

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 10,425,817 B2
APPLICATION NO. : 16/200037
DATED : September 24, 2019
INVENTOR(S) : Torvinen et al.

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Drawings

In Fig. 4, Sheet 3 of 11, Line 4, delete “identifier” and insert -- identifier) --, therefor.

In Fig. 4, Sheet 3 of 11, Line 5, delete “(null-scheme,” and insert -- (null-scheme), --, therefor.

In Fig. 15, Sheet 9 of 11, Line 5, delete “identifier” and insert -- identifier) --, therefor.

In Fig. 15, Sheet 9 of 11, Line 5, delete “(null-scheme,” and insert -- (null-scheme), --, therefor.

In the Specification

In Column 7, Line 61, delete “FIG. 3-8:” and insert -- FIGS. 3-8: --, therefor.

In Column 12, Line 7, delete “and or” and insert -- and/or --, therefor.

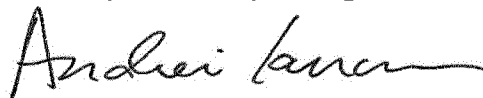
In Column 17, Line 63, delete “an Home” and insert -- a Home --, therefor.

In the Claims

In Column 21, Line 13, in Claim 1, delete “identifier” and insert -- identifier, --, therefor.

In Column 22, Line 13, in Claim 10, delete “(SUPI) ,” and insert -- (SUPI), --, therefor.

Signed and Sealed this
Twenty-first Day of April, 2020



Andrei Iancu
Director of the United States Patent and Trademark Office



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/200,037	11/26/2018	Vesa TORVINEN	3602-1734US2	8611
6449	7590	04/02/2020		
ROTHWELL, FIGG, ERNST & MANBECK, P.C. 607 14TH STREET, N.W. SUITE 800 WASHINGTON, DC 20005			EXAMINER HO, HUY C	
			ART UNIT	PAPER NUMBER
			2644	
			NOTIFICATION DATE	DELIVERY MODE
			04/02/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTO-PAT-Email@rfem.com



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

Patent No.: 10425817
Issue Date: 09/24/2019
Appl. No.: 16/200,037
Filed: 11/26/2018

PART (A) RESPONSE FOR CERTIFICATES OF CORRECTION

This is a decision on the Certificate of Correction request filed 05 March 2020.

The request for issuance of Certificate of Correction for the above-identified correction(s) under the provisions of 37 CFR 1.322 and/or 1.323 is hereby:

(Check one)

☒ Approved ☐ Approved in Part ☐ Denied

Comments: _____

PART (B) PETITION UNDER 37 CFR 1.324 OR 37 CFR 1.48

☐ This is a decision on the petition filed _____ to correct inventorship under 37 CFR 1.324.

☐ This is a decision on the request under 37 CFR 1.48, petition filed _____. In view of the fact that the patent has already issued, the request under 37 CFR 1.48 has been treated as a petition to correct inventorship under 37 CFR 1.324.

The petition is hereby: ☐ Granted ☐ Dismissed

Comment: _____

The patented filed is being forwarded to Certificate of Corrections Branch for issuance of a certificate naming only the actual inventor or inventors.

/KATHY W WANG-HURST/
Supervisory Patent Examiner, Art Unit 2644
Technology Center 2600
Phone: (571)270-5371

Certificates of Correction Branch email: CustomerServiceCoC@uspto.gov CoC Central Phone Number: (703) 756-1814

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

IN RE APPLICATION OF: U.S. Patent No. 10,425,817

USPTO CONFIRMATION CODE: 8611

APPLICATION NO.: 16/200,037

FILED: November 26, 2018

EXAMINER: Huy C Ho

GROUP ART UNIT: 2644

FOR: SUBSCRIPTION CONCEALED IDENTIFIER

37 CFR 1.322 & 37 CFR 1.323 REQUEST FOR CERTIFICATE OF CORRECTION
FOR USPTO AND/OR APPLICANT MISTAKE

HONORABLE COMMISSIONER OF PATENTS & TRADEMARKS

SIR:

The following is a request for a certificate of correction in Serial Number 16/200,037, now Patent Number 10,425,817.

A certificate of correction under 35 USC 254 is respectfully requested in the above-identified patent.

The errors were the fault of both the applicant and USPTO and, accordingly, please charge **\$150.00** to our Deposit Account No. 50-1379. In the event that a further fee is required, please charge the amount to the same Deposit Account.

The exact locations where the errors appear in the patent and patent application are as follows:

In Fig. 4, Sheet 3 of 11, Line 4, delete “identifier” and insert - - identifier) - -, therefor.

(ORIGINALLY FILED SPECIFICATION, IN THE DRAWINGS DATED NOVEMBER 26, 2018, SHEET 3 (PAGE 256 OF FW), FIGURE 4, LINE 4)

In Fig. 4, Sheet 3 of 11, Line 5, delete “(null-scheme,” and insert - - (null-scheme), - -, therefor.

(ORIGINALLY FILED SPECIFICATION, IN THE DRAWINGS DATED NOVEMBER 26, 2018, SHEET 3 (PAGE 256 OF FW), FIGURE 4, LINE 5)

In Fig. 15, Sheet 9 of 11, Line 5, delete “identifier” and insert - - identifier) - -, therefor.

(ORIGINALLY FILED SPECIFICATION, IN THE DRAWINGS DATED NOVEMBER 26, 2018, SHEET 9 (PAGE 262 OF FW), FIGURE 15, LINE 5)

In Fig. 15, Sheet 9 of 11, Line 5, delete “(null-scheme,” and insert - - (null-scheme), - -, therefor.

(ORIGINALLY FILED SPECIFICATION, IN THE DRAWINGS DATED NOVEMBER 26, 2018, SHEET 9 (PAGE 262 OF FW), FIGURE 15, LINE 6)

In Column 7, Line 61, delete “FIG. 3-8:” and insert - - FIGS. 3-8: - -, therefor.

(ORIGINALLY FILED SPECIFICATION DATED NOVEMBER 26, 2018, PAGE 11 OF 35, PARAGRAPH [0079], LINE 2)

In Column 12, Line 7, delete “and or” and insert - - and/or - -, therefor.

(ORIGINALLY FILED SPECIFICATION DATED NOVEMBER 26, 2018, PAGE 17 OF 35, PARAGRAPH [00100], LINE 3)

In Column 17, Line 63, delete “an Home” and insert - - a Home - -, therefor.

(ORIGINALLY FILED SPECIFICATION DATED NOVEMBER 26, 2018, PAGE 26 OF 35, LINE 2)

In Column 21, Line 13, in Claim 1, delete “identifier” and insert - - identifier, - -, therefor.

(AMENDMENTS TO THE CLAIMS DATED APRIL 23, 2019, PAGE 2 OF 11, CLAIM 1, LINE 12)

In Column 22, Line 13, in Claim 10, delete “(SUPI),” and insert - - (SUPI), - -, therefor.

(AMENDMENTS TO THE CLAIMS DATED APRIL 23, 2019, PAGE 4 OF 11, CLAIM 13, LINE 2)

The requested corrections are attached on Form PTO 1050.

Respectfully Submitted

, 2020

DATE

/Ronald J. Ward, Reg#54870/

Ronald J. Ward
Registration No. 54,870
Attorney of Record

UNITED STATES PATENT AND TRADEMARK OFFICE CERTIFICATE OF CORRECTION

Page 1 of 2

PATENT NO. : 10,425,817 B2

APPLICATION NO. : 16/200,037

ISSUE DATE : September 24, 2019

INVENTOR(S) : Torvinen, et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In Fig. 4, Sheet 3 of 11, Line 4, delete “identifier” and insert - - identifier) - -, therefor.

In Fig. 4, Sheet 3 of 11, Line 5, delete “(null-scheme,” and insert - - (null-scheme), - -, therefor.

In Fig. 15, Sheet 9 of 11, Line 5, delete “identifier” and insert - - identifier) - -, therefor.

In Fig. 15, Sheet 9 of 11, Line 5, delete “(null-scheme,” and insert - - (null-scheme), - -, therefor.

In Column 7, Line 61, delete “FIG. 3-8:” and insert - - FIGS. 3-8: - -, therefor.

In Column 12, Line 7, delete “and or” and insert - - and/or - -, therefor.

In Column 17, Line 63, delete “an Home” and insert - - a Home - -, therefor.

MAILING ADDRESS OF SENDER (Please do not use customer number below):

6300 Legacy, MS EVR 1-C-11
Plano, TX 75024
972-583-8656

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1.0 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Attention Certificate of Corrections Branch, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE CERTIFICATE OF CORRECTION

Page 2 of 2

PATENT NO. : 10,425,817 B2

APPLICATION NO. : 16/200,037

ISSUE DATE : September 24, 2019

INVENTOR(S) : Torvinen, et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In Column 21, Line 13, in Claim 1, delete "identifier" and insert - - identifier, - -, therefor.

In Column 22, Line 13, in Claim 10, delete "(SUPD) ," and insert - - (SUPD), - -, therefor.

MAILING ADDRESS OF SENDER (Please do not use customer number below):

6300 Legacy, MS EVR 1-C-11
Plano, TX 75024
972-583-8656

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1.0 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Attention Certificate of Corrections Branch, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	16200037			
Filing Date:	26-Nov-2018			
Title of Invention:	SUBSCRIPTION CONCEALED IDENTIFIER			
First Named Inventor/Applicant Name:	Vesa TORVINEN			
Filer:	Brian Michael Kearns/Amber Rodgers			
Attorney Docket Number:	3602-1734US2			
Filed as Large Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
CERTIFICATE OF CORRECTION	1811	1	150	150

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				150

Electronic Acknowledgement Receipt

EFS ID:	38780002
Application Number:	16200037
International Application Number:	
Confirmation Number:	8611
Title of Invention:	SUBSCRIPTION CONCEALED IDENTIFIER
First Named Inventor/Applicant Name:	Vesa TORVINEN
Customer Number:	6449
Filer:	Brian Michael Kearns/Amber Rodgers
Filer Authorized By:	Brian Michael Kearns
Attorney Docket Number:	3602-1734US2
Receipt Date:	05-MAR-2020
Filing Date:	26-NOV-2018
Time Stamp:	14:19:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	\$ 150
RAM confirmation Number	E202035E19493795
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Certificate of Correction	P72588-US2_2020-03-05_CoC_Request_Letter.pdf	141388	no	3
			522be8f0033c8162fb8efabe81af4df8f04b8957		
Warnings:					
Information:					
2	Request for Certificate of Correction	P72588-US2_2020-03-05_CoC.pdf	137118	no	3
			04d849400b17b36fc1e31942876720b199ae78f5		
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30239	no	2
			0af84d7087348c018797d18ec9b817d22dfb6f92		
Warnings:					
Information:					
Total Files Size (in bytes):			308745		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					



APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/200,037	09/24/2019	10425817	3602-1734US2	8611

6449 7590 09/04/2019

ROTHWELL, FIGG, ERNST & MANBECK, P.C.
607 14th Street, N.W.
SUITE 800
WASHINGTON, DC 20005

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Vesa TORVINEN, Sauvo, FINLAND;
Telefonaktiebolaget LM Ericsson (publ), Stockholm, SWEDEN;
Noamen BEN HENDA, Stockholm, SWEDEN;
David CASTELLANOS ZAMORA, Madrid, SPAIN;
Prajwol Kumar NAKARMI, Sollentuna, SWEDEN;
Pasi SAARINEN, Jarfalla, SWEDEN;
Monica WIFVESSON, Lund, SWEDEN;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/200,037	11/26/2018	Vesa TORVINEN	3602-1734US2	8611
6449	7590	08/29/2019		
ROTHWELL, FIGG, ERNST & MANBECK, P.C. 607 14th Street, N.W. SUITE 800 WASHINGTON, DC 20005			EXAMINER HO, HUY C	
			ART UNIT	PAPER NUMBER
			2644	
			NOTIFICATION DATE	DELIVERY MODE
			08/29/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTO-PAT-Email@rfem.com

Corrected Notice of Allowability	Application No. 16/200,037	Applicant(s) TORVINEN et al.	
	Examiner HUY C HO	Art Unit 2644	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 08/26/2019.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on ____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are 1,3,5-11,13-16,19-20 and 22-23. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov**.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) ☐ All b) ☐ Some *c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.

