Examiner applied it. Despite this, Petitioner contends that the Examiner materially erred by “overlooking” relevant teachings of Naslund. However, the simple truth is that Naslund does not teach or suggest multiple

limitations of the challenged independent claims. *See Infra* Section V.D.

II. LEVEL OF SKILL IN THE ART

For purposes of this response only, Patent Owner Koninklijke KPN N.V. (“KPN”) does not dispute the qualifications of a person of ordinary skill in the art (“POSITA”) proposed by Petitioner. Pet., 6. KPN reserves the right to propose its own qualifications should the Board institute trial. KPN’s expert, Dr. Jacob Sharony, far exceeds these qualifications. Ex. 2001 ¶¶2-10, 42-44.

III. CLAIM CONSTRUCTION

KPN applies the plain and ordinary meaning and does not believe that express construction is necessary to resolve the parties’ disputes.

IV. OVERVIEW OF PATENT

The ’235 Patent is directed toward a system and method for preventing the misuse and disruption of mobile devices in telecommunications networks. Ex. 1001, 1:22-34. A brief overview of the prior art problem and disclosed solution are described below.

A. THE PROBLEM

Malicious code (known as “malware”) may carry out cyber-attacks by exploiting security flaws in the authentication process. *Id.*, 1:35-37. For example, malware may be used to carry out so-called “man-in-the-middle” attacks, where the

attacker injects itself between the mobile device and telecommunications network to gain illicit access to the network. *Id.*

As one example, the authentication and key agreement (“AKA”) process in a GSM network authenticates only the mobile device to the network, but not the other way around. *Id.*, 1:37-39. As conceptually depicted below, because the authentication process is only one-way, it is vulnerable to man-in-the-middle attacks where the attacker pretends to be a valid base station. *Id.*, 1:39-41.

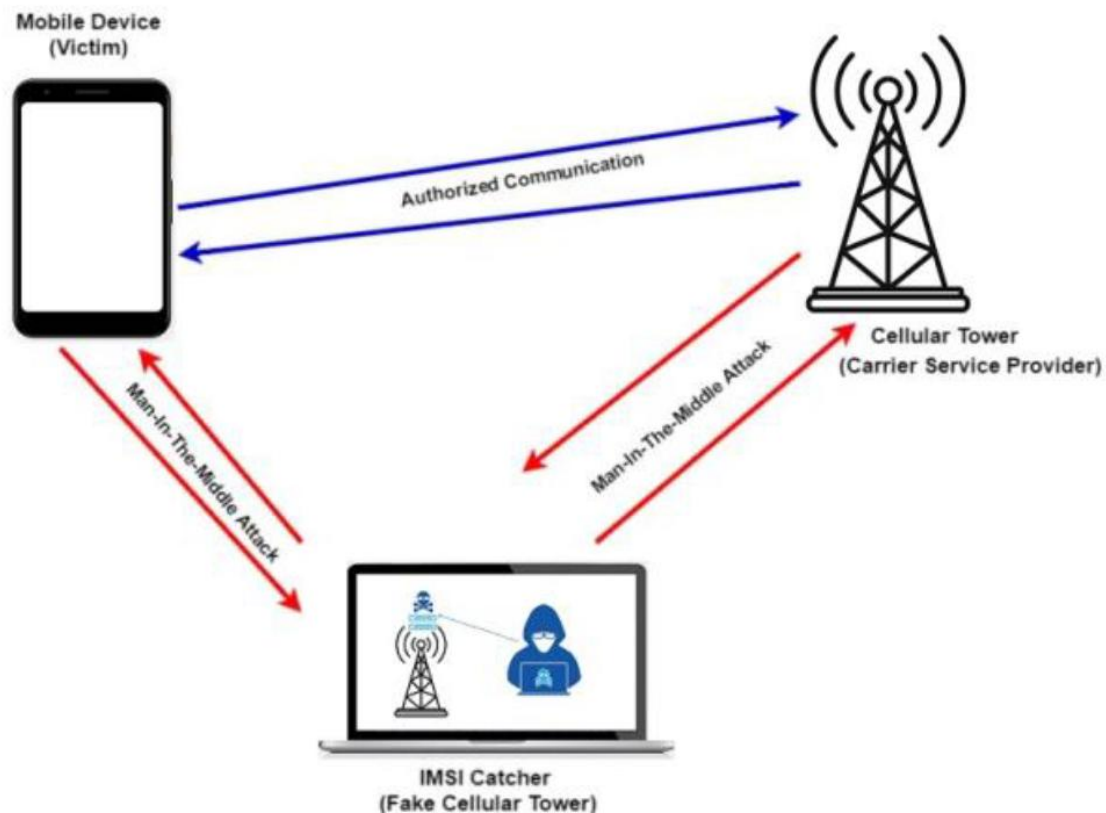
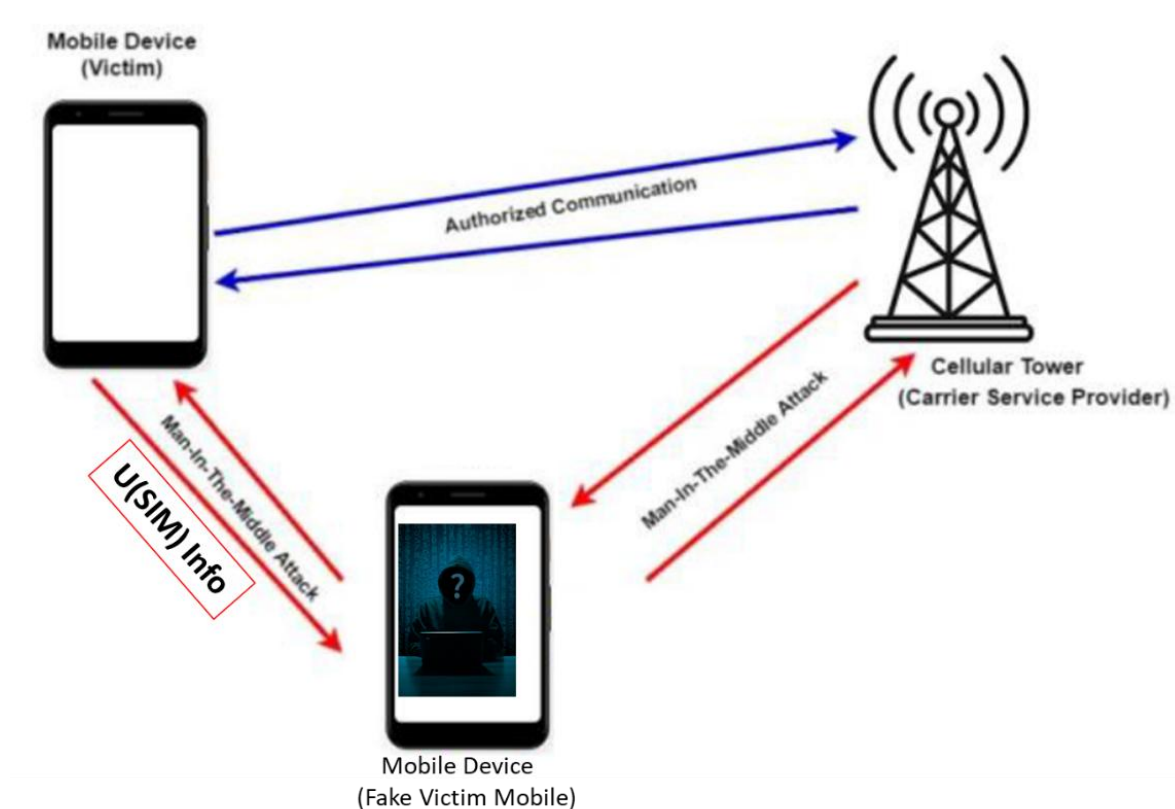


Fig. 3. Man-in-the-middle Attack.

In a UMTS network, the AKA process relies on mutual authentication to mitigate part of the threats posed by base station attacks. *Id.*, 1:41-48. Specifically,

the UMTS AKA relies on mutual authentication where the mobile device and Visitor Location Register (VLR) authenticate themselves to each other. *Id.* However, this process is still vulnerable to man-in-the-middle attacks because the attacker may pretend to be the mobile device user by using the authentication information from the (U)SIM of the victim, as conceptually depicted below. *Id.*, 1:49-54.



“Such a man-in-the-middle attack allows network access as if the connection was set up by the victim. As the network cannot distinguish between a legal situation and such attack the malware allows to set up calls on the expenses of the victim thereby causing substantial damage.” *Id.*, 1:54-69.

B. THE SOLUTION

The '235 Patent is directed toward a novel method and system for preventing man-in-the-middle attacks. While various embodiments are disclosed, this discussion focuses on two embodiments in reference to Figure 4 (reproduced below).

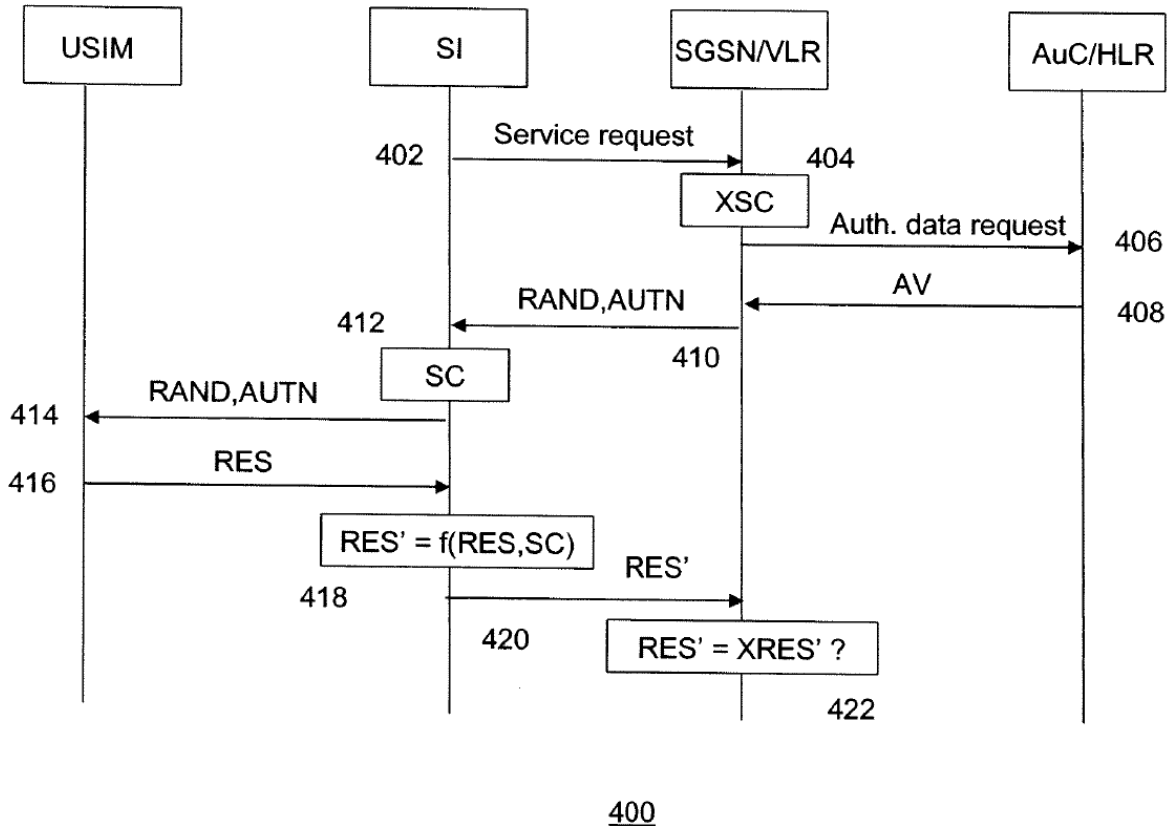


Figure 4

The process begins in step **402** with the terminal requesting service from the network, which may trigger the RF interface module of the terminal to setup a wireless communication channel between the terminal and access node of the network. Ex. 1001, 8:52-61. A service request then may be transmitted to the SGSN/VLR of the network over the channel. *Id.*