2. ☐ Certified copies of the priority documents have been received in Application No. ____.

3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: ____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date ____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892) 2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date ____. 3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material ____. 4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____.	5. ☐ Examiner's Amendment/Comment 6. ☐ Examiner's Statement of Reasons for Allowance 7. ☐ Other _____.
---	---

/HUY C HO/ Primary Examiner, Art Unit 2644	
---	--



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/200,037	11/26/2018	Vesa TORVINEN	3602-1734US2	8611
6449	7590	08/26/2019		
ROTHWELL, FIGG, ERNST & MANBECK, P.C. 607 14th Street, N.W. SUITE 800 WASHINGTON, DC 20005			EXAMINER HO, HUY C	
			ART UNIT	PAPER NUMBER
			2644	
			NOTIFICATION DATE	DELIVERY MODE
			08/26/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTO-PAT-Email@rfem.com

Corrected Notice of Allowability	Application No. 16/200,037	Applicant(s) TORVINEN et al.	
	Examiner HUY C HO	Art Unit 2644	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 04/23/2019.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are See Continuation Sheet. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov**.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) ☐ All b) ☐ Some *c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.

2. ☐ Certified copies of the priority documents have been received in Application No. _____.

3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

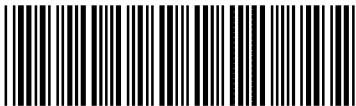
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892) 2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____ 3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____ 4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____	5. ☐ Examiner's Amendment/Comment 6. ☐ Examiner's Statement of Reasons for Allowance 7. ☒ Other <u>See Attached Corrected Issue Classification</u> .
--	--

/HUY C HO/ Primary Examiner, Art Unit 2644	
---	--

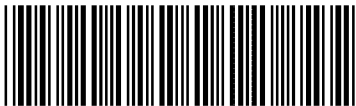
Continuation of 3. The allowed claim(s) is/are: 1,3,5-11,13-16,19-20 and 22

Issue Classification 	Application/Control No. 16/200,037	Applicant(s)/Patent Under Reexamination TORVINEN et al.	
	Examiner HUY C HO	Art Unit 2644	

CPC						
Symbol					Type	Version
H04W	/	12	/	06	F	2013-01-01
H04L	/	63	/	0414	I	2013-01-01
H04L	/	63	/	06	I	2013-01-01
H04W	/	12	/	02	I	2013-01-01
H04W	/	12	/	04	I	2013-01-01
H04L	/	9	/	3066	I	2013-01-01
H04L	/	63	/	0428	I	2013-01-01
H04W	/	8	/	18	I	2013-01-01
H04W	/	60	/	00	I	2013-01-01
H04L	/	9	/	083	I	2013-01-01
H04L	/	9	/	0841	I	2013-01-01
H04L	/	9	/	088	I	2013-01-01
H04L	/	9	/	321	I	2013-01-01
H04L	/	63	/	123	A	2013-01-01
H04W	/	12	/	10	A	2013-01-01
H04L	/	2463	/	061	A	2013-01-01
H04W	/	12	/	00518	A	2019-01-01
H04L	/	2209	/	80	A	2013-01-01

CPC Combination Sets					
Symbol			Type	Set	Ranking
/	/				

NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 17	
/HUY C HO/ Primary Examiner, Art Unit 2644 (Primary Examiner) _____ (Date) _____		O.G. Print Claim(s) 1	O.G. Print Figure 3

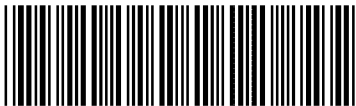
Issue Classification 	Application/Control No. 16/200,037	Applicant(s)/Patent Under Reexamination TORVINEN et al.
	Examiner HUY C HO	Art Unit 2644

INTERNATIONAL CLASSIFICATION			
CLAIMED			
H04M	/	1	/ 66
NON-CLAIMED			
/		/	

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS
455	411

CROSS REFERENCES(S)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)					
455	410	435.1	435.2	435.3		
380	277	278	279	280	281	282
380	283	284	285			

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	17	
/HUY C HO/ Primary Examiner, Art Unit 2644	19 August 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

Issue Classification 	Application/Control No. 16/200,037	Applicant(s)/Patent Under Reexamination TORVINEN et al.
	Examiner HUY C HO	Art Unit 2644

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47															
CLAIMS															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	8	10	14	19										
	2	9	11	15	20										
2	3		12		21										
	4	10	13	16	22										
3	5	11	14	17	23										
4	6	12	15												
5	7	13	16												
6	8		17												
7	9		18												

NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 17	
/HUY C HO/ Primary Examiner, Art Unit 2644 (Primary Examiner) _____ (Date) 19 August 2019		O.G. Print Claim(s) 1	O.G. Print Figure 3

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

6449 7590 07/10/2019
ROTHWELL, FIGG, ERNST & MANBECK, P.C.
607 14th Street, N.W.
SUITE 800
WASHINGTON, DC 20005

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/200,037	11/26/2018	Vesa TORVINEN	3602-1734US2	8611

TITLE OF INVENTION: SUBSCRIPTION CONCEALED IDENTIFIER

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$1000	\$0.00	\$0.00	\$1000	10/10/2019

EXAMINER	ART UNIT	CLASS-SUBCLASS
HO, HUY C	2644	455-411000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

- (1) The names of up to 3 registered patent attorneys or agents OR, alternatively, 1 Rothwell, Figg, Ernst & Manbeck P.C.
- (2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 _____
- 3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Telefonaktiebolaget LM Ericsson (publ)

Stockholm, Sweden

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☒ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

- ☒ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)
- ☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 02-2135

5. Change in Entity Status (from status indicated above)

- ☐ Applicant certifying micro entity status. See 37 CFR 1.29
- ☐ Applicant asserting small entity status. See 37 CFR 1.27
- ☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature Brian S. Rosenbloom

Typed or printed name Brian S. Rosenbloom

Date 2-17-2019

Registration No. 41276

Electronic Patent Application Fee Transmittal

Application Number:	16200037			
Filing Date:	26-Nov-2018			
Title of Invention:	SUBSCRIPTION CONCEALED IDENTIFIER			
First Named Inventor/Applicant Name:	Vesa TORVINEN			
Filer:	Brian S. Rosenbloom/Xania Steele			
Attorney Docket Number:	3602-1734US2			
Filed as Large Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	1501	1	1000	1000

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				1000

Electronic Acknowledgement Receipt

EFS ID:	36810900
Application Number:	16200037
International Application Number:	
Confirmation Number:	8611
Title of Invention:	SUBSCRIPTION CONCEALED IDENTIFIER
First Named Inventor/Applicant Name:	Vesa TORVINEN
Customer Number:	6449
Filer:	Brian S. Rosenbloom/Xania Steele
Filer Authorized By:	Brian S. Rosenbloom
Attorney Docket Number:	3602-1734US2
Receipt Date:	07-AUG-2019
Filing Date:	26-NOV-2018
Time Stamp:	16:10:40
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	\$ 1000
RAM confirmation Number	E201987G11269423
Deposit Account	022135
Authorized User	Xania Steele

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

Lenovo Ex. 1009

Page 26

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	3602-1734US2_Issue-Fee-Transmittal.pdf	3177254	no	1
			b82678a5e2eb75c73ad2f9e89b171e75fc357ff9		
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30121	no	2
			98ab1c1c32ecdb1978479330a4b47b9713d79e8d		
Warnings:					
Information:					
Total Files Size (in bytes):			3207375		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No. : 16/200037
First Named Inventor : Vesa TORVINEN
Filed : November 26, 2018
TC/A.U. : 2644
Examiner : Huy C. Ho

Docket No. : 3602-1734US2
Customer No. : 6449
Confirmation No. : 8611

SUBMISSION OF DECLARATION

Director of the United States Patent
and Trademark Office
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

Submitted herewith are the declarations of the inventors in connection with the above-identified patent application.

The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 02-2135.

Respectfully submitted,

/Brian S. Rosenbloom/

By _____
Brian S. Rosenbloom
Attorney for Applicant
Registration No. 41,276
ROTHWELL, FIGG, ERNST & MANBECK, p.c.
Suite 800, 607 14th Street, N.W.
Washington, D.C. 20005
Telephone: (202)783-6040

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)	
<i>Caution: A person may not execute an oath or declaration for an application unless that person has reviewed and understands the contents of the application, including the claims, and is aware of the duty to disclose to the US Patent and Trademark Office all information known to the person to be material to patentability as defined in 37 CFR 1.56.</i>	
Title of Invention	SUBSCRIPTION CONCEALED IDENTIFIER
As the below named inventor, I hereby declare that: This declaration is directed to: ☐ The attached application, or ☒ United States application or PCT international application number <u>16/200037</u> filed on <u>February 12, 2019</u> The above-identified application was made or authorized to be made by me. I believe that I am the original inventor or an original joint inventor of a claimed invention in the application. I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.	
LEGAL NAME OF INVENTOR	
Typed Name of Inventor: Vesa TORVINEN	
Signature of Inventor: 	Date (optional):

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)**

Caution: A person may not execute an oath or declaration for an application unless that person has reviewed and understands the contents of the application, including the claims, and is aware of the duty to disclose to the US Patent and Trademark Office all information known to the person to be material to patentability as defined in 37 CFR 1.56.

Title of
Invention

SUBSCRIPTION CONCEALED IDENTIFIER

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number 16/200037
filed on February 12, 2019

The above-identified application was made or authorized to be made by me.

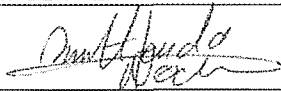
I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

LEGAL NAME OF INVENTOR

Typed Name of Inventor: Noamen BEN HENDA

Signature of Inventor:



Date (optional): 2019-03-01

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)**

Caution: A person may not execute an oath or declaration for an application unless that person has reviewed and understands the contents of the application, including the claims, and is aware of the duty to disclose to the US Patent and Trademark Office all information known to the person to be material to patentability as defined in 37 CFR 1.56.

Title of
Invention

SUBSCRIPTION CONCEALED IDENTIFIER

As the below named inventor, I hereby declare that:

This declaration is directed to:

- ☐ The attached application, or
- ☒ United States application or PCT international application number 16/200037
filed on February 12, 2019.

The above-identified application was made or authorized to be made by me.

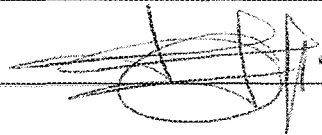
I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

LEGAL NAME OF INVENTOR

Typed Name of Inventor: David CASTELLANOS ZAMORA

Signature of Inventor:



Date (optional):

Last Modified 7/11/2019

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)**

Caution: A person may not execute an oath or declaration for an application unless that person has reviewed and understands the contents of the application, including the claims, and is aware of the duty to disclose to the US Patent and Trademark Office all information known to the person to be material to patentability as defined in 37 CFR 1.56.

Title of
Invention

SUBSCRIPTION CONCEALED IDENTIFIER

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number 16/200037
filed on February 12, 2019

The above-identified application was made or authorized to be made by me.

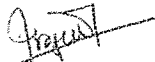
I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

LEGAL NAME OF INVENTOR

Typed Name of Inventor: Prajwol Kumar NAKARMI

Signature of Inventor:



Date (optional): 1st March, 2019

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)**

Caution: A person may not execute an oath or declaration for an application unless that person has reviewed and understands the contents of the application, including the claims, and is aware of the duty to disclose to the US Patent and Trademark Office all information known to the person to be material to patentability as defined in 37 CFR 1.56.

Title of
Invention

SUBSCRIPTION CONCEALED IDENTIFIER

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number 16/200037
filed on February 12, 2019.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

LEGAL NAME OF INVENTOR

Typed Name of Inventor: Pasi SAARINEN

Signature of Inventor:

Date (optional):

**DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN
APPLICATION DATA SHEET (37 CFR 1.76)**

Caution: A person may not execute an oath or declaration for an application unless that person has reviewed and understands the contents of the application, including the claims, and is aware of the duty to disclose to the US Patent and Trademark Office all information known to the person to be material to patentability as defined in 37 CFR 1.56.

Title of
Invention

SUBSCRIPTION CONCEALED IDENTIFIER

As the below named inventor, I hereby declare that:

This declaration is directed to:



The attached application, or



United States application or PCT international application number 16/200037
filed on February 12, 2019.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

LEGAL NAME OF INVENTOR

Typed Name of Inventor: Monica WIFVESSON

Signature of Inventor:

Monica Wifvesson

Date (optional): *2019-03-01*

Electronic Acknowledgement Receipt

EFS ID:	36553947
Application Number:	16200037
International Application Number:	
Confirmation Number:	8611
Title of Invention:	SUBSCRIPTION CONCEALED IDENTIFIER
First Named Inventor/Applicant Name:	Vesa TORVINEN
Customer Number:	6449
Filer:	Brian S. Rosenbloom/Xania Steele
Filer Authorized By:	Brian S. Rosenbloom
Attorney Docket Number:	3602-1734US2
Receipt Date:	11-JUL-2019
Filing Date:	26-NOV-2018
Time Stamp:	13:05:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	3602-1734US2_SubmissionDec.pdf	17679 05cf99ec6058c6aa813c396597be571052f0e50f	no	1

Warnings:

Lenovo Ex. 1009

Page 35

Information:					
2	Oath or Declaration filed	3602-1734US2_Declarations. pdf	630428	no	6
			142c60928d9f35010bcf8ade9625285b694 c1c15		
Warnings:					
Information:					
Total Files Size (in bytes):				648107	
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

6449 7590 07/10/2019
ROTHWELL, FIGG, ERNST & MANBECK, P.C.
607 14th Street, N.W.
SUITE 800
WASHINGTON, DC 20005

EXAMINER

HO, HUY C

ART UNIT

PAPER NUMBER

2644

DATE MAILED: 07/10/2019

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/200,037	11/26/2018	Vesa TORVINEN	3602-1734US2	8611

TITLE OF INVENTION: SUBSCRIPTION CONCEALED IDENTIFIER

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$1000	\$0.00	\$0.00	\$1000	10/10/2019

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

6449 7590 07/10/2019
ROTHWELL, FIGG, ERNST & MANBECK, P.C.
607 14th Street, N.W.
SUITE 800
WASHINGTON, DC 20005

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/200.037	11/26/2018	Vesa TORVINEN	3602-1734US2	8611

TITLE OF INVENTION: SUBSCRIPTION CONCEALED IDENTIFIER

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$1000	\$0.00	\$0.00	\$1000	10/10/2019

EXAMINER	ART UNIT	CLASS-SUBCLASS
HO, HUY C	2644	455-411000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

1 _____

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☐ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

☐ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. Change in Entity Status (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/200,037	11/26/2018	Vesa TORVINEN	3602-1734US2	8611
6449	7590	07/10/2019	EXAMINER	
ROTHWELL, FIGG, ERNST & MANBECK, P.C. 607 14th Street, N.W. SUITE 800 WASHINGTON, DC 20005			HO, HUY C	
			ART UNIT	PAPER NUMBER
			2644	

DATE MAILED: 07/10/2019

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

<i>Notice Requiring Inventor's Oath or Declaration</i>	Application No. 16/200,037	Applicant(s) Vesa TORVINEN	
	Examiner HO, HUY C	Art Unit 2644	

This notice is an attachment to the Notice of Allowability (PTOL-37), or the Notice of Allowability For A Design Application (PTOL-37D).

An inventor's oath or declaration in compliance with 37 CFR 1.63 or 1.64 executed by or with respect to each inventor has not yet been submitted.

An oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each inventor (for any inventor for which a compliant oath, declaration, or substitute statement has not yet been submitted) **MUST** be filed no later than the date on which the issue fee is paid. See 35 U.S.C. 115(f). Failure to timely comply will result in ABANDONMENT of this application.

A properly executed inventor's oath to declaration has not been received for the following inventor(s):

If applicant previously filed one or more oaths, declarations, or substitute statements, applicant may have received an informational notice regarding deficiencies therein.

The following deficiencies are noted:

INFORMAL ACTION PROBLEMS

- A properly executed inventor's oath or declaration has not been received for the following inventor(s): **Vesa TORVINEN, Noamen BEN HENDA, David CASTELLANOS ZAMORA, Prajwol Kumar NAKARMI, Pasi SAARINEN, and Monica WIFVESSON.**

Applicant may submit the inventor's oath or declaration at any time before the Notice of Allowance and Fee(s) Due, PTOL-85, is mailed.

Questions relating to this Notice should be directed to the Application Assistance Unit at 571-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 16/200,037	Applicant(s) TORVINEN et al.	
	Examiner HUY C HO	Art Unit 2644	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 04/23/2019.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are See Continuation Sheet. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov**.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) ☐ All b) ☐ Some *c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.

2. ☐ Certified copies of the priority documents have been received in Application No. _____.

3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file areply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892) 2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____. 3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____. 4. ☒ Interview Summary (PTO-413), Paper No./Mail Date. <u>20190629</u> .	5. ☐ Examiner's Amendment/Comment 6. ☒ Examiner's Statement of Reasons for Allowance 7. ☐ Other _____.
--	--

/HUY C HO/ Primary Examiner, Art Unit 2644	
---	--

Continuation of 3. The allowed claim(s) is/are: 1,3,5-11,13-16,19-20 and 22-23

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Response to Arguments

2. Applicant's arguments filed on 04/23/20119 have been fully considered and are persuasive. The rejection of claims 1, 3, 5-11, 13-16, 19, 20, 22 and 23 has been withdrawn.

Allowable Subject Matter

3. Claims 1, 3, 5-11, 13-16, 19, 20, 22 and 23 are allowed.

4. The following is an examiner's statement of reasons for allowance:

The arguments made in the Applicant Arguments/Remarks on 04/23/20119 have been fully considered and are persuasive. Further search has been updated. However, no reference is found alone or in any combination with the prior art of record to provide the teachings, suggestions or disclosures of the unique claimed features/limitations from the independent claims filed on 04/23/20119.

Therefore, claims 1, 3, 5-11, 13-16, 19, 20, 22 and 23 are deemed allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to HUY C HO whose telephone number is (571)270-1108. The examiner can normally be reached on M-F 8AM-5PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, KATHY WANG-HURST can be reached on (571)270-5371. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

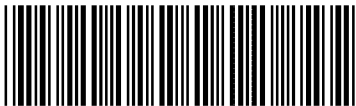
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications

Art Unit: 2644

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/HUY C HO/

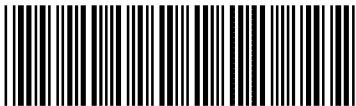
Primary Examiner, Art Unit 2644

Issue Classification 	Application/Control No. 16/200,037	Applicant(s)/Patent Under Reexamination TORVINEN et al.	
	Examiner HUY C HO	Art Unit 2644	

CPC						
Symbol					Type	Version
H04W	/	12	/	06	F	2013-01-01
H04L	/	63	/	0414	I	2013-01-01
H04L	/	63	/	06	I	2013-01-01
H04W	/	12	/	02	I	2013-01-01
H04W	/	12	/	04	I	2013-01-01
H04L	/	9	/	3066	I	2013-01-01
H04L	/	63	/	0428	I	2013-01-01
H04W	/	8	/	18	I	2013-01-01
H04W	/	60	/	00	I	2013-01-01
H04L	/	9	/	083	I	2013-01-01
H04L	/	9	/	0841	I	2013-01-01
H04L	/	9	/	088	I	2013-01-01
H04L	/	9	/	321	I	2013-01-01
H04L	/	63	/	123	A	2013-01-01
H04W	/	12	/	10	A	2013-01-01
H04L	/	2463	/	061	A	2013-01-01
H04W	/	12	/	00518	A	2019-01-01
H04L	/	2209	/	80	A	2013-01-01

CPC Combination Sets					
Symbol				Type	Set

NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 16	
/HUY C HO/ Primary Examiner, Art Unit 2644 (Primary Examiner) _____ (Date) _____		O.G. Print Claim(s) 1	O.G. Print Figure 3

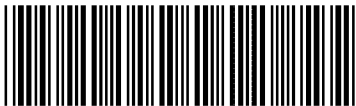
Issue Classification 	Application/Control No. 16/200,037	Applicant(s)/Patent Under Reexamination TORVINEN et al.
	Examiner HUY C HO	Art Unit 2644

INTERNATIONAL CLASSIFICATION			
CLAIMED			
H04M	/	1	/ 66
NON-CLAIMED			
/		/	

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS
455	411

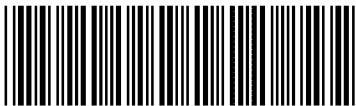
CROSS REFERENCES(S)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)					
455	410	435.1	435.2	435.3		
380	277	278	279	280	281	282
380	283	284	285			

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	16	
/HUY C HO/ Primary Examiner, Art Unit 2644	03 July 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