In step **404**, the SGSN/VLR may determine the service interface (e.g., Bluetooth, WiFi, GSM, UMTS) through which contact was established with the terminal. *Id.*, 8:61-64. Based on the identified service interface, an expected service code XSC may be determined using, for example, a look-up table that is substantially identical to the service table stored in the service interface (SI) module of the terminal. *Id.*, 8:64-9:4.

At step **406**, the SGSN/VLR may send an authentication data request to the AuC/HLR of the network. *Id.*, 9:5-7. In step **408**, the AuC/HLR then may generate an authentication vector AV and sends it to the SGSN/VLR. *Id.*, 9:7-11.

In step **410**, an Authentication and Ciphering request may be sent from the SGSN/VLR to the terminal. *Id.*, 9:9-12. The request may include a RAND (i.e., a random challenge) and AUTN (i.e., authentication token). *Id.*

At step **412**, the terminal may identify a service code associated with the interface used by the SI module to communicate with the RF module of the terminal, and forward the digital signal (including the RAND and AUTN) to the USIM of the terminal (step **414**). *Id.*, 9:11-16.

In this particular embodiment, at step **416** the USIM may calculate the authentication response RES *without* relying on the service code (e.g., using the f1-f5 algorithms of the UMTS AKA discussed at Ex. 1001, 7:5-24) and send the authentication response RES back to the SI module. *Id.*, 9:16-20. At step **418**, the SI

module then may use the service code and one-way function f to determine a modified authentication response $RES' = f(RES, SC)$, “hence securely inserting information about the communication channel through which the request was received.” *Id.*, 9:20-24.

In step **420**, the modified authentication response RES' then may be transmitted back to the SGSN/VLR in the network for comparison with a modified expected response $XRES'$ (step **422**). *Id.*, 9:26-28. “The expected response $XRES'$ may be determined by the SIU using the one-way function f with the expected response RES determined on the basis of the UMTS AKA and the SC as the input parameters: $XRES' = f(XRES, SC)$.” *Id.*, 9:28-32. The network then may compare the RES' and $XRES'$ to determine if they match, which indicates that the terminal is not corrupted by malware or otherwise compromised. *Id.*, 9:33-44.

While the described embodiment involves modifying an authentication response RES and expected authentication response $XRES$ based on a service code to generate a modified response RES' and expected response $XRES'$, the specification discloses another embodiment where the authentication response RES is instead calculated on the basis of the service code. Specifically, the specification teaches that “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 and subsequently calculate a response RES on the basis of an authentication

and key agreement (AKA) of a telecommunications standard.” *Id.*, 9:60-65. For instance, “in the case of a GSM service the SIM may perform the steps: $RAND' = f(RAND, SC)$ and $RES = A3(RAND', K_C)$.” *Id.*, 9:64-67. Thus, rather than modifying the authentication response RES to generate RES', this embodiment may modify the RAND based on the service code and then use the modified RAND' to calculate the authentication response RES'.

Under either approach, man-in-the-middle attacks are thwarted, because “it is not possible or at least very difficult for malware to detect and/or modify the service channel information.” *Id.*, 2:33-38.

V. INSTITUTION SHOULD BE DENIED

A. Grounds 1-2 Fail Because TS-33.402 Does Not Qualify as Prior Art

The inventors conceived of the claimed invention no later than October 8, 2008—before the October 14, 2008 publication date of TS-33.402—as evidenced by an earlier draft of the foreign priority application for the '235 Patent, European Patent Application No. 08021705 (Ex. 2016, “the EP Application”). *Infra* Section V.A.1. The invention was constructively reduced to practice when the EP Application was filed on December 15, 2008. *Infra* Section V.A.2. And the inventors and their prosecution counsel exercised reasonably continuous diligence from October 8 to December 15. *Infra* Section V.A.3.

Given that TS-33.402 is not prior art, but is exclusively relied on for at least

one limitation of the independent claims in Grounds 1 and 2, Petitioner cannot prevail on those grounds.

1. The Invention Was Conceived Before TS-33.402

The invention was conceived no later than October 8, 2008, as evidenced by a draft of the EP Application filed on Dec. 15, 2008. *See* Ex. 1001, cover page.

The draft EP Application was attached to an October 8, 2008 email from prosecution counsel Erik Visscher to inventor Frank Muller, among others. Ex. 2013.¹ Draft text of the specification was attached as “Service based authentication (8-10-2008).doc” (Ex. 2014) and draft figures were attached as “service based auth (8-10-2008).ppt” (Ex. 2015). *Id.* The file name text “8-10-2008” is in the European time format day-month-year, which is the date of the email. Reference to the “draft EP Application” herein refers to the combination of the draft text and figures. Both Messrs. Visscher and Muller offer sworn testimony authenticating the email and draft EP Application. Ex. 2010 ¶¶3-4; Ex. 2011 ¶¶5-6.²

As shown in the table below, the draft EP Application constitutes clear

¹ All citations are to the translated version of the native language email, which is the immediately preceding exhibit number.

² The production of correspondence/documents exchanged with prosecution counsel is not, and should not be, interpreted as a waiver of any privilege as to any other correspondence/documents. To the extent any tribunal determines otherwise, such waiver should have the most limited scope possible.

evidence of conception of all challenged claims no later than October 8. KPN relies on the same claim limitation nomenclature (*e.g.*, 1[a], 1[b]) as set forth in the “LIST OF CHALLENGED CLAIMS” at the beginning of the Petition. Dr. Sharony’s declaration includes the table below but with the full text of each limitation reproduced for the convenience of the Board. Ex. 2001, 22-33.

Claim Element	Conception Evidence
1[pre]	“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]	“sending a service request for access to a network service;” <i>Id.</i> , 2:20-21.
1[b]	“receiving in response to the service request an authentication request from the network;” <i>Id.</i> , 2:21-23.
1[c]	“identifying the communication channel through which the authentication request was received;” <i>Id.</i> , 2:23-24.
1[d]	“determining a service code associated with the identified communication channel;” <i>Id.</i> , 2:34-36.
1[e]	“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	“the terminal comprises an 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. ... 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....”). A POSITA would thus understand that the “radio module” in the passage above thus qualifies or includes a “service interface (SI) module” as claimed. Ex. 2001, 23-24.
3[pre]	“the authentication request comprises authentication information, preferably a random challenge RAND” Ex. 2014, 3:28-30.
3[a]	“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]	“the authentication request comprises authentication information, preferably a random challenge RAND....” <i>Id.</i> , 3:36-38.
4[a]	“generating ... an authentication response RES;” <i>Id.</i> , 4:1-4.
4[b]	“modifying the authentication parameter RES on the basis the identified communications channel.” <i>Id.</i> , 4:4-6.
5[pre]/[a]	“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]	“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)....” <i>Id.</i> , 13:11-23; <i>see also id.</i> 5:29-35, 18:30-32.
5[c]	“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]/[a]	“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 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	“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]	See Claim 2 above (identifying “radio module” as service interface module).
8[a]	“The radio module 118 ... includes an RF interface comprising an RF receiver The RF interface [“communications 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. While the EP Application does not use the term “authentication signal,” a POSITA would understand the “authentication requests” from the network are “authentication signals.” Ex.

	2001, 27-28.
8[b]	“the terminal comprises an identity module, preferably a removable identity module, and a radio module [“channel identifier”] 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>, 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]	“Preferably, the radio module comprises one or more trusted module [“channel interface”] 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.” Ex. 2001, 28-29.
8[d]	“means for modifying [“modifier”] 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>, 12:5-10, 12:21-23.
9	[i] “In another embodiment, the terminal comprises an identity module ... and a radio module [“service interface 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....” <i>Id.</i>, 3:8-27. [ii] “The identity module may comprise a processor [“modifier”],

	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 [“calculator”] a response comprising one or more authentication parameters upon the reception of a random challenge.” Ex. 2014, 9:20-27. [iii] “the (U)SIM [“identity module”] may modify the calculated response RES on the basis of the service code” <i>Id.</i>, 12:9-10; <i>see also id.</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]). Ex. 1002 ¶48.
10[pre]	(i) “Operating System (OS) 126 of the terminal comprises ... memory for storing program instructions” Ex. 2014, 8:33-37. (ii) <i>See</i> Claim 2 (radio module is a “service interface module”)
10[a]	<i>See</i> Claim 1[b]
10[b]	<i>See</i> Claim 1[c]
10[c]	<i>See</i> Claim 1[d]
10[d]	“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]	“Network node for service based authentication to a network, the network node comprising:” <i>Id.</i>, 20:10-11.
11[a]	“the network node comprising ...means for receiving [“receiver”] 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. Ex. 2001, 31-32.

11[b]	“ 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 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]	[i] <i>See</i> 1[b] [ii] <i>See</i> 1[c]-[d] [iii] <i>See</i> 10[d].
12[b]	[i] <i>See</i> 11[a]-[b] [ii] <i>See</i> 11[c] [iii] <i>See</i> 6[a]
13	“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.

2. The Invention Was Constructively Reduced to Practice on December 15, 2008.

The claimed invention was constructively reduced to practice on December

15, 2008, the date the EP Application was filed. Ex. 1001, 1; *see Frazer v. Schlegel*, 498 F.3d 1283, 1288 (Fed. Cir. 2007) (“The filing of a patent application is a constructive reduction to practice of the invention disclosed therein.”).