Issue Classification 	Application/Control No. 16/200,037	Applicant(s)/Patent Under Reexamination TORVINEN et al.
	Examiner HUY C HO	Art Unit 2644

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47															
CLAIMS															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1		10	13	19										
	2	8	11	14	20										
2	3		12		21										
	4	9	13	15	22										
3	5	10	14	16	23										
4	6	11	15												
5	7	12	16												
6	8		17												
7	9		18												

NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 16	
/HUY C HO/ Primary Examiner, Art Unit 2644 (Primary Examiner) _____ (Date) _____		03 July 2019 O.G. Print Claim(s) 1	O.G. Print Figure 3

Search Notes 	Application/Control No. 16/200,037	Applicant(s)/Patent Under Reexamination TORVINEN et al.
	Examiner HUY C HO	Art Unit 2644

CPC - Searched*		
Symbol	Date	Examiner
H04W12/00; H04W12/001; H04W12/02; H04W12/04; H04W12/06; H04W12/0602; H04W12/0605; H04W8/18; H04W60/00; H04L63/0414; H04L63/0428	03/07/2019	HH

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
455	411	03/07/2019	HH

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
EAST Database Search	03/07/2019	HH
Inventor Search	03/07/2019	HH
Search updated	07/03/2019	HH

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
455	410	03/07/2019	HH
380	277-282; 283-285	03/07/2019	HH

/HUY C HO/ Primary Examiner, Art Unit 2644	
---	--

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	"20130003971".PN.	US-PGPUB; USPAT;	OR	ON	2019/03/07; 14:41
S2	134	((("TORVINEN" near3 ("Vesa")) OR (("BEN" near3 ("HENDA" near3 ("Noemen")) OR (("CASTELLANOS" near3 ("ZAMORA" near3 ("David")) OR (("NAKARMI" near3 ("Prajwol")) OR (("SAARI" near3 ("Pasi")) OR (("WIFFE" near3 ("Monica")))).INV.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT;	OR	ON	2019/03/07; 15:29
S3	223000	455/410-411 380/277-282 380/283-285 H04W12/00 H04W12/001 H04W12/02 H04W12/04 H04W12/06 H04W12/0602 H04W12/0605 H04W8/18 H04W60/00 H04L63/0414 H04L63/0428).cds,qpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/07; 18:47
S4	218974	S3 and (@ad<"20170725" @rlad<"20170725")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/07; 18:50
S5	90862	S4 and (authentica\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/07; 18:52
S6	56433	S5 and (server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/07; 18:52
S7	0	S6 and (SUCI)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/07; 18:52
S8	6289	S6 and ((encrypt\$3 cipher\$3 encode encoding) near4 (identifier identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/07; 18:54
S9	41	S8 and (conceal\$3 near4 (id identifier identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/07; 18:55
S10	13	S9 and ((decrypt\$3 decoding decode decipher\$3 de\$conceal\$3 reveal\$3) near4 (id identifier identifier))	US-PGPUB; USPAT;	OR	ON	2019/03/07; 18:56

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S11	4	S10 and (home near4 network near4 (id identification identifier))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/07; 18:58
S12	17	("20020004898" "20050289643" "20060235796" "20070107047" "20080123850" "20080260149" "6260147" "6785823" "7042988").PN. OR ("7594113").URPN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/07; 19:28
S13	15	("20020004898" "20050289643" "20060235796" "20070107047" "20080123850" "20080260149" "6260147" "6785823" "6904466" "6911974" "7042988" "7088822" "7224804" "7594113").PN. OR ("7945777").URPN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/07; 19:35
S14	142	("6175743" "6175922").PN. OR ("6260147").URPN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/07; 19:41
S15	2	(SUPI (subscription near4 permanent near4 identifier)) same (encrypt\$3 decrypt\$3) same (SUCI (subscription near4 concealed near4 identifier)) same (server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 17:49
S16	0	S15 and (@ad<"20170725" @riad<"20170725")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 17:49
S17	5	(SUPI (subscription near4 permanent near4 identifier)) same (encrypt\$3 decrypt\$3) same (SUCI (subscription near4 concealed near4 identifier))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 17:49
S18	0	S17 and (@ad<"20170725" @riad<"20170725")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 17:49
S19	16	(SUPI (subscription near4 permanent near4 identifier)) same (encrypt\$3 decrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 17:50
S20	9	S19 and (@ad<"20170725" @riad<"20170725")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 17:50
S21	9	S20 and (server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 17:50
S22	9	S21 and ((conceal\$3 hidden encrypt\$3) near4 (id identifier identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 17:51

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S23	0	(subscription near4 permanent near4 identifier) same (encrypt\$3 decrypt\$3) same (subscription near4 concealed near4 identifier)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 18:11
S24	230665	(455/410-411 455/435.1-435.3 380/277-282 380/283-285 H04W12/00 H04W12/001 H04W12/02 H04W12/04 H04W12/06 H04W12/0602 H04W12/0605 H04W8/18 H04W60/00 H04L63/0414 H04L63/0428).cds,cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 18:36
S25	226507	S24 and (@ad<"20170725" @riad<"20170725")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 18:37
S26	26623	S25 and (authenticat\$3 near4 server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 18:38
S27	9822	S26 and (subscriber)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 18:39
S28	312	S27 and (home near4 network near4 (id identifier identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 18:40
S29	189	S28 and (encrypt\$3 decrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 18:40
S30	96	S29 and (scheme)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 18:41
S31	4	S29 and (conceal\$3 near4 (identifier id identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 18:41
S32	79	S29 and ((private public) near5 (key identifier identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2019/03/11; 18:43

S33	43	S32 and ((encrypt\$3 encod\$3) near4 (id identifier identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11: 18:52
S34	15	S33 and ((decrypt\$3 decod\$3) near4 (id identifier identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11: 18:54
S35	2508	(elliptic near4 curve near5 encryption)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13: 13:29
S36	573	(elliptic near4 curve near5 encryption near5 scheme)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13: 13:29
S37	0	(elliptic near4 curve near5 encryption near5 integrate near5 scheme)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13: 13:29
S38	266	(elliptic near4 curve near5 encryption near5 integrated near5 scheme)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13: 13:30
S39	262	S38 and (@ed<"20170725" @rlad<"20170725")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13: 13:30
S40	50	S39 and ((conceal\$3 encrypt\$3) near4 (id identifier identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13: 13:30
S41	0	S39 and ((conceal\$3) near4 (id identifier identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13: 13:30
S42	60	S39 and ((conceal\$3 encrypt\$3) near4 (subscription id identifier identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13: 13:31

S43	0	S42 and (home near4 network near5 (identifier identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 13:32
S44	11	S42 and (home near4 network)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 13:32
S45	11	S44 and (server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 13:32
S46	11	S45 and (public private)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 13:33
S47	0	S46 and (anchor)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 13:33
S48	11	S46 and (security)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 13:33
S49	266	(elliptic near4 curve near5 encryption near5 integrated near5 scheme)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 16:16
S50	262	S49 and (@ad<"20170725" @rlad<"20170725")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 16:16
S51	262	S50	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 16:16
S52	0	S51 and (null\$encryption near3 scheme)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 16:39
S53	0	S51 and (null\$encryption)	US-PGPUB; USPAT; USOCR;	OR	ON	2019/03/13; 16:49

						FPRS; EPO; JPO; DERWENT; IBM_TDB			
S54	45	(null\$encryption)				US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 16:49
S55	3	(null\$encryption near3 scheme)				US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 16:49
S56	3	S55 and (@ed<"20170725" @rlad<"20170725")				US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 16:49
S57	1	S56 and (authentical\$ near4 server)				US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 16:49
S58	5	((null\$encryption (null near2 encryption)) near3 scheme)				US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 16:52
S59	0	S58 and ((elliptic near4 curve near5 encryption near5 integrated near5 scheme)				US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 16:52
S60	5	S58 and (@ed<"20170725" @rlad<"20170725")				US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 17:06
S61	0	S60 and ((elliptic near4 curve near5 encryption)				US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 17:10
S62	0	S60 and ((elliptic curve) near5 encryption)				US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 17:10
S63	1	S60 and (authentical\$ near4 server)				US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2019/03/13; 17:11

S64	3	S60 and (authenticat\$3 server)	US-PGPUB; USPAT; USOCR; FPRS; EPO, JPO; DERWENT; IBM, TDB	OR	ON	2019/03/13; 17:11
S65	214	((null\$encryption (null near2 encryption)) near3 (algorithm scheme))	US-PGPUB; USPAT; USOCR; FPRS; EPO, JPO; DERWENT; IBM, TDB	OR	ON	2019/03/13; 17:14
S66	2	S65 and (elliptic near4 curve near5 encryption near5 integrated near5 scheme)	US-PGPUB; USPAT; USOCR; FPRS; EPO, JPO; DERWENT; IBM, TDB	OR	ON	2019/03/13; 17:14
S67	2	S66 and (@ad<"20170725" @rlad<"20170725")	US-PGPUB; USPAT; USOCR; FPRS; EPO, JPO; DERWENT; IBM, TDB	OR	ON	2019/03/13; 17:14
S68	214	S65 and (@ad<"20170725" @rlad<"20170725")	US-PGPUB; USPAT; USOCR; FPRS; EPO, JPO; DERWENT; IBM, TDB	OR	ON	2019/03/13; 17:22
S69	96	S68 and (authenticat\$3 near4 server)	US-PGPUB; USPAT; USOCR; FPRS; EPO, JPO; DERWENT; IBM, TDB	OR	ON	2019/03/13; 17:22
S70	1	S69 and (SUPI (subcription near4 permanent near4 identifier))	US-PGPUB; USPAT; USOCR; FPRS; EPO, JPO; DERWENT; IBM, TDB	OR	ON	2019/03/13; 17:22
S71	5	"20140019751"	US-PGPUB; USPAT; USOCR; FPRS; EPO, JPO; DERWENT; IBM, TDB	OR	ON	2019/03/25; 11:19
S72	8	"9,338,164"	US-PGPUB; USPAT; USOCR; FPRS; EPO, JPO; DERWENT; IBM, TDB	OR	ON	2019/03/25; 11:46
S73	2	"20180285602"	US-PGPUB; USPAT; USOCR; FPRS; EPO, JPO; DERWENT; IBM, TDB	OR	ON	2019/03/25; 12:23
S74	52	(20030046541 7188360 20190054899)	US-PGPUB; USPAT; USOCR; FPRS; EPO, JPO; DERWENT; IBM, TDB	OR	ON	2019/03/25;

EAST Search History

				USPAT; USOCR; FPRS; EPO, JPO; DERWENT; IBM_TDB			12:24
S75	2	(SUPI (subscription near4 permanent near4 identifi\$6)) same (authentica\$3) same (server) same (SUCI (subscription near4 conceal\$3 near4 identifi\$6)) same (encrypt\$3) same (decrypt\$3)		US-PGPUB; USPAT; USOCR; FPRS; EPO, JPO; DERWENT; IBM_TDB	OR	ON	2019/06/28; 10:36
S76	0	S75 and (@ad<"20170725" @rlad<"20170725")		US-PGPUB; USPAT; USOCR; FPRS; EPO, JPO; DERWENT; IBM_TDB	OR	ON	2019/06/28; 10:42
S77	5	(SUPI (subscription near4 permanent near4 identifi\$6)) and (authentica\$3) and server and (SUCI (subscription near4 conceal\$3 near4 identifi\$6)) and (encrypt\$3) and (decrypt\$3)		US-PGPUB; USPAT; USOCR; FPRS; EPO, JPO; DERWENT; IBM_TDB	OR	ON	2019/06/28; 10:43
S78	1	S77 and (@ad<"20170725" @rlad<"20170725")		US-PGPUB; USPAT; USOCR; FPRS; EPO, JPO; DERWENT; IBM_TDB	OR	ON	2019/06/28; 10:43
S79	2	("20190098502").PN.		US-PGPUB; USPAT; USOCR; DERWENT	OR	ON	2019/06/28; 10:43
S80	1	("20130003971").PN.		US-PGPUB; USPAT	OR	ON	2019/06/28; 12:55
S81	2	("20190098502").PN.		US-PGPUB; USPAT; USOCR; DERWENT	OR	ON	2019/06/28; 12:56
S82	2	("20190098502").PN.		US-PGPUB; USPAT; USOCR; DERWENT	OR	ON	2019/06/29; 13:38
S83	0	("not" near6 (encrypt\$3) near5 (home near4 network near4 (identification identifier)))		US-PGPUB; USPAT; USOCR; FPRS; EPO, JPO; DERWENT; IBM_TDB	OR	ON	2019/06/29; 13:53
S84	0	((("not" "no") near6 (encrypt\$3) near5 (home near4 network near4 (identification identifier))))		US-PGPUB; USPAT; USOCR; FPRS; EPO, JPO; DERWENT; IBM_TDB	OR	ON	2019/06/29; 13:53
S85	0	((("not" "no" (dont do\$not)) near6 (encrypt\$3) near5 (home near4 network near4 (identification identifier))))		US-PGPUB; USPAT; USOCR; FPRS; EPO, JPO; DERWENT; IBM_TDB	OR	ON	2019/06/29; 13:54
S86	8	((("not" "no" (dont do\$not)) with (encrypt\$3) with (home near4 network near4 (identification identifier))))		US-PGPUB; USPAT; USOCR;	OR	ON	2019/06/29; 13:54

file:///C:/Users/bho3/Documents/e-Red%20Folder/16200037/EASTSearchHistory.16200037_AccessibleVersion.htm[7/3/2019 11:48:11 AM]

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S87	8	S86 and (@ad<"20170725" @rlad<"20170725")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/06/29; 13:55
S88	8	S87 and (subscri\$5)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/06/29; 13:55
S89	8	S88 and (authentica\$)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/06/29; 13:55
S90	8	((("not" "no" (dont do\$not))) with (encrypt\$3) with (home near4 network near4 (identification identifier)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/06/29; 13:56
S91	8	S90 and (@ad<"20170725" @rlad<"20170725")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/06/29; 13:56
S92	8	S91 and (subscri\$5)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/06/29; 13:56
S93	8	S92	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/06/29; 13:56
S94	8	S93 and (authentica\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/06/29; 14:09
S95	2	("20190098502").PN.	US-PGPUB; USPAT; USOCR; DERWENT	OR	ON	2019/07/02; 11:50
S96	2	("20180054512").PN.	US-PGPUB; USPAT; USOCR; DERWENT	OR	ON	2019/07/02; 12:15
S97	2	("20190098502").PN.	US-PGPUB; USPAT; USOCR; DERWENT	OR	ON	2019/07/03; 09:50

S98	2	SUPI same SUCI same (subscription) same (identifier) same (encrypt\$3) same (decrypt\$3) same (authentication\$3) same (home network) same (server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/03; 10:04
S99	0	S98 and (@ad<"20170725" @rlad<"20170725")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/03; 10:04
S100	2	SUPI same SUCI same (subscription) same (identifier) same (encrypt\$3) same (decrypt\$3) same (authentication\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/03; 10:04
S101	3	SUPI same SUCI same (subscription) same (identifier) same (encrypt\$3) same (decrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/03; 10:05
S102	5	SUPI same SUCI same (subscription) same (identifier) same (encrypt\$3 decrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/03; 10:05
S103	0	S102 and (@ad<"20170725" @rlad<"20170725")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/03; 10:05
S104	5	SUPI same SUCI same (subscription) same (encrypt\$3 decrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/03; 10:06
S105	0	S104 and (@ad<"20170725" @rlad<"20170725")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/03; 10:07
S106	5	SUPI same SUCI same (subscription) same (encrypt\$3 decrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/03; 10:07
S107	17	SUPI same SUCI same (subscription)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/03; 10:07
S108	5	S107 and (@ad<"20170725" @rlad<"20170725")	US-PGPUB; USPAT; USOCR;	OR	ON	2019/07/03; 10:08

		FPRS; EPO; JPO; DERWENT; BM_TDB			
--	--	--	--	--	--

7/3/2019 11:48:06 AM
C:\Users\hho3\Documents\EAST\Workspaces\16200037.wsp

Electronic Acknowledgement Receipt

EFS ID:	35804597
Application Number:	16200037
International Application Number:	
Confirmation Number:	8611
Title of Invention:	SUBSCRIPTION CONCEALED IDENTIFIER
First Named Inventor/Applicant Name:	Vesa TORVINEN
Customer Number:	6449
Filer:	Brian S. Rosenbloom/Sabrina Mayfield
Filer Authorized By:	Brian S. Rosenbloom
Attorney Docket Number:	3602-1734US2
Receipt Date:	23-APR-2019
Filing Date:	26-NOV-2018
Time Stamp:	16:16:44
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	3602-1734US2_Reply.pdf	62800	no	11
			2a108377336a1d5f9f62cf921a967fc86ca339bd		

Warnings:

Lenovo Ex. 1009

Page 63

Information:	
Total Files Size (in bytes):	62800
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.	

Application No. : 16/200,037
First Named Inventor : Vesa TORVINEN
Filed : 11/26/2018

Art Unit : 2644
Examiner : Ho, Huy C.

Docket : 3602-1734US2
Customer No. : 6449
Confirmation No. : 8611

Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

REPLY TO NON-FINAL OFFICE ACTION

This Reply is in response to the Non-Final Office Action having a notification date of
March 28, 2019.

Amendments to the Claims begin on page 2 of this paper.

Remarks begin on page 7 of this paper.

Amendments to the Claims:

1. (Currently Amended) A method performed by an authentication server in a home network of a user equipment (UE) for obtaining a subscription permanent identifier (SUPI), wherein the SUPI is a globally unique identifier allocated to a subscriber and the SUPI comprises a home network identifier identifying a home network of the subscriber and a subscription identifier identifying a subscription within the home network, the method comprising:

the authentication server receiving a subscription concealed identifier (SUCI) generated by the UE, wherein the SUCI ~~which~~ comprises an encrypted part ~~in which at least a part of the SUPI is encrypted~~, and a clear-text part, ~~which comprises a home~~ and wherein a) the encrypted part of the SUCI generated by the UE comprises the subscription identifier identifying the subscription within the home network, but the encrypted part of the SUCI generated by the UE does not include the home network identifier and b) the clear-text part of the SUCI generated by the UE comprises i) the home network identifier ~~and~~, ii) an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the ~~SUPI~~ subscription identifier in the SUCI, and iii) a public key identifier for a public key of the home network, but the clear-text part of the SUCI generated by the UE does not comprise the subscription identifier;

the authentication server determining a de-concealing server to use to decrypt the encrypted part of the SUCI;

the authentication server sending the SUCI to the de-concealing server; and
after the authentication server sends the SUCI to the de-concealing server, the authentication server receiving the SUPI in response.

2. (Cancelled).

3. (Original) The method of claim 1, wherein the de-concealing server is one of a plurality of de-concealing servers, and the determining of the de-concealing server is based on information received from the UE.

4. (Cancelled).

5. (Original) The method of claim 1, further comprising receiving the SUCI from the UE as part of a registration procedure for registering the UE with a wireless communication network.

6. (Original) The method of claim 1, further comprising receiving the SUCI from the UE via an authentication request from a Security Anchor Function.

7. (Original) The method of claim 1, further comprising sending the SUCI and a request for an authentication vector for authenticating the UE to the determined de-concealing server in the same message.

8. (Currently Amended) The method of claim 1, wherein
the SUPI home network identifier comprises a Mobile Subscription Identification Number, MSIN, consists of a Mobile Country Code, MCC, and a Mobile Network Code, MNC, and where the MSIN is encrypted in the encrypted part of the SUCI, and the MCC and the MNC are the home network identifier in the clear text part of the SUCI, and
the subscription identifier is a Mobile Subscription Identification Number (MSIN).

9. (Original) The method of claim 1, wherein the SUPI is a Network Access Identifier.

10. (Currently Amended) The method of claim 1, wherein the encryption scheme is an Elliptic Curve Integrated Encryption Scheme (ECIES) ~~and the clear text part of the SUCI comprises an ephemeral public key of the UE for use in the ECIES.~~

11. (Currently Amended) A method, performed by a de-concealing server, for providing a subscription permanent identifier (SUPI) to an authentication server, wherein the SUPI is a globally unique identifier allocated to a subscriber and the SUPI comprises a home network identifier identifying a home network of the subscriber and a subscription identifier identifying a subscription within the home network, the method comprising:

the de-concealing server receiving, from the authentication server, a subscription concealed identifier (SUCI) ~~which comprises an encrypted part in which at least a part of the SUPI is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by a UE to encrypt the SUPI in the SUCI and which is supported by the de-concealing server generated by the UE,~~ wherein the SUCI comprises an encrypted part and a clear-text part, and wherein a) the encrypted part of the SUCI generated by the UE comprises the subscription identifier identifying the subscription within the home network, but the encrypted part of the SUCI generated by the UE does not include the home network identifier and b) the clear-text part of the SUCI generated by the UE comprises i) the home network identifier, ii) an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the subscription identifier in the SUCI, and iii) a public key identifier for a public key of the home network, but the clear-text part of the SUCI generated by the UE does not comprise the subscription identifier;

the de-concealing server decrypting the encrypted part of the SUCI, using the encryption scheme indicated by the encryption scheme identifier to obtain the SUPI; and

the de-concealing server sending the SUPI to the authentication server.

12. (Cancelled).

13. (Currently Amended) A method performed by a user equipment (UE) for concealing a subscription permanent identifier (SUPI), wherein the SUPI is a globally unique identifier allocated to a subscriber and the SUPI comprises a home network identifier identifying a home network of the subscriber and a subscription identifier identifying a subscription within the home network, the method comprising:

the UE generating a subscription concealed identifier (SUCI) which comprises ~~an encrypted part in which at least a part of a subscription permanent identifier (SUPI) is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI~~ an encrypted part and a clear-text part, wherein a) the encrypted part of the SUCI generated by the UE comprises the subscription identifier identifying the subscription within a home network, but

the encrypted part of the SUCI generated by the UE does not include the home network identifier and b) the clear-text part of the SUCI generated by the UE comprises i) the home network identifier, ii) an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the subscription identifier in the SUCI, and iii) a public key identifier for a public key of the home network, but the clear-text part of the SUCI generated by the UE does not comprise the subscription identifier; and

the UE transmitting the SUCI to an authentication server for forwarding of the SUCI to a de-concealing server capable of decrypting the ~~SUPI~~encrypted part.