3. The Inventor and Prosecution Counsel Exercised Reasonably Continuous Diligence.

Having established prior conception and constructive reduction to practice, KPN must demonstrate that the reasonably continuous diligence was exercised from October 13, 2008 (*i.e.*, the day before the alleged publication date of TS-33.402) to the EP Application’s filing date of December 15, 2008 (hereafter, “Critical Period”). KPN makes this showing below.

a) The Diligence Standard

As the Federal Circuit has explained, the diligence standard does not require demonstrating that the inventors “*continuously* exercised reasonable diligence throughout the critical period,” but instead merely requires a showing that there was “*reasonably continuous* diligence.” *Perfect Surgical Techniques, Inc. v. Olympus Am., Inc.*, 841 F.3d 1004, 1009 (Fed. Cir. 2016) (emphases in original). “Under this standard, an inventor is not required to work on reducing his invention to practice every day during the critical period.... And periods of inactivity within the critical period do not automatically vanquish a patent owner’s claim of reasonable diligence.” *Id.* Indeed, “the purpose of the diligence requirement is to show that the

invention was not abandoned or set aside.” *ATI Techs. ULC v. Iancu*, 920 F.3d 1362, 1373 (Fed. Cir. 2019) (reversing Board finding of lack of diligence).

Since *ATI Technologies*, the Board has found reasonably continuous diligence even in the absence of corroborating documentary evidence of activity for multiple days within a critical period. See e.g., *Google LLC v. Valtrus Innovations Ltd.*, IPR2022-01545, Paper 84 at 20-22 (Aug. 13, 2024) (rejecting arguments that a three-week period of unexplained activity demonstrates a lack of diligence because they “amount to an attempt ‘to scour the patent owner’s corroborating evidence in search of intervals of time where the patent owner has failed to substantiate some sort of activity’” and determining that “in light of the evidence as a whole, ‘the invention was not abandoned or unreasonably delayed.’”); *Unified Patents, LLC v. Flexiworld Techs, Inc.*, IPR2022-00775, Paper 41 at 17-19 (PTAB Nov. 1, 2023) (finding reasonably continuous diligence for the critical period despite alleged 14-day, 20-day, and 21-day periods of no evidence of activity, and noting that “the point of the diligence analysis ... is to assure that, in light of the evidence as a whole, ‘the invention was not abandoned or unreasonably delayed’”).

b) The Standard is Met

KPN demonstrates reasonably continuous diligence via the testimony of inventor Frank Muller and foreign patent prosecution attorney Erik Visscher, together with corroborating documentary evidence.

Mr. Muller is a Dutch citizen residing in the Delft, Netherlands. Ex. 2010 ¶1. He holds a Master's of Science Degree in Electrical Engineering. *Id.* During the Critical Period, Mr. Muller was (and still is) a Senior Scientist at Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek TNO ("TNO"), which is a leading telecommunications technology consulting company. *Id.* ¶¶1-2. Mr. Muller is a prolific inventor of wireless communications technologies, having been a named inventor in numerous U.S. and foreign patents, several of which have been successfully litigated. *See e.g., Koninklijke KPN NV v. Telefonaktiebolaget LM Ericsson*, 2:21-cv-00113 (E.D. Tex. 2021) (obtaining \$35M+ verdict for infringement of '235 Patent). During the Critical Period, Mr. Muller performed assignments for KPN and one other TNO client. Ex. 2010 ¶2.

Erik Visscher is also a Dutch citizen and has been an attorney at De Vries & Metman since 2007. Ex. 2011 ¶1. During the Critical Period, Mr. Visscher performed prosecution work for KPN and many other clients. *Id.* ¶¶2-3 (citing Ex. 2041). He was responsible for drafting and filing the EP Application, including coordinating with Mr. Muller. *Id.* ¶4.

The Critical Period begins on October 13, 2008. The draft EP Application had been sent by Mr. Visscher to Mr. Muller for review on October 8. Ex. 2013. However, Mr. Muller was on vacation from October 1 to October 19 "road-tripping" across the United States. Ex. 2010 ¶¶5-6 (citing Ex. 2050; Ex. 2018, 2); Ex. 2011

¶7. As the Federal Circuit has explained, inactivity due to an inventor’s vacation does not preclude a finding of diligence, as it is reasonable for an inventor to take vacations. *Griffith v. Kanamaru*, 816 F.2d 624, 626 (Fed. Cir. 1987) (“it is not unreasonable for inventor to delay completing a patent application until after returning from a three week vacation in Sweden”) (citing *Reed v. Tornqvist*, 436 F.2d 501, 504-05 (C.C.P.A. 1971)); *see also Perfect Surgical*, 841 F.3d 1004 at 1017 (Schall, J., dissenting) (approvingly discussing *Reed*); *Unified Patents*, IPR2022-00775, Paper 41 at 19 (considering that critical period was “holiday-filled” when analyzing diligence).

Mr. Muller returned to work on October 20 and resumed his ordinary work duties, which included efforts to catch-up on issues and updates that accrued while he was on his multiweek vacation. Ex. 2010 ¶7. This included preparing for an October 22 to October 25 business trip to Chicago on behalf of KPN for a matter unrelated to the EP Application. *Id.* (citing Ex. 2046-2049). The business trip was part of Mr. Muller’s ordinary job duties and obligations. *Id.*; *Mycogen Plant Sci., Inc. v. Monsanto Co.*, 252 F.3d 1306, 1316 (Fed. Cir. 2001) (“Proof of reasonable diligence ... does not require a party to work constantly on the invention or to drop all other work.”).

On October 28 (Tuesday), Mr. Muller was working on a quotation for another TNO client and had a progress meeting with his manager. Ex. 2010 ¶8. He began

reviewing the draft EP Application by at least October 29, 2008, which was the first availability he had to review the draft given his other work obligations and duties. *Id.* (citing Ex. 2018, 2). He reviewed the EP Application during the period of October 29 to November 5, and the draft “really got [him] thinking” and so he “need[ed] some more time for [his] response” and edits to the draft. *Id.*; Ex. 2018, 2.

On November 6, Mr. Muller provided feedback to Mr. Visscher in an email regarding the draft EP Application, and explained that he would “explain [his] train of thought in more detail” in a follow-up email. Ex. 2018, 1. Mr. Muller continued to review the draft EP Application over the coming days and provided his detailed thoughts to Mr. Visscher in a November 10 email, which also included a redlined version of the draft EP Application containing his edits and comments. Ex. 2010 ¶¶9-10 (citing Ex. 2020, 3-4).

Messrs. Muller and Visscher continued to exchange emails relating to the substance of the draft EP Application on November 12, 13, 17 and 18, including a teleconference on November 17. *Id.* ¶11 (citing Ex. 2020, 1-3). Over that period, Mr. Visscher “incorporated a large part of the changes” that were discussed, but he still needed to “go through the entire text and figures again to make the story consistent.” *Id.* (citing Ex. 2020, 1); Ex. 2011 ¶8. Consequently, Mr. Visscher effectively took lead on the draft to make additional revisions pursuant to the discussions with Mr. Muller. Ex. 2010 ¶11; Ex. 2011 ¶8.

From November 12 to November 25, Mr. Visscher exercised reasonably continuous diligence in further preparing the draft EP Application for filing, culminating with a revised draft sent to Mr. Muller on November 25. Ex. 2011 ¶8 (citing Ex. 2026, 1). As Mr. Visscher explained, the changes made to the application were so “substantial” that he asked Mr. Muller to “take another look at this amended version before the application is filed.” Ex. 2026, 1. Moreover, during the entire Critical Period (including from November 18 to November 25), Mr. Visscher was diligent in attending to prosecution matters for KPN and many other clients. Ex. 2011 ¶8 (citing Ex. 2041).

Mr. Muller then reviewed draft EP Application over the period of November 25 to December 8, which included a foreign business trip with KPN in Taipei from November 30 to December 5 on a matter unrelated to the draft EP Application. Ex. 2010 ¶12 (citing Ex. 2024, 1; Ex. 2030, 1; Ex. 2032, 1; Ex. 2036, 1). On December 9 (one business-day after returning from Taipei), Mr. Muller provided additional thoughts to Mr. Visscher regarding the draft EP Application, as well as a revised draft with his comments. Ex. 2010 ¶13 (citing Ex. 2034, 1). Mr. Muller also proposed additional edits to the figures to Mr. Visscher. *Id.*

The following day (December 10), Mr. Visscher provided a revise draft of the EP Application. Ex. 2010 ¶13; Ex. 2011 ¶9 (citing Ex. 2038, 1; Ex. 2040, 1; Ex. 2044; Ex. 2045). The EP Application was filed on December 15—a mere five days

later. *See Google*, IPR2022-01545, Paper 84 at 20-22 (finding reasonably continuous diligence where draft patent application was finalized August 8, 2001 and the application was filed on August 27, 2001, even though the three-week gap was unexplained).

In view of the above, Messrs. Muller and Visscher were reasonably diligent in attempting to constructively reduce the invention to practice. Ex. 2010 ¶14; Ex. 2011 ¶10. Indeed, “the record shows that in light of the evidence ***as a whole***, the invention was not ***abandoned or unreasonably delayed***.” *Perfect Surgical*, 841 F.3d at 1009.³

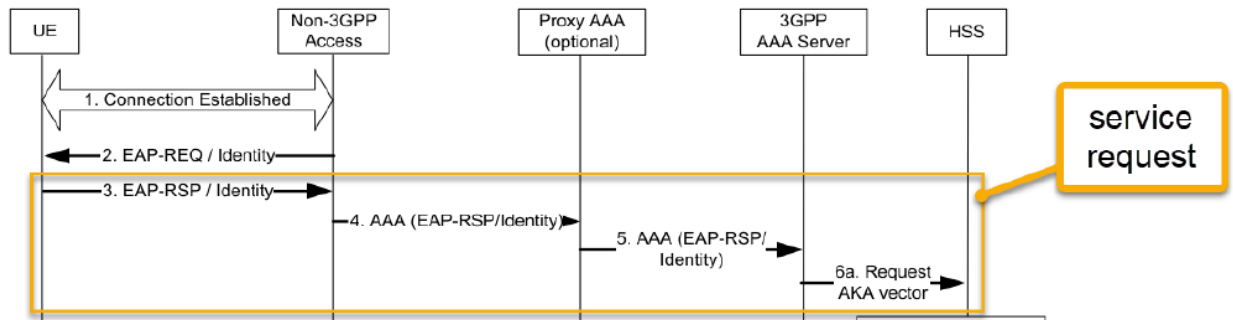
B. Ground 1 Fails on the Merits

Ground 1 challenges Claims 1, 3-7 and 11-13 as obvious based on TS-33.402 alone, or in view of Arkko. Pet., 4-5. But even if TS-33.402 qualified as prior art (it does not), Petitioner fails to demonstrate that the combination teaches all elements of any independent claim.

³ Patent Owner has an abundance of additional evidence (e.g., emails) further evidencing reasonably continuous diligence during the Critical Period, and will produce that evidence should the Board determine that additional evidence is necessary.