14. (Original) The method of claim 13, wherein the SUCI is transmitted in a request to register with a wireless communication network (30).

15. (Original) The method of claim 13, wherein generating the SUCI comprises using a tamper resistant secure hardware component of the UE to generate the SUCI.

16. (Original) The method of claim 13, wherein transmitting the SUCI to the authentication server comprises transmitting the SUCI to the authentication server in response to an identifier request message received from an Authentication and Mobility management Function, AMF, as part of a procedure for registering the UE with a wireless communication network.

17. (Cancelled)

18. (Cancelled)

19. (Original) The method of claim 13, wherein the encryption scheme is an Elliptic Curve Integrated Encryption Scheme.

20. (Currently Amended) A user equipment (UE) for concealing a subscription permanent identifier (SUPI) , wherein the SUPI is a globally unique identifier allocated to a subscriber and

the SUPI comprises a home network identifier identifying a home network of the subscriber and a subscription identifier identifying a subscription within the home network, the UE comprising:

processing circuitry and memory circuitry, the memory circuitry containing instructions executable by the processing circuitry, wherein the UE is operative to:

generate a subscription concealed identifier (SUCI) which comprises an encrypted part in which at least a part of a Subscription Permanent Identifier (SUPI) is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI an encrypted part and a clear-text part, wherein a) the encrypted part of the SUCI generated by the UE comprises the subscription identifier identifying the subscription within a home network, but the encrypted part of the SUCI generated by the UE does not include the home network identifier and b) the clear-text part of the SUCI generated by the UE comprises i) the home network identifier, ii) an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the subscription identifier in the SUCI, and iii) a public key identifier for a public key of the home network, but the clear-text part of the SUCI generated by the UE does not comprise the subscription identifier; and

transmit the SUCI to an authentication server for forwarding of the SUCI to a de-concealing server capable of decrypting the SUPI.

21. (Cancelled)

22. (Original) The UE of claim 20, wherein the SUPI comprises a Mobile Subscription Identification Number.

23. (Original) The UE of claim 20, wherein the SUPI is a Network Access Identifier.

REMARKS

Claims 1, 3, 5-11, 13-16, 19, 20, 22, and 23 are pending in the application. Claims 1, 11, 13, and 20 are independent. Claims 2, 4, 12, 17, 18, and 21 are cancelled. No new matter has been added by the amendments. Applicant respectfully requests reconsideration.

I. Rejections of Claims Under 35 U.S.C. §102

Original claims 1-3, 5-9, 11-17, and 20-23 stand rejected under 35 U.S.C. §102 as allegedly being anticipated by Lee (US 20160094988). Applicant requests reconsideration.

A. Independent Claim 1

Claim 1 is not anticipated by Lee for at least the following three independent reasons.

i. First Reason Claim 1 is not Anticipated by Lee

Claim 1 is not anticipated by Lee for at least the reason that Lee does not disclose:

a subscription concealed identifier (SUCI) generated by [a] UE, wherein the SUCI comprises an encrypted part and a clear-text part, and wherein a) the encrypted part of the SUCI generated by the UE comprises the subscription identifier identifying [a] subscription within the home network, but the encrypted part of the SUCI generated by the UE does not include the home network identifier and b) the clear-text part of the SUCI generated by the UE comprises ... the home network identifier, ... but the clear-text part of the SUCI generated by the UE does not comprise the subscription identifier,

as required by claim 1, as amended.

Lee discloses a system in which a UE transmits to an MME a NAS Attach request that comprises: i) the UE's IMSI, ii) a serving network identifier (SN_id), and iii) a key (KEK).

According to Lee, "[i]f public key encryption is used, the IMSI, SN_id, and KEK may be encrypted ... [but if] shared key encryption is used, the SN_id and KEK may be encrypted"

(See Li at paragraph [0073]). Accordingly, Lee appears to disclose that the NAS message either

includes i) an encrypted IMSI or ii) an IMSI that is not encrypted (i.e., a clear-text IMSI).

Hence, because Lee discloses either encrypting the IMSI or not encrypting the IMSI, then, even if we accept that an IMSI is a form of SUPI because the IMSI includes a subscription identifier in the form of an MSIN and includes a home network identifier in the form of an MCC+MNC, Lee does not disclose that the UE generates a NAS message in which the MSIN portion of the IMSI (subscription identifier) is encrypted but the MCC+MNC portion of the IMSI (home network identifier) is not encrypted, as is required by claim 1 as amended.

That is, Lee discloses either: i) a NAS message transmitted by the UE in which both the MSIN portion of the IMSI and the MCC+MNC portion of the IMSI are encrypted or ii) a NAS message transmitted by the UE in which both the MSIN portion of the IMSI and the MCC+MNC portion of the IMSI are not encrypted. But nowhere does Lee disclose a UE transmitting any message in which the MSIN portion of the IMSI is encrypted, but the MCC+MNC portion of the IMSI (home network identifier) is not encrypted.

For at least this reason Lee does not anticipate claim 1.

ii. Second Reason Claim 1 is not Anticipated by Lee

Claim 1 is not anticipated by Lee for at least the further reason that Lee does not disclose:

the clear-text part of the SUCI generated by the UE comprises i) the home network identifier, ii) an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the subscription identifier in the SUCI, and iii) a public key identifier for a public key of the home network,

as required by claim 1, as amended.

This feature of claim 1 was originally presented in dependent claim 2, which is now cancelled. Accordingly, Applicant will address here the Office remarks for claim 2. In rejecting claim 2, the Office takes the position that the above highlighted feature is disclosed in paragraphs 8

and 9 of Lee. (See Office Action at page 5). Applicant disagrees.

Paragraph 8 of Lee discloses a UE transmitting a “first request” where the first request includes “a unique identifier of the UE and encrypted information.” Lee further discloses that the encrypted information “includes an identifier of the serving network and a randomly selected key encryption key (KEK).” Similarly, paragraph 9 of Lee discloses “information encrypted by the UE” wherein the information encrypted by the UE “includes a randomly selected KEK and a second serving network identifier.” But there is nothing in either paragraph 8 or 9 that discloses the request transmitted by UE includes a clear-text part (i.e., an unencrypted part) that includes “a public key identifier for a public key of the home network.” Accordingly, the rejection of claim 1 should be withdrawn for at least this further reason.

iii. Third Reason Claim 1 is not Anticipated by Lee

Claim 1 is not anticipated by Lee for at least the further reason that Lee does not disclose:

after the authentication server sends the SUCI to the de-concealing server, the authentication server receiving the SUPI in response,

as required by claim 1.

The Office contends that Lee discloses this feature and cites to Lee at paragraphs 94-99 and 104-110. (See Office Action at page 3). These paragraphs of Lee disclose the interaction between the MME 810 and the HSS 812 (see Figure 4 of Lee). The Examiner appears to contend that the MME 810 and the HSS 812 correspond to the claimed authentication server and de-concealing server, respectively. But, even if we assume for the sake of argument that the MME 810 and the HSS 812 correspond to the claimed authentication server and de-concealing server, respectively, Lee does not disclose that the MME receives any SUPI from the HSS.

Instead, Lee discloses that the HSS responds to the MME by sending to the MME an

encrypted key (i.e. KEK) encrypted using the MME's public key and an encrypted authentication vector that is encrypted using the key (KEK). (See Lee at paragraphs 96 and 110). Neither the key (KEK) nor the authentication vector, considered alone or in combination, corresponds to the claimed SUPI, which is a "globally unique identifier allocated to a subscriber and ... comprises a home network identifier identifying a home network of the subscriber and a subscription identifier identifying a subscription within the home network." Accordingly, for at least this further reason Lee does not anticipate claim 1.

B. Independent Claims 11, 13, and 20

Relevant remarks for claim 1 apply to claims 11, 13, and 20.

CONCLUSION

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding objections and rejections, and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance.

If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

If any fees are required, such as, but not limited to, any extension of time fee under 37 C.F.R. 1.17, Applicant hereby petitions for an extension of time, if necessary, and authorizes the Office to charge all required fees to deposit account number 02-2135.

RESPECTFULLY SUBMITTED,					
<i>NAME AND REG. #</i>	Brian Rosenbloom, Registration # 41,276				
<i>SIGNATURE</i>	/Brian Rosenbloom/			<i>DATE</i>	2019-04-23
<i>Address</i>	Rothwell, Figg, Ernst & Manbeck, P.C. Suite 800, 607 14 th Street, N.W. Washington, D.C. 20005				
<i>Email:</i>	brosenbloom@rfem.com	<i>Tel:</i>	202-626-3531	<i>Fax:</i>	202-783-6031

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875				Application or Docket Number 16/200,037		Filing Date 11/26/2018		☐ To be Mailed	
ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO									
APPLICATION AS FILED - PART I									
		(Column 1)	(Column 2)						
FOR		NUMBER FILED	NUMBER EXTRA		RATE (\$)		FEE (\$)		
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))		N/A	N/A		N/A				
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))		N/A	N/A		N/A				
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))		N/A	N/A		N/A				
TOTAL CLAIMS (37 CFR 1.16(i))		minus 20 = *		x \$100 =					
INDEPENDENT CLAIMS (37 CFR 1.16(h))		minus 3 = *		x \$460 =					
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))		If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).							
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))									
* If the difference in column 1 is less than zero, enter "0" in column 2.					TOTAL				
APPLICATION AS AMENDED - PART II									
		(Column 1)		(Column 2)	(Column 3)				
AMENDMENT	04/23/2019	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	* 17	Minus	** 23	= 0	x \$100 =		0	
	Independent (37 CFR 1.16(h))	* 4	Minus	*** 4	= 0	x \$460 =		0	
	☐ Application Size Fee (37 CFR 1.16(s))								
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
						TOTAL ADD'L FEE		0	
		(Column 1)		(Column 2)	(Column 3)				
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	*	Minus	**	=	x \$0 =			
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x \$0 =			
	☐ Application Size Fee (37 CFR 1.16(s))								
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
						TOTAL ADD'L FEE			
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.						LIE			
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".						/TRINA RIDDICK/			
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".									
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.									

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/200,037	11/26/2018	Vesa TORVINEN	3602-1734US2	8611
6449	7590	03/28/2019		
ROTHWELL, FIGG, ERNST & MANBECK, P.C. 607 14th Street, N.W. SUITE 800 WASHINGTON, DC 20005			EXAMINER HO, HUY C	
			ART UNIT	PAPER NUMBER
			2644	
			NOTIFICATION DATE	DELIVERY MODE
			03/28/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTO-PAT-Email@rfem.com

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Claim Rejections - 35 USC § 102

2. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(a)(2) the claimed invention was described in a patent issued under section 151, or in an application for patent published or deemed published under section 122(b), in which the patent or application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention.