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

Petitioner annotates Fig. 6.2-1 of TS-33.402 to arbitrarily identify the “EAP-RESP/Identity” message (orange) from the terminal as the alleged “service request:”



Pet., 20-21. Petitioner provides no explanation as to *why* or *how* that message constitutes a “service request,” but simply states that it does in conclusory fashion.

Regardless, Petitioner is mistaken that EAP Response/Identity message is a “**service** request.” The EAP Response/Identity is a response to a request by the network **for identification** in the first step of the **authentication** process, not a request for **service** by the terminal. Indeed, EAP stands for “**extensible authentication** protocol.” Ex. 1006, 7. The “EAP Request/Identity” is transmitted from the “**authenticator**” in the network to the terminal. *Id.*, 13.

Petitioner’s mapping is contradicted by its arguments based on Naslund. Petitioner acknowledges that Naslund does not explicitly disclose a service request as claimed and instead argues that “in order to initiate the AuC generating the ‘expected response XRES ...’ the AuC would need to know the specific user that it

is authenticating. A POSITA would understand that this could only be done if the user's terminal *first* requests access to the network to *initiate* the authentication protocol." Pet., 55-56. In other words, Petitioner represents that the service request is not *part of* the authentication protocol, but rather may *initiate* the authentication protocol. Thus, based on Petitioner's own logic, the EAP-RSP/Identity cannot constitute a service request as claimed, as EAP-RSP/Identity is part of the extensible authentication protocol and does not *initiate* that authentication protocol.

In view of the above, the EAP-RSP/Identity of TS-33.402 would not be understood to be a "service request." Nor can it be disclosed by TS-33.402, as it teaches that "1. A connection is established between the UE and the trusted non-3GPP access network, using a procedure specific to the non-3GPP access network (*which is out of scope for the present document*)." Ex. 1006, 13. Because TS-33.02 is silent as to the specific activity occurring before the EAP-REQ/Identity is sent, it cannot disclose a service request as claimed. And even if Petitioner *could have* offered an obviousness theory to attempt to address this limitation, Petitioner is precluded from doing so now. *See Netflix, Inc. v. DivX, LLC*, 84 F.4th 1371, 1377 (Fed. Cir. 2023) ("[W]e have rejected, many times, post-hoc attempts on appeal to include additional, new arguments not contained in the petition.").

2. Claim 1[e]

a) TS-33.402 does not teach that "the authentication response

**depends on the identified communication channel” or is
“calculated on the basis of ... the determined service code.”**

Petitioner identifies the “AKA Response/AKA-Challenge message” as the alleged “authentication response” and argues this limitation is satisfied because the new MAC value is part of the message and is calculated based on the “access network identity” (alleged “service code”). Pet., 27-29. Petitioner’s MAC value theory is misplaced and misleading, because it is premised on improperly identifying the entire “EAP-RSP/AKA-Challenge message” as the “authentication response,” rather than correctly identifying “RES” as the “authentication response” as understood by a POSITA. Ex. 2001 ¶¶51-52.

It is helpful to first understand *why* Petitioner misidentifies the entire “EAP-RSP/AKA-Challenge message” as the authentication response, rather than identifying the actual authentication response—namely “RES.” It is because the RES is in ***no way*** based on or determined by the “access network identity” (alleged “service code”). *Id.* ¶53 (explaining that the authentication response is calculated by $RES = f_{2K}(RAND)$) (citing Ex. 2003, 11, 24).

Moreover, the new MAC and authentication response RES are contained ***as separate values*** within the “EAP Response/AKA-Challenge message.” *Id.* ¶54. Specifically, TS-33.402 teaches that “[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 added). A POSITA would thus understand that “RES” is the authentication response and is contained **within** the EAP-Response/AKA-Challenge message **separately** from the MAC value. Ex. 2001 ¶54.

The fact that the authentication response and new MAC are distinct elements contained within the EAP message is important, because Petitioner alleges 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). In other words, Petitioner is mapping the claimed “authentication response” to the entire EAP message rather than to the authentication response RES **contained within** the EAP-RSP/AKA-Challenge message. Petitioner then attempts to use this incorrect mapping to argue that the authentication response (alleged EAP-RSP/AKA-Challenge message) “depends on” and is “calculated on the basis of ... the determined service code” because the new MAC value relies on the network access identity (alleged “service code”) and “covers” the EAP-RSP/AKA-Challenge message.

Petitioner’s MAC value theory is fundamentally flawed because a POSITA would have understood **RES** to be the authentication response—not the entire EAP-

RSP/AKA-Challenge message. Ex. 2001 ¶55. The dispositive issue here is what a POSITA would consider to be the “authentication response” in the AKA-Challenge process of TS-33.402. Is it the entire EAP-RSP/AKA-Challenge message (as alleged by Petitioner) or the element *specifically defined and referred to as* the “authentication response” in the 3GPP specification (as alleged by KPN)?

The independent evidence overwhelming demonstrates that a POSITA would have understood “RES” to be the authentication response in the AKA-Challenge process of TS-33.402. For example, TS-133.102 provides a conceptual illustration of the AKA process:

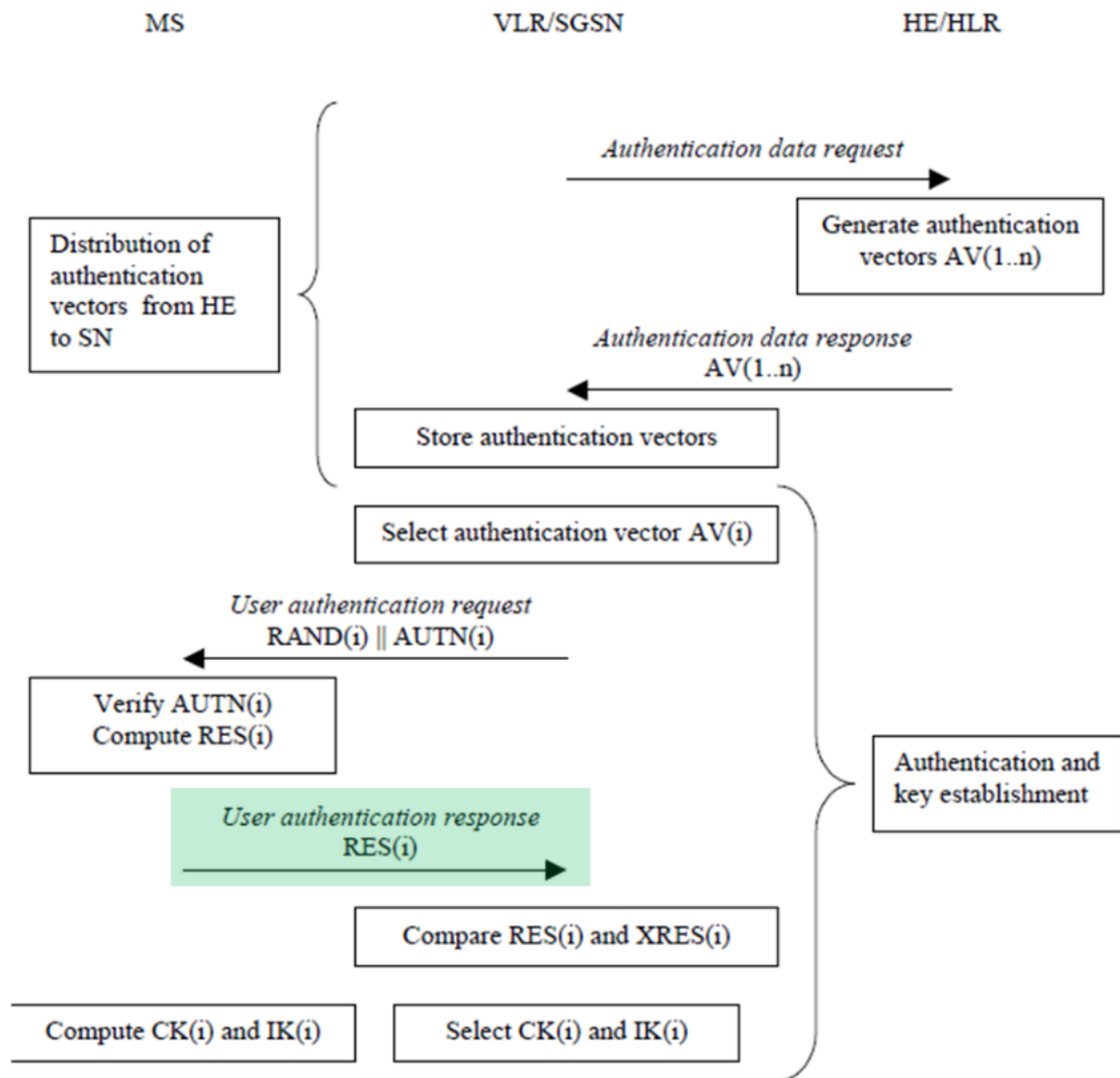


Figure 5: Authentication and key agreement

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.*, 28 (“The **authentication response (RES)** shall have a variable length....”). Indeed, it is abbreviated “RES” because it is the authentication **RESPONSE**. Ex. 2001 ¶55. This is consistent with Figure 8 of TS-133.102:

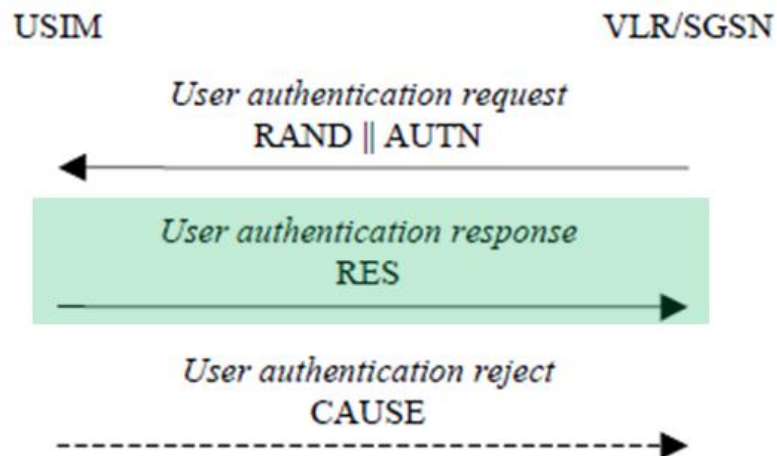


Figure 8: Authentication and key establishment

Id. ¶56 (citing Ex. 2003, 22). Notably, the new MAC value is not illustrated as being associated with the “User **authentication response**.” *Id.*

Other objective references likewise show that a POSITA would have understood RES to be the authentication response in TS-33.402. *Id.* ¶57 (citing *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:

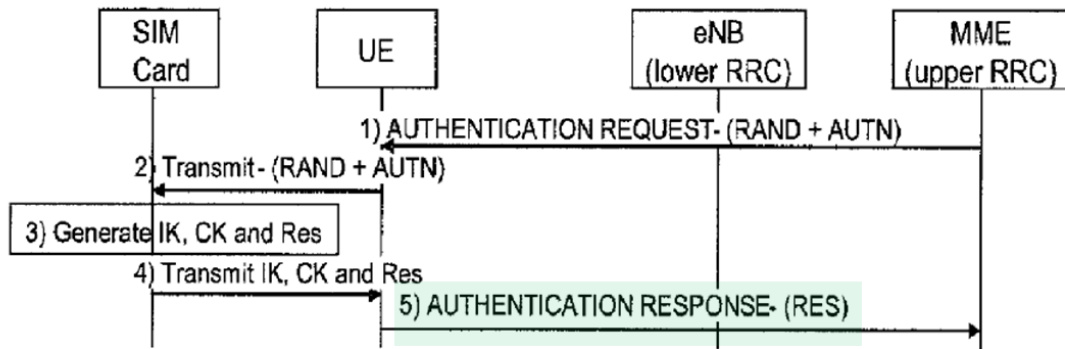
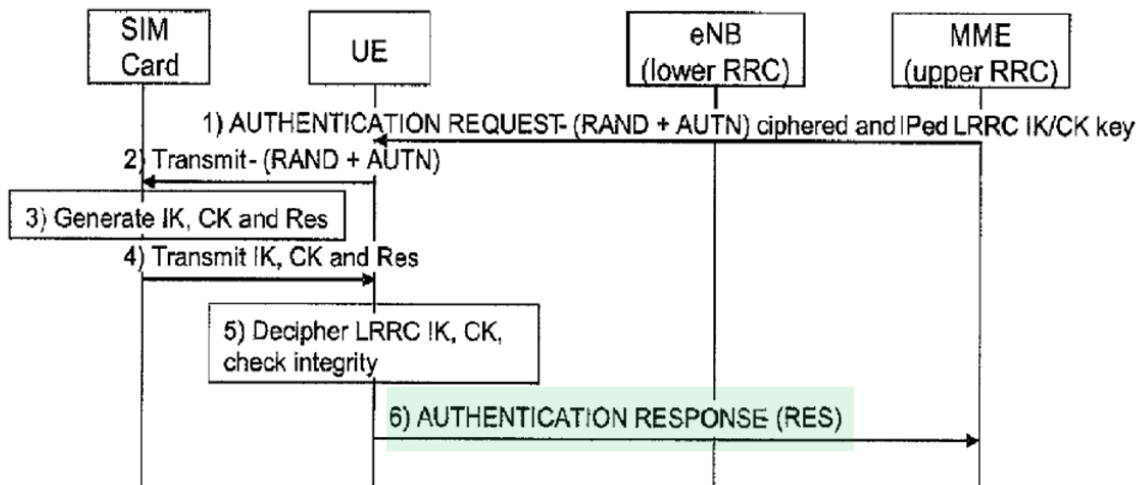


Fig. 12



Ex. 2006, 9:45-49 (“the UE responsively generates an authentication response RES”); Ex. 2001 ¶57.

Perhaps most importantly, the evidence above is wholly consistent with repeated and exclusive teachings from the specification of the ’235 Patent that “RES” is understood to be the authentication response in the AKA-Challenge process. See Ex. 2001 ¶58 (citing *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**....”). In fact, Petitioner implicitly acknowledges that “RES” is the known-abbreviation for the “authentication response” when Petitioner expressly identifies the authentication response of Naslund as “authentication response **RES**’.” See Pet., 62-63.

As shown by the evidence 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.” Ex. 2001 ¶59. Petitioner improperly maps the entire EAP message to the “authentication response” by ignoring the fact that RES is *explicitly* defined, and referred to as, the “authentication response” in the UMTS standard itself (TS-133.102), consistent with the numerous objective references discussed above. Petitioner’s MAC value theory also disregards that the ’235 Patent exclusively refers to the authentication response as RES (consistent with the evidence above) and teaches that the authentication response RES is calculated or modified based on the service code. See *e.g.*, Ex. 1001, 9:60-10:5, 2:51-3:4.

The ordinary meaning of a claim term is not “the meaning of the term in the abstract,” but “the meaning to the ordinary artisan after reading the entire patent.” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1321 (Fed. Cir. 2005) (en banc). Moreover, the ordinary artisan is presumed to have a certain level of background knowledge, which Petitioner admits includes at least two years of experience working with cellular telecommunications, radio-access network architectures, or cellular network security management. Pet., 6. The evidence above demonstrates that the background knowledge would have included the understanding that the authentication response in an AKA-Challenge is RES. *See Ericsson, Inc. v. Koninklijke KPN N.V.*, IPR2023-00524, Paper 13 at 10-11, 29 (PTAB Aug. 21, 2023) (determining that “signalling” should be construed consistent with its usage in the specification and 3GPP standards documentation referenced in the patent, and rejecting effort to broadly read it to refer to exchanging any signal). This is consistent with the teachings of the specification. *See e.g.*, Ex. 1001 at 7:1-3, 7:30-33, 8:20, 9:16-20, 9:67-10:3, 10:39-43. Because the authentication response of TS-33.402 ***as understood by one of ordinary skill in the art*** is RES and RES is not calculated or based in any way on the “access network identity,” Petitioner’s MAC value theory fails.

b) TS-33.402 has not been shown to teach that “the [authentication] response is calculated on the basis of the information in the authentication request.”

Petitioner argues 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.

The authentication response RES is not “calculated” by the UE based on AUTN and the received MAC. Ex. 2001 ¶¶60-61. Petitioner argues 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 merely teaches that whether AUTN and the received MAC are correct dictates *whether calculations are performed* to compute RES, IK and CK—those calculations are not *based on* AUTN or the received MAC. Ex. 2001 ¶61 (citing Ex. 1006, 15 (“If AUTN is incorrect, the terminal rejects the authentication If AUTN is correct, the USIM application computes RES, IK and CK..... The UE then ... checks the received MAC with the new derived keying material.”)). Because AUTN and the received MAC (i.e., alleged “information in the authentication request”) are not used to calculate the authentication response RES, Petitioner’s invalidity theory fails. *Id.*

This is true **even under Petitioner’s identification of the entire EAP-Response/AKA-Challenge message**, 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.*

3. 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.”

Petitioner alleges that:

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**.

Pet., 29-30. Petitioner is mistaken for several reasons.

First, Petitioner is incorrect that that the authentication request is “modified” to check the received MAC (see underlined portion above). Ex. 2001 ¶¶62-63. The received MAC is only used as an input to a (keyed hash) calculation, to **verify** that the MAC is correct. *Id.* (citing Ex. 1016, 63). Indeed, Petitioner admits that 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. *Id.*

This is fundamentally different than modifying the authentication information as claimed. *Id.* For example, 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 $RES' = A3(RAND', KC)$.

Ex. 1001, 9:60-67. Thus, the RAND of the authentication request is modified by the terminal to generate RAND', which is a function of both RAND and SC. Under any plausible interpretation of “modifying,” the act of using an input to verify a hash value does not qualify. Ex. 2001 ¶64.

Second, Petitioner applies an unreasonable interpretation of “generating the authentication response on the basis of the modified authentication information.” As Petitioner admits, 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. *Id.* ¶65 (citing Ex. 1006, 15). If the MAC value is incorrect, the message is not calculated. *Id.* If the MAC value is correct, the message is calculated, but the MAC value forms ***no basis*** of the calculation. *Id.* The value of the message is thus ***entirely independent*** of the

incoming MAC value. *Id.* As such, 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”). *Id.*

Further, Petitioner’s invalidity theory is contradicted by the ’235 Patent’s specification. The specification repeatedly and exclusively uses the phrase “on the basis of” to refer to generating a value based on a particular input parameter. Ex. 2001 ¶66 (citing *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: $RAND' = f(RAND, SC)$...”), 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: $RES' = A3(RAND, KC)$ 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”)). Indeed, the phrase “on the basis of” is used in the specification 21 times—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). *See Phillips*, 415 F.3d at 1315 (“The specification ... is the single best guide to the meaning of a disputed term.”).

Petitioner’s interpretation is also inconsistent with the invention described in the specification. Ex. 2001 ¶67. 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.” *Id.* (citing 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. *Id.*

For instance, the specification teaches that the SIM of a terminal may perform

the step of $RAND' = f(RAND, \underline{SC})$, 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.* Thus, RES' is 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 $RAND' = f(RAND, \underline{XSC})$, which is then used as an input parameter to generate XRES' for comparison to RES'. *Id.*, 10:6-16. 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. Ex. 2001 ¶68.

With this understanding, Petitioner's interpretation of “the terminal generating the authentication response on the basis of the modified authentication information” is even more untenable. Under Petitioner's application of that phrase, “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. *Id.* ¶69. Indeed, the network would not be able to authenticate the terminal if the terminal does not use RAND' to generate its authentication response. *Id.* For the reasons above, a POSITA would not understand TS-33.402 to teach this limitation, which is fundamentally different than the disclosed MAC check process. *Id.*

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

Petitioner alleges that TS-33.402 teaches this limitation because it 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). Petitioner is mistaken for at least two reasons.

First, Petitioner’s invalidity theory is premised on incorrectly mapping “the authentication response” to the EAP-Response/AKA-Challenge message. Ex. 2001 ¶¶70-71. But as explained with respect to limitation 1[e], that message is not the “authentication response.” *Supra* Section V.B.2.a. Rather, the message *includes* the authentication response—which is expressly defined and understood to be **RES** as evidenced by numerous objective references. *Id.* TS-33.402 does not teach modifying **RES** on the basis of the identified communications channel, which is why

Petitioner resorts to improperly mapping to the EAP-Response/AKA-Challenge message. Indeed, TS-33.402 explicitly 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. Ex. 2001 ¶71 (citing 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.”))).

Second, even if the EAP-Response/AKA-Challenge message would have been understood to be the “authentication response” (it would not), this limitation would still not be met by TS-33.402. As Petitioner admits, 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). “Covering” refers to the fact that the MAC value is similar to **a signature on** the EAP message to *prevent* modification of the message. Ex. 2001 ¶72 (citing 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.**”))).

There is a fundamental difference between **signing** the EAP message with the MAC and **modifying** the message. *Id.* ¶73. When the MAC is applied, it is simply **appended to** the EAP message as a signature—the content of the EAP message itself

remains the same. *Id.* (citing 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**”). Indeed, the content of the EAP message before and after covering with the MAC is exactly the same—the “covering” process does nothing to change the content but simply adds a signature. *Id.* “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 that is being authenticated. *Id.* The MAC is similar to a digital signature used for email signature authentication, which verifies the authenticity of an email but does not modify or affect its underlying content. *Id.*

“Covering” with a MAC is fundamentally different than what is claimed and described in the ’235 Patent. *Id.* ¶74. The specification repeatedly and exclusively 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 expansive interpretation of “modifying,” simply transmitting a message over a network necessarily means it is “modified” because all messages undergo some form of encapsulation (e.g., broken into packets to be transmitted via the IP protocol) when transmitted across a network. *See Ericsson*, IPR2023-00524, Paper 13 at 33 (denying institution and determining that petitioner’s attempt to characterize SMS messaging as a “signalling” message

simply because it contains a message header would “would equally apply *to practically any message* with a header, and thus is overly broad”). A POSITA would not understanding “modifying” to have such an expansive meaning. Ex. 2001 ¶74.

5. Claim 5[a]

Petitioner fails to carry its burden on the “service request” limitation for the same reasons discussed with respect to Claim 1[a]. *Supra* Section V.B.1.

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

Petitioner takes conflicting positions on what it considers to be “the expected response,” presumably because it has to identify one element as the “expected response” to try and invalidate Claim 5, while inconsistently identify another element as the “expected response” to try invalidate Claim 6 (dependent on claim 5). Specifically, Petitioner first alleges 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 service request was sent to the network.” Pet., 32-33. Petitioner thus initially alleges that XRES is the “expected response.” *See also id.*, 34-35 (relying on XRES as “the expected response” for Claim 6). However, Petitioner then alters its theory, alleging that the “new authentication vector” is “the expected response.” *Id.*, 32-33 (“Thus, the authentication vector is an *expected response*, and it is determined on the basis

of the *expected service code*.”).

It appears that Petitioner relies on the “new authentication vector” as the “expected response” for purposes of Claim 5 because it is calculated using the alleged service code (i.e., access network identity). But Petitioner then relies on XRES as the “expected response” for Claim 6 because only the XRES is actually “compared” to the authentication response RES. This inconsistency is reason enough to deny institution. *See Huizhou TCL Mobile Commc’n Co. Ltd. v. Wi-LAN Inc.*, IPR2020-00302, Paper 8 at 10 (PTAB Aug. 3, 2020) (denying institution where petitioner “fails to reconcile these two conflicting positions, and, therefore, ... has not sufficiently explained how the ranging request message of Figure 7 is transmitted ‘over a random access channel,’ as recited in claims 1 and 6”).

In any event, TS-33.402 does not teach this limitation. The “new authentication vector” is not an “expected response—“XRES” is the expected response. Ex. 2001 ¶¶75-76. Indeed, Petitioner earlier admits 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 admits, it is XRES and RES that are compared—the authentication vector is never compared to anything by the server. *Id.*, 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 response RES to authenticate the terminal. Ex. 2001 ¶76.

This understanding is consistent with repeated and exclusive teachings from the specification of the ’235 Patent using “XRES” to refer to the expected authentication response. Ex. 2001 ¶77 (citing *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**”)).

That a POSITA would understand XRES to be the expected response in the AKA-Challenge of TS-33.402 is further evidenced by numerous independent references describing the AKA-Challenge process. Ex. 2001 ¶78. 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.*, 22. TS-133.102 also provides a schematic diagram showing how the expected response XRES is compared to the authentication response RES:

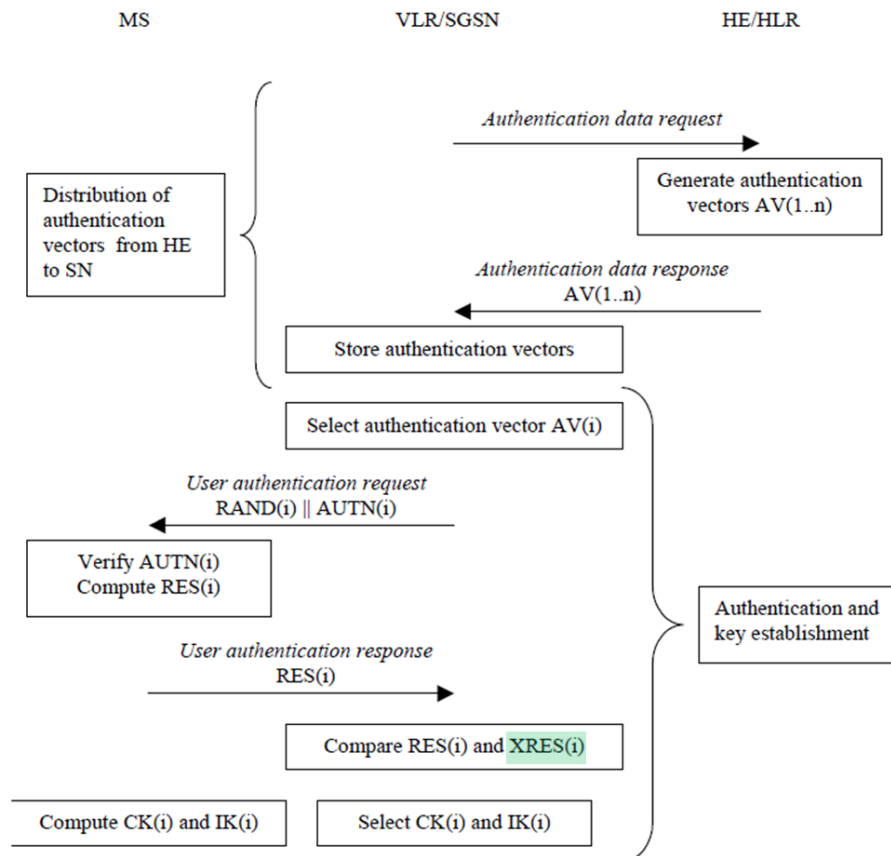


Figure 5: Authentication and key agreement

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.”)

Other independent references likewise show that a POSITA would have

understood XRES to be the expected response in TS-33.402. Ex. 2001 ¶79 (citing *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....”)). In fact, 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]. In other words, outside of these proceedings Samsung acknowledges that XRES is understood by those of skill in the art to be the “expected response” in an AKA-Challenge, which is consistent with TS-33.402. Ex. 2001 ¶79.

In view of the evidence 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. *Id.* ¶80. This is an important fact because XRES

is *not* determined based on the access network identity (alleged “service code”). *Id.* Nor can Petitioner allege as much, as XRES (green) is determined exclusively based on the message authentication function f2 and RAND (orange), specifically $XRES = f2(RAND, K)$:

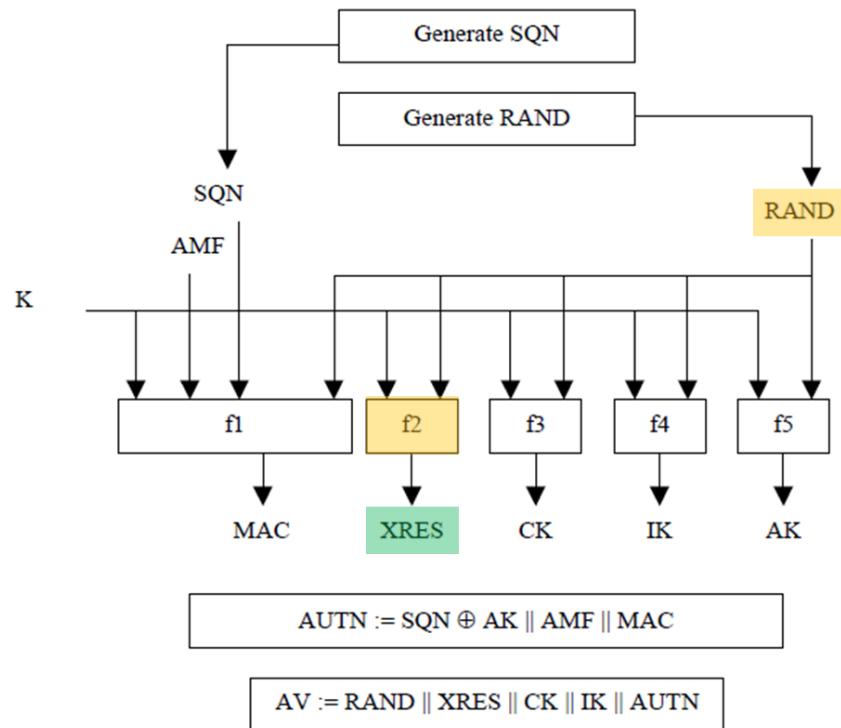


Figure 7: Generation of authentication vectors

Id. (citing Ex. 2003, 21-22). This is why Petitioner disingenuously identifies the authentication vector as the “expected response,” rather than the actual expected response XRES as understood by a POSITA. More specifically, Petitioner misidentifies the new authentication vector as the “expected response” so that it can rely on the fact that the vector is calculated based on a key derivation process involving CK’ and IK’ that are generated using the “access network identity.”

However, the authentication vector is **not** the expected response—the expected response is **XRES**, and **XRES** is *not* calculated based on the access network identity.

Id. Because the expected response XRES of TS-33.402 is in no way calculated based on or determined by the access network identity, TS-33.402 does not teach this limitation. *Id.*

7. Claim 6[a]-[b]

Claim 6[a] requires “**comparing** the expected response with the authentication response sent by the terminal to the network” and 6[b] requires “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 identifies the “new authentication vector” as the alleged “expected response,” but then alters its theory to allege that XRES is the “expected response” for Claim 6. Pet., 34-35.

Petitioner cannot have it both ways, and this inconsistency is reason enough to deny institution. *See Huizhou TCL Mobile Commc’n* IPR2020-00302, Paper 8 at 10. Regardless, Petitioner’s inconsistent theory also fails on the merits. If the “new authentication vector” is “the expected response” as alleged in Claim 5, it must necessarily be “the expected response” for Claim 6. However, TS-33.402 does not teach that new authentication vector is **compared**. Ex. 2001 ¶82.

This is precisely why Petitioner changes and/or conflates its theory midstream

to identify XRES as “the expected response.” Specifically, Petitioner relies on TS-33.402 teaching that the “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). 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” and thus cannot satisfy Claim 5[c]. Ex. 2001 ¶83 (citing Ex. 2003, 22 (“expected response $XRES = f_{2K}(\mathbf{RAND})$ where f_2 is a (possibly truncated) message authentication function”)). Consequently, if XRES is the expected authentication response, neither Claim 5 nor 6 can be invalid based on TS-33.402. *Id.* And if the “new authentication vector” would have been understood to be “the expected response” in TS-33.402 (it would not), Claim 6[a] cannot be invalid based on TS-33.402 because the vector is never “compared” as required. *Id.*

8. 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.”

Petitioner argues 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 fails for the reasons discussed with respect to Claim 5[c]. *Supra* Section V.B.6. 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. Ex. 2001 ¶84. Instead, XRES is simply compared to the received authentication response RES “as is.” *Id.* (citing 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. *Id.*

9. 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;”

Petitioner relies on its discussion of limitation 4[b] for this limitation. Pet., 37. However, TS-33.402 does not teach a modified response that is based on a determined service code. *See supra* V.B.4; Ex. 2001 ¶85.