4. *Claim(s) 1-3, 5-9, 11-17 and 20 is/are rejected under 35 U.S.C. 102(a)(2) as being anticipated by Lee et al. (Publication No. US 2016/0094988).*

Regarding claim 1, Lee teaches a method performed by an authentication server in a home network of a user equipment (UE) for obtaining a subscription permanent identifier (SUPI) (*Lee, the Abstract*), the method comprising:

receiving a subscription concealed identifier (SUCI) which comprises an encrypted part in which at least a part of the SUPI is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI (*Lee, pp [7]-[10]; Figures 12, 14 and 16, pp [94]-[98], or [104]-[110]*);

determining a de-concealing server to use to decrypt the encrypted part of the SUCI (*Lee, Figures 12, 14 and 16, pp [94]-[99], [104]-[110]*);

sending the SUCI to the de-concealing server (*Lee, Figures 12, 14 and 16, pp [94]-[98], or [104]-[110]*); and

receiving the SUPI in response (*Lee, Figures 12, 14 and 16, pp [94]-[98], or [104]-[110]*).

Regarding claim 11, Lee teaches a method, performed by a de-concealing server, for providing a subscription permanent identifier (SUPI) to an authentication server (*Lee, the Abstract*), the method comprising:

receiving, from the authentication server, a subscription concealed identifier (SUCI) which comprises an encrypted part in

which at least a part of the SUPI is encrypted, and a clear text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by a UE to encrypt the SUPI in the SUCI and which is supported by the de-concealing server (*Lee, pp [7]-[10]; Figures 12, 14 and 16, pp [94]-[98], or [104]-[110]*);

decrypting the encrypted part of the SUCI, using the encryption scheme indicated by the encryption scheme identifier to obtain the SUPI (*Lee, Figures 12, 14 and 16, pp [94]-[99], [104]-[110]*); and

sending the SUPI to the authentication server (*Lee, Figures 12, 14 and 16, pp [94]-[99], [104]-[110]*).

Regarding claim 13, Lee teaches a method performed by a user equipment (UE) (*Lee, the Abstract*), the method comprising:

generating a subscription concealed identifier (SUCI) which comprises an encrypted part in which at least a part of a subscription permanent identifier (SUPI) is encrypted, and a clear text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI (*Lee, pp [7]-[10]; Figures 12, 14 and 16, pp [94]-[98], or [104]-[110]*); and

transmitting the SUCI to an authentication server for forwarding of the SUCI to a de-concealing server capable of

decrypting the SUPI (*Lee, Figures 12, 14 and 16, pp [94]-[99], [104]-[110]*)).

Regarding claim 20, *Lee* teaches a user equipment (UE) (*Lee, the Abstract*), comprising:

processing circuitry and memory circuitry, the memory circuitry containing instructions executable by the processing circuitry (*Lee, Figure 4, pp [46]-[47]*), wherein the UE is operative to:

generate a subscription concealed identifier (SUCI) which comprises an encrypted part in which at least a part of a Subscription Permanent Identifier (SUPI) is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI (*Lee, pp [7]-[10]; Figures 12, 14 and 16, pp [94]-[98], or [104]-[110]*); and

transmit the SUCI to an authentication server for forwarding of the SUCI to a de-concealing server capable of decrypting the SUPI (*Lee, Figures 12, 14 and 16, pp [94]-[99], [104]-[110]*)).

Regarding claim 2, *Lee* teaches the method of claim 1, wherein the clear-text part of the SUCI comprises a public key identifier for a public key of the home network (*Lee, pp [8]-[9]*)).

Regarding claim 3, Lee teaches the method of claim 1, wherein the de-concealing server is one of a plurality of de-concealing servers, and the determining of the de-concealing server is based on information received from the UE (*Lee, Figures 7 and 8, pp [63]-[64]*).

Regarding claim 5, Lee teaches the method of claim 1, further comprising receiving the SUCI from the UE as part of a registration procedure for registering the UE with a wireless communication network (*Lee, Figures 12, 14 and 16, pp [104]-[110]*).

Regarding claim 6, Lee teaches the method of claim 1, further comprising receiving the SUCI from the UE via an authentication request from a Security Anchor Function (*Lee, pp [59]-[61]*).

Regarding claim 7, Lee teaches the method of claim 1, further comprising sending the SUCI and a request for an authentication vector for authenticating the UE to the determined de-concealing server in the same message (*Lee, pp [8]-[10]*).

Regarding claim 8, Lee teaches the method of claim 1, wherein the SUPI comprises a Mobile Subscription Identification Number, MSIN, a Mobile Country Code, MCC, and a Mobile Network Code, MNC, and where the MSIN is encrypted in the encrypted part of the SUCI, and the MCC and the MNC are the home network

identifier in the clear-text part of the SUCI (*Lee, pp [73]-[75]*).

Regarding claim 9, Lee teaches the method of claim 1, wherein the SUPI is a Network Access Identifier (*Lee, pp [7]-[9]*).

Regarding claim 12, Lee teaches the method of claim 11, wherein the clear-text part of the SUCI also comprises a key identifier used for identifying a decryption key used for decrypting the SUPI (*Lee, pp [7]-[10], [104]-[110]*).

Regarding claim 14, Lee teaches the method of claim 13, wherein the SUCI is transmitted in a request to register with a wireless communication network (*Lee, pp [7]-[10]*).

Regarding claim 15, Lee teaches the method of claim 13, wherein generating the SUCI comprises using a tamper resistant secure hardware component of the UE to generate the SUCI (*Lee, pp [7]-[10]*).

Regarding claim 16, Lee teaches the method of claim 13, wherein transmitting the SUCI to the authentication server comprises transmitting the SUCI to the authentication server in response to an identifier request message received from an Authentication and Mobility management Function, AMF, as part of a procedure for registering the UE with a wireless communication network (*Lee, pp [7]-[10]*).

Regarding claim 17, Lee teaches the method of claim 13, wherein the clear-text part comprises a public key identifier for the home network (*Lee*, pp [7]-[10]).

Regarding claim 21, Lee teaches the UE of claim 20, wherein the clear-text part comprises a public key identifier for the home network (*Lee*, pp [7]-[10], [104]-[110]).

Regarding claim 22, Lee teaches the UE of claim 20, wherein the SUPI comprises a Mobile Subscription Identification Number (*Lee*, pp [73]-[75]).

Regarding claim 23, Lee teaches the UE of claim 20, wherein the SUPI is a Network Access Identifier (*Lee*, pp [7]-[9]).

Claim Rejections - 35 USC § 103

5. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

6. This application currently names joint inventors. In considering patentability of the claims the examiner presumes that the subject matter of the various claims was commonly owned as of the effective filing date of the claimed invention(s) absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and effective filing dates of each claim that was not commonly owned as of the effective filing date of the later invention in order for the examiner to

consider the applicability of 35 U.S.C. 102(b) (2) (C) for any potential 35 U.S.C. 102(a) (2) prior art against the later invention.

7. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 4 and 18 is/are rejected under 35 U.S.C. 103 as being unpatentable over Lee et al. (Publication No. US 2016/0094988) and further in view of Hsu et al. (Publication No. US 2014/0019751).

Regarding claim 4, Lee does not teach the method of claim 1, wherein the encryption scheme is a null-encryption scheme.

Hsu teaches "encryption scheme is a null-encryption scheme" (*Hsu, the Abstract, pp [13], [16]-[17]*).

Therefore, it would have been obvious to a person of ordinary skill in the art before the effective filing date of the claimed invention was made to modify Lee by incorporating Hsu's teachings of encrypting transmitting packets/data using null-encryption scheme to provide security in protecting information transmitted over the wireless network.

Regarding claim 18, Lee does not teach the method of claim 13, wherein the encryption scheme is a null-encryption scheme.

Hsu teaches "encryption scheme is a null-encryption scheme" (*Hsu, the Abstract, pp [13], [16]-[17]*).

Therefore, it would have been obvious to a person of ordinary skill in the art before the effective filing date of the claimed invention was made to modify Lee by incorporating Hsu's teachings of encrypting transmitting packets/data using null-encryption scheme to provide security in protecting information transmitted over the wireless network.

9. Claims 10 and 19 is/are rejected under 35 U.S.C. 103 as being unpatentable over Lee et al. (Publication No. US 2016/0094988) and further in view of Liu et al. (Patent No. US 9,338,164).

Regarding claim 10, Lee does not teach the method of claim 1, wherein the encryption scheme is an Elliptic Curve Integrated Encryption Scheme (ECIES) and the clear-text part of the SUCI comprises an ephemeral public key of the UE for use in the ECIES.

Liu teaches "encryption scheme is an Elliptic Curve Integrated Encryption Scheme (ECIES) and the clear-text part of the SUCI comprises an ephemeral public key of the UE for use in the ECIES" (*Liu, Col. 6 Lines 30-40*).

Therefore, it would have been obvious to a person of ordinary skill in the art before the effective filing date of the claimed invention was made to modify Lee by incorporating Liu's teachings two-way authentication method using elliptic curve cryptography (ECC) algorithms to encrypt communications between mobile devices and an authentication server to provide the secure communication channel.

Regarding claim 19, Lee does not teach the method of claim 13, wherein the encryption scheme is an Elliptic Curve Integrated Encryption Scheme.

Liu teaches "encryption scheme is an Elliptic Curve Integrated Encryption Scheme (ECIES) and the clear-text part of the SUCI comprises an ephemeral public key of the UE for use in the ECIES" (*Liu, Col. 6 Lines 30-40*).

Therefore, it would have been obvious to a person of ordinary skill in the art before the effective filing date of the claimed invention was made to modify Lee by incorporating Liu's teachings two-way authentication method using elliptic curve cryptography (ECC) algorithms to encrypt communications between mobile devices and an authentication server to provide the secure communication channel.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HUY C HO whose telephone number is (571)270-1108. The examiner can normally be reached on M-F 8AM-5PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, KATHY WANG-HURST can be reached on (571)270-5371. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

Art Unit: 2644

like assistance from a USPTO Customer Service Representative or
access to the automated information system, call 800-786-9199
(IN USA OR CANADA) or 571-272-1000.