10. 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”

Petitioner relies on its analysis with respect to limitation 11[c]. Pet., 38. TS-33.402 fails to teach this limitation for the same reason discussed with respect to limitation 11[c]. *Supra* Section V.B.8; Ex. 2001 ¶86.

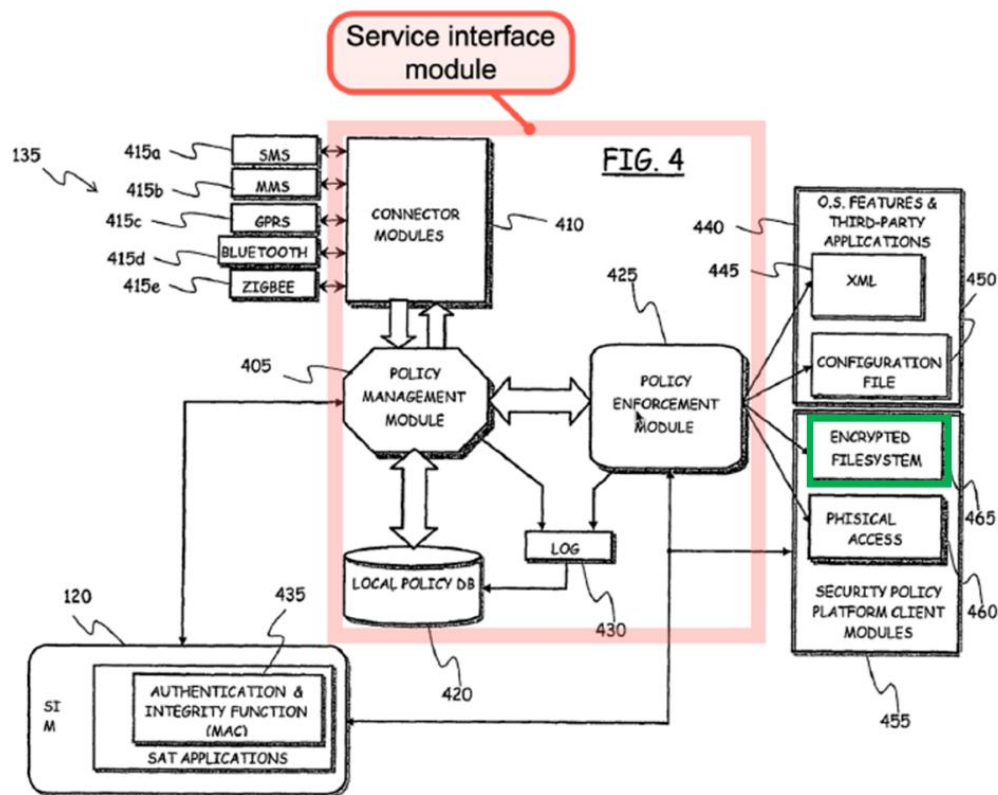
C. Ground 2 Fails on the Merits

Ground 2 challenges Claims 2, 8-10 and 13 as obvious based on TS-33.402 (with or without Arkko) in view of Aldera. Pet., 4-5. Ground 2 fails to demonstrate any claim is unpatentable for the reasons discussed 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.”

Petitioner’s invalidity theory here is flawed for at least three reasons. For one, 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, TS-33.402 does not teach that function for the reasons discussed with respect to limitation 4[b]. *Supra* Section V.B.4. Consequently, the combination of TS-33.402 and Aldera fails for the same reason that TS-33.402 alone fails. Ex. 2001 ¶89.

Second, Petitioner identifies the “encryption function” 465 as the alleged “modifier.” Pet., 49. Pursuant to Petitioner’s own mappings (shown below), the encryption function 465 (green box, added by KPN) is *not* part of the alleged “service interface module” (red box, added by Petitioner).



Pet. 43. However, 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), Petitioner cannot prevail on its invalidity theory. Ex. 2001 ¶90.

Third, Petitioner fails to explain why it would have been obvious to have the “encryption function 465” perform the alleged “modifying.” TS-33.402 teaches that “the UE runs AKA algorithms **on the USIM application** on UICC.” Ex. 1006, 15. 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 this teaching. Ex. 2001 ¶91. Indeed, it appears that the sole reason that Petitioner did not propose the USIM performing the AKA algorithms as taught by TS-33.402 is that this would result in the alleged “modifier” residing in SIM 120 (alleged “identity module”) rather than in the alleged “service interface module” as required by the claim.

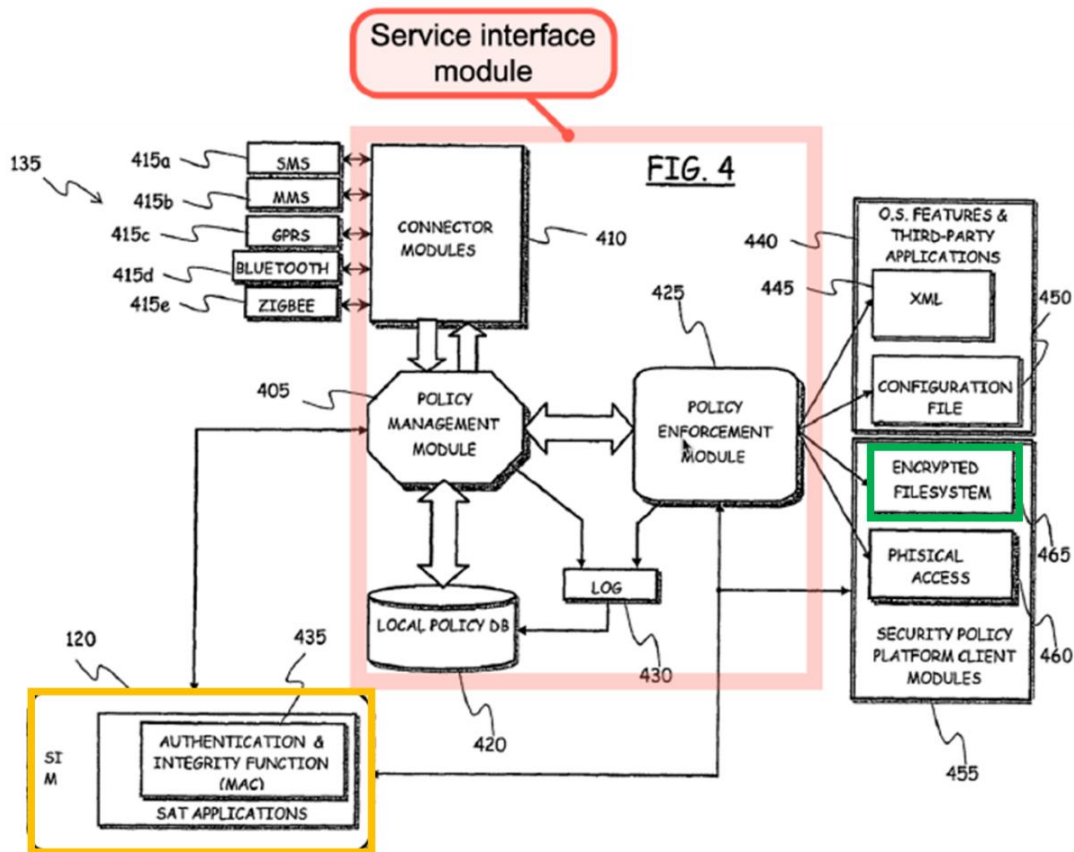
2. Claim 9: “An identity module ... comprising ... a modifier for modifying the response on the basis of a predetermined mathematical function using a service code associated with the identified communication channel.”

There are at least two problems with Petitioner’s theory as to this claim limitation.

First, as with Claim 8[d], Petitioner relies on Aldera for the “modifier” *structure*, but relies exclusively on TS-33.402 for the “modifying” *functionality*. Pet., 50. Consequently, the combination of TS-33.402 and Aldera fails for the same reason that TS-33.402 alone fails with respect to Claim 4[b]. *Supra* Section V.B.4; Ex. 2001 ¶92.

Second, Petitioner’s assertion 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. Ex. 2001 ¶93. For Claim 8, Petitioner alleges that the “encryption function” 465 is the “modifier” associated with the “service interface module” (red

box added by Petitioner). Pet., 43.⁴



Yet, for Claim 9 Petitioner alleges that the “modifier” resides in the alleged “**identity module**” (i.e., SIM 120, orange box added by KPN). Pet., 49-50. 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. Because Petitioner fails to provide any rationale for incorporating the alleged “modifier” in

⁴ As noted with respect to Claim 8[d], the encryption function 465 is not part of the alleged “service interface module” and thus Petitioner fails to carry its burden on that limitation under Petitioner’s own invalidity mappings. *Supra* Section V.C.1.

the SIM 120 (orange) rather than as the encryption function 465 (green), Petitioner cannot carry its burden of proving obviousness. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (obviousness requires “identify[ing] a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does”).

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.”

Petitioner relies on its discussion of limitation 8[d] for this limitation, which itself relies exclusively on the analysis of TS-33.402 relating to limitation 4[b]. Pet., 52. However, TS-33.402 does not teach this limitation for the reasons discussed with respect to limitation 4[b]. *Supra* Section V.B.4; Ex. 2001 ¶94.

D. Ground 3 Fails on the Merits

Ground 3 challenges Claims 1-7 and 13 as obvious based on Naslund. Pet., 4-5. Petitioner acknowledges that the Examiner considered Naslund during original examination and thoroughly applied it to the claims. *Id.*, 8-10. Contrary to Petitioner’s position, the Examiner correctly determined that Naslund fails to render any claims unpatentable for at least the reasons below.

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

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

Contrary to what Petitioner argues, a POSITA would not understand this to teach a service code associated with the identification communication channel. Ex. 2001 ¶¶96-97. 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; Pet., 11. Pursuant to Claim 8[b], the claimed “service code” must identify “the communication channel *through which the authentication signal was received.*” The “Security-enhancing sub application” codes cannot satisfy this requirement under any reasonable interpretation of the claims. Ex. 2001 ¶97.

A POSITA would instead understand that each code (e.g., 01 through 07)

represents a particular “Security-enhancing sub **application**,” which is why the codes are listed in the column “Security-enhancing sub application” (green). *Id.* ¶98. The codes are thus associated with security-enhancing sub applications, not an identified communication channel as claimed. Indeed, 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. *Id.* (citing 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.”))).

That the codes cannot identify the channel upon which the authentication request was received is further confirmed by the fact that the same codes are used in policies having **different** “Interface” parameters. *Id.* ¶99. For example, as shown below (purple annotations added by KPN), in row two code “01” is included in a policy listing “Normal” interface, but in row ten the same code 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

The codes thus cannot be associated with the identified communication channel, as each code can be included in policies involving **different** “Interface” parameters. *Id.* Indeed, this is precisely why Petitioner conspicuously fails to discuss or address row ten—that row demonstrates that the codes are not associated with the identified communication channel. 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. *Id.*

Similarly problematic for Petitioner is the fact that **different** codes may be part of different security policies that include the **same** “Interface” parameter. *Id.* ¶100. For example, as shown above, the policies of rows 2, 6, 7 and 8 include the **same** interface “Normal” as the “Interface” parameter but have **different** “Security-

enhancing sub application” codes. Thus, the codes may be 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). *Id.*

The fallacy of Petitioner’s theory here is even more apparent when viewed in the context of the claim as a whole. *Id.* ¶101. 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 “Security-enhancing sub application” 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”). *Id.* Even under Petitioner’s theory on Naslund, the 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. *Id.*

Moreover, 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. *Id.* ¶102. 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. *Id.* Petitioner’s interpretation of Naslund flies in the face of this claimed premise, because the “Security-enhancing sub application” codes of Naslund can be associated with *multiple* interfaces (e.g., Bluetooth *and* 3G radio)—they would do nothing to 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. *Id.*

Petitioner thus fails to demonstrate that Naslund teaches or suggests Claim 1[d]. While Petitioner speculates that the Examiner overlooked these teachings of Naslund, the clear conclusion to be drawn is that the Examiner correctly determined that the alleged service codes are not associated with an identified communication channel. Instead, they are associated with the “Security-enhancing sub application,” which is why the codes are listed in that column.

2. Claim 1[e]

Petitioner states that in Naslund the authentication response RES' “is

calculated using the RAND value from the authentication request.” Pet., 63.⁵ However, Petitioner then makes the unsubstantiated leap 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:

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 plainly wrong.

First, Petitioner fails to substantiate that the authentication response RES’ is in any way dependent on the selected security-enhancing sub application. The only portion of Naslund cited by Petitioner to support this assertion is page 17, lines 3-8. That is nothing more than a vague statement that different security policies can be

⁵ Notably, Petitioner considers RES’ to be the “authentication response” for Naslund, which contradicts Petitioner’s theory on TS-33.402 that the entire EAP-RSP/AKA-Challenge message is the “authentication response” (rather than RES contained within that message).

customized and selected, and nothing in the passage even begins to suggests determining the ***authentication response RES'*** based on the alleged service code. “It is of the utmost importance that petitioners in the IPR proceedings adhere to the requirement that the initial petition identify ‘with particularity’ the ‘evidence that supports the grounds for the challenge to each claim.’” *Intelligent Bio-Systems, Inc. v. Illumina Cambridge, Ltd.*, 821 F.3d 1359, 69 (Fed. Cir. 2016) (quoting 35 U.S.C.S. § 312(a)(3)). Petitioner fails to adhere to this requirement because it does not identify any portion of Naslund that supports its assertion. While Petitioner cites Dr. Almeroth’s declaration, he simply parrots back what is recited in the Petition and relies exclusively on the same citation of Naslund. *Compare* Ex. 1003 ¶¶209 with Pet. 64. His testimony is thus entitled to no weight. *See Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9 at 15 (PTAB Aug. 24, 2022) (precedential).

Second, even assuming that the AKA processing by the terminal differs depending on the selected security-enhancing sub application, that still would not teach that the authentication response RES' is “***calculated on the basis of the determined service code.***” Ex. 2001 ¶¶103-104. While 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. *Id.* Petitioner clearly understands what “calculating” means, as it points to the “challenge RAND”

as being the claimed “information in the authentication request” upon which the claimed “calculation” is based. Pet., 63. The challenge RAND is clearly part of the function used to calculate an authentication response RES, whereas the alleged service code clearly is **not**. Ex. 2001 ¶104 (citing Ex. 2003, 24 (“the USIM computes $RES = f2K(RAND)$ ”)). Naslund itself teaches “**comput[ing]** a response and/or one or more keys **based on** the challenge RAND (and the stored security key),” showing 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.

Recognizing this, Petitioner resorts to the tenuous argument 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’ and Petitioner cites nothing in Naslund to the contrary. Indeed, simply “selecting among” different “customized security-enhancing modules or sub application” (Ex. 1005, 17:5-8) to perform AKA operations does not teach calculating RES’ based on a service code. Ex. 2001 ¶105.

Additionally, Claim 1[e] recites 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. *Supra* Section V.D.1. 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. *Id.* Thus, while the security-enhancing sub application is dependent on its corresponding code, the code is not dependent on any identified communication channel. Ex. 2001 ¶106.

Third, the plain claim language 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. Consequently, Naslund does not teach the latter half of this limitation. *Id.* ¶107.

3. Claim 2

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”:

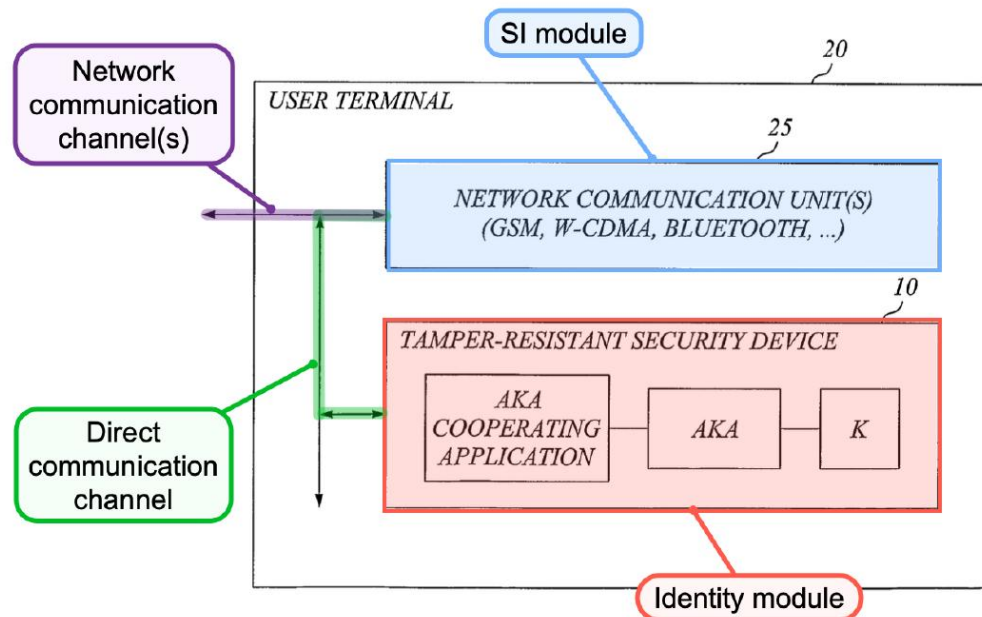


Fig. 4

Pet., 65-66.

Petitioner fails to demonstrate that Naslund teaches that the alleged SI module is “configured to **securely** communication with the identity module.” Petitioner relies exclusively on teachings *from the '235 Patent* that its SI module can “provide a secure communication channel ... with the UICC ... connected to the SI module.” Pet., 65 (citing Ex. 1001, 8:1-3). Indeed, Petitioner does not actually cite or discuss any portion of Naslund to support that the alleged SI module *of Naslund* is

configured to provide “secure” communication. To the contrary, Naslund teaches only that the terminal “generally has some form of communication capabilities”—Naslund is entirely 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. Ex. 2001 ¶¶108-109. This is in stark contrast to 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. Petitioner fails to identify any comparable teaching in Naslund regarding the network communication unit(s) 25. Ex. 2001 ¶109.

Petitioner also fails to demonstrate that Naslund teaches that the alleged SI module is “configured to ... *to identify* the communications channel through which the authentication request was received.” For example, 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. Petitioner simply assumes that the “network communication unit(s)” 25 of Naslund identifies the interface that the authentication request was received on. However, Naslund is silent as to which component of the terminal performs the interface identification, and instead only vaguely states that “the terminal (mobile)” determines the interface. Ex. 2001 ¶110 (quoting Ex. 1005, 19:23-29). If anything,

Naslund strongly suggests that the interface identification would be performed by the SIM. *Id.* (citing Ex. 1005, 23:21-23 (“[A]ll AKA related processing takes place on the SIM, including the security enhancing step.”)). Petitioner thus fails to demonstrate that the alleged SI module performs the claimed channel identification.

4. Claim 3[a]

Petitioner contends 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.

Naslund does not teach that the identified channel, or even the “Security-enhancing sub application” code for that matter, serves as the basis for the alleged modified authentication request. 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. *Supra* Section V.D.1. The identified channel thus cannot serve as “the basis” of those modifications. Ex. 2001 ¶¶111-112. 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. *Id.* ¶112. 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'. *Id.* (citing Ex. 1001, 9:60-66).

5. Claim 4[b]

Petitioner contends 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. This is essentially the same theory applied to Claim 3[a] and thus fails for the same reasons. *Supra* Section V.D.4; Ex. 2001 ¶113.

6. Claim 5[b]-[c]

Petitioner’s invalidity theory on Claim 5 is misplaced for several reasons. For one, this claim recites “the network generating an expected service code on the basis of the type of communications channel the service request ***was sent*** to the network.” Thus, the expected service code must be generated *after* the service request has been sent by the terminal to the network. Petitioner cannot carry its burden of showing that Naslund teaches this, because Petitioner does not address or explain *when* the alleged expected service code of Naslund is generated. Petitioner instead focuses solely on *whether* (not when) Naslund generates an expected service code.

Moreover, Petitioner’s contention 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” is premised on the same flawed logic offered by Petitioner with respect to Claims 1[d] and 1[e]. *Supra* Sections V.D.1-2. 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. Ex. 2001 ¶114. For Claim 5, Petitioner further 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. Pet., 71. Naslund thus fails to teach these limitations for the same reasons it fails to teach Claims 1[d] and 1[e]. Ex. 2001 ¶114.

VI. CONCLUSION

For the reasons above, KPN requests that the Board deny institution.

Dated: May 27, 2025

Respectfully submitted,

/Stephen D. Zinda/

Stephen D. Zinda

Registration No. 67,272

Counsel for KPN

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 42.6(e)(4), the undersigned certifies that on May 27, 2025, a copy of the foregoing document (*Patent Owner's Preliminary Response*, including all Exhibits), was served via electronic mail on the following attorneys of record at the indicated e-mail address(es):

jimglass@quinnemanuel.com
johnmckee@quinnemanuel.com
quincylu@quinnemanuel.com
ronhagiz@quinnemanuel.com
landonsmith@quinnemanuel.com
leonlin@quinnemanuel.com

/Stephen D. Zinda/
Stephen D. Zinda

CERTIFICATE OF COMPLIANCE

The undersigned certifies that this document complies with the type-volume limitations set forth in 37 C.F.R. § 42.24 *et seq.* This document, excluding those portions excluded pursuant to § 42.24(a)(1), contains 13,988 words as calculated by the “Word Count” feature of Microsoft Word for Office 365, the program used in creating it.

/Stephen D. Zinda/
Stephen D. Zinda