/HUY C HO/

Primary Examiner, Art Unit 2644

Notice of References Cited	Application/Control No. 16/200,037		Applicant(s)/Patent Under Reexamination TORVINEN et al.	
	Examiner HUY C HO		Art Unit 2644	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20160094988-A1	03-2016	Lee; Soo Bum	H04L9/0825	380/270
*	B	US-9338164-B1	05-2016	Liu; Quentin	H04L63/0869	1/1
*	C	US-20140019751-A1	01-2014	Hsu; Raymond Tah-Sheng	H04L63/0428	713/153
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

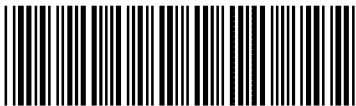
FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

<i>Search Notes</i> 	Application/Control No. 16/200,037	Applicant(s)/Patent Under Reexamination TORVINEN et al.
	Examiner HUY C HO	Art Unit 2644

CPC - Searched*		
Symbol	Date	Examiner
H04W12/00; H04W12/001; H04W12/02; H04W12/04; H04W12/06; H04W12/0602; H04W12/0605; H04W8/18; H04W60/00; H04L63/0414; H04L63/0428	03/07/2019	HH

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
455	411	03/07/2019	HH

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
EAST Database Search	03/07/2019	HH
Inventor Search	03/07/2019	HH

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
455	410	03/07/2019	HH
380	277-282; 283-285	03/07/2019	HH

/HUY C HO/ Primary Examiner, Art Unit 2644	
---	--

Doc code: IDS

PTO/SB/08a (02-18)

Doc description: Information Disclosure Statement (IDS) Filed

Approved for use through 11/30/2020. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		16200037	
	Filing Date		2018-11-26	
	First Named Inventor	Vesa TORVINEN		
	Art Unit	2491		
	Examiner Name			
	Attorney Docket Number	3602-1734US2		

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20130003971	A1	2013-01-03	FORSBERG et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²ⁱ	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2016/209126	WO	A1	2016-12-29	TELEFONAKTIEBOLAG ET LM ERICSSON		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16200037
Filing Date	2018-11-26
First Named Inventor	Vesa TORVINEN
Art Unit	2491
Examiner Name	
Attorney Docket Number	3602-1734US2

1	International Search Report and Written Opinion dated November 7, 2018 issued in International Application No. PCT/EP2018/069432. (16 pages)	☐
2	Ericsson, "Clause 6.12.5 (NF discovery with SUCI)", 3GPP TSG SA WG3 (Security) Meeting #90bis; S-180824; (February 26-March 2, 2018); San Diego. (2 pages)	☐
3	Nokia, "UDM and SIDF discovery", 3GPP TSG SA WG3 (Security) Meeting #90Bis; S3-180767; (February 26-March 2, 2018); San Diego. (2 pages)	☐
4	3GPP TS 33.501 V0.2.0 (2017-05); 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Architecture and Procedures for 5G System (Release 15). (25 pages)	☐
5	3GPP TR 33.899 V1.2.0 (2017-06); 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on the security aspects of the next generation system (Release 14). (586 pages)	☐
6	AHOLA, K. et al., "5G Enablers for Network and System Security and Resilience", 5G-ENSURE, Deliverable D3.6; 5G-PPP security enablers open specifications (v2.0), (January 5, 2017). (294 pages)	☐
7	3GPP TS 23.003 V15.0.0 (2017-06); 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Numbering, addressing and identification (Release 15). (108 pages)	☐
8	3GPP TS 23.501 V1.0.0 (2017-06); 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System Architecture for the 5G System; Stage 2 (Release 15). (146 pages)	☐
9	3GPP TS 33.220 V15.0.0 (2017-06); 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (Release 15). (93 pages)	☐
10	ABOBA, B. et al., "The Network Access Identifier", Network Working Group; Request for Comments: 4282 (December 2005). (16 pages)	☐
11	SIMON, D. et al., "The EAP-TLS Authentication Protocol", Network Working Group; Request for Comments: 5216 (March 2008). (34 pages)	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16200037
Filing Date	2018-11-26
First Named Inventor	Vesa TORVINEN
Art Unit	2491
Examiner Name	
Attorney Docket Number	3602-1734US2

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/HUY C HO/	Date Considered	03/07/2019
--------------------	------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	16200037
Filing Date	2018-11-26
First Named Inventor	Vesa TORVINEN
Art Unit	2491
Examiner Name	
Attorney Docket Number	3602-1734US2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Brian S. Rosenbloom/	Date (YYYY-MM-DD)	2018-12-06
Name/Print	Brian S. Rosenbloom	Registration Number	41276

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Bibliographic Data

Application No: 16/200,037

Foreign Priority claimed: ☐ Yes ☒ No

35 USC 119 (a-d) conditions met: ☐ Yes ☒ No ☐ Met After Allowance

Verified and Acknowledged:

/HUY C HO/

HH

Examiner's Signature

Initials

Title:

SUBSCRIPTION CONCEALED IDENTIFIER

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/26/2018	455	2644	3602-1734US2
RULE			

APPLICANTS

Telefonaktiebolaget LM Ericsson (publ), Stockholm, SWEDEN

INVENTORS

Vesa TORVINEN Sauvo, FINLAND

Noamen BEN HENDA Stockholm, SWEDEN

David CASTELLANOS ZAMORA Madrid, SPAIN

Prajwol Kumar NAKARMI Sollentuna, SWEDEN

Pasi SAARINEN Jarfalla, SWEDEN

Monica WIFVESSON Lund, SWEDEN

CONTINUING DATA

This application is a CON of PCT/EP2018/069432 07/17/2018

PCT/EP2018/069432 has PRO of 62536632 07/25/2017

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

12/14/2018

STATE OR COUNTRY

FINLAND

ADDRESS

ROTHWELL, FIGG, ERNST & MANBECK, P.C.

607 14th Street, N.W.

SUITE 800

WASHINGTON, DC 20005

UNITED STATES

FILING FEE RECEIVED

\$6,620

EAST Search History
EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	5	"20140019751"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/25; 11:19
L2	8	"9,338,164"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/25; 11:46
L3	2	"20180285602"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/25; 12:23
L4	52	(20030046541 7188360 20190054899)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/25; 12:24
S1	1	("20130003971").PN.	US-PGPUB; USPAT	OR	ON	2019/03/07; 14:41
S2	134	((("TORVINEN") near3 ("Vesa")) OR (("BEN") near3 ("HENDA") near3 ("Noamen")) OR (("CASTELLANOS") near3 ("ZAMORA") near3 ("David")) OR (("NAKARMI") near3 ("Prajwol")) OR (("SAARINEN") near3 ("Pasi")) OR (("WIFVESSON") near3 ("Monica"))).INV.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	ON	2019/03/07; 15:29
S3	223000	(455/410-411 380/277-282 380/283-285 H04W12/00 H04W12/001 H04W12/02 H04W12/04 H04W12/06 H04W12/0602 H04W12/0605 H04W8/18 H04W60/00 H04L63/0414 H04L63/0428).ccls,cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/07; 18:47
S4	218974	S3 and (@ad<"20170725" @riad<"20170725")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/07; 18:50
S5	90862	S4 and (authenticat\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/07; 18:52
S6	56433	S5 and {server}	US-PGPUB; USPAT;	OR	ON	2019/03/07; 18:52

			USOCR; FPRS; EPO; JPO; DERWENT; ISM_TDS			
S7	0	S6 and (SUCI)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; ISM_TDS	OR	ON	2019/03/07 18:52
S8	6289	S6 and ((encrypt\$3 cipher\$3 encode encoding) near4 (identifier identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; ISM_TDS	OR	ON	2019/03/07 18:54
S9	41	S8 and (conceal\$3 near4 (id identifier identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; ISM_TDS	OR	ON	2019/03/07 18:55
S10	13	S9 and ((decrypt\$3 decoding decode decipher\$3 de\$conceal\$3 reveal\$3) near4 (id identifier identifier))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; ISM_TDS	OR	ON	2019/03/07 18:56
S11	4	S10 and (home near4 network near4 (id identifier identifier))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; ISM_TDS	OR	ON	2019/03/07 18:58
S12	17	("20020004898" "20050289643" "20060235796" "20070107047" "20080123850" "20080260149" "6260147" "6785823" "7042988").PN. OR ("7594113").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2019/03/07 19:28
S13	15	("20020004898" "20050289643" "20060235796" "20070107047" "20080123850" "20080260149" "6260147" "6785823" "6904466" "6911974" "7042988" "7088822" "7224804" "7594113").PN. OR ("7945777").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2019/03/07 19:35
S14	142	("6175743" "6175922").PN. OR ("6260147").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2019/03/07 19:41
S15	2	(SUPI (subscription near4 permanent near4 identifier)) same (encrypt\$3 decrypt\$3) same (SUCI (subscription near4 concealed near4 identifier)) same (server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; ISM_TDS	OR	ON	2019/03/11 17:49
S16	0	S15 and (@ad<"20170725" @rlad<"20170725")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; ISM_TDS	OR	ON	2019/03/11 17:49
S17	5	(SUPI (subscription near4 permanent near4 identifier)) same (encrypt\$3 decrypt\$3) same (SUCI (subscription near4 concealed near4 identifier))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; ISM_TDS	OR	ON	2019/03/11 17:49
S18	0	S17 and (@ad<"20170725" @rlad<"20170725")	US-PGPUB; USPAT;	OR	ON	2019/03/11 17:49

				USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S19	16	(SUPI (subscription near4 permanent near4 identifier)) same (encrypt\$3 decrypt\$3)		US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 17:50
S20	9	S19 and (@ad<"20170725" @rled<"20170725")		US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 17:50
S21	9	S20 and (server)		US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 17:50
S22	9	S21 and ((conceal\$3 hidden encrypt\$3) near4 (id identifier identification))		US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 17:51
S23	0	(subscription near4 permanent near4 identifier) same (encrypt\$3 decrypt\$3) same (subscription near4 concealed near4 identifier)		US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 18:11
S24	230665	(455/410-411 455/435.1-435.3 380/277-282 380/283-285 H04W12/00 H04W12/001 H04W12/02 H04W12/04 H04W12/06 H04W12/0602 H04W12/0605 H04W8/18 H04W60/00 H04L63/0414 H04L63/0428).cdts,cpc.		US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 18:36
S25	226507	S24 and (@ad<"20170725" @rled<"20170725")		US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 18:37
S26	26623	S25 and (authentical\$3 near4 server)		US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 18:38
S27	9822	S26 and (subscriber)		US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/11; 18:39
S28	312	S27 and (home near4 network near4 (id identifier identification))		US-PGPUB; USPAT; USOCR; FPRS;	OR	ON	2019/03/11; 18:40

			EPO; JPO; DERWENT; IBM_TDS			
S29	189	S28 and (encrypt\$3 decrypt\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDS	OR	ON	2019/03/11; 18:40
S30	96	S29 and (scheme)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDS	OR	ON	2019/03/11; 18:41
S31	4	S29 and ((conceal\$3 near4 (identifier id identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDS	OR	ON	2019/03/11; 18:41
S32	79	S29 and ((private public) near5 (key identifier identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDS	OR	ON	2019/03/11; 18:43
S33	43	S32 and ((encrypt\$3 encod\$3) near4 (id identifier identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDS	OR	ON	2019/03/11; 18:52
S34	15	S33 and ((decrypt\$3 decod\$3) near4 (id identifier identification))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDS	OR	ON	2019/03/11; 18:54
S35	2508	(elliptic near4 curve near5 encryption)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDS	OR	ON	2019/03/13; 13:29
S36	573	(elliptic near4 curve near5 encryption near5 scheme)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDS	OR	ON	2019/03/13; 13:29
S37	0	(elliptic near4 curve near5 encryption near5 integrate near5 scheme)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDS	OR	ON	2019/03/13; 13:29
S38	266	(elliptic near4 curve near5 encryption near5 integrated near5 scheme)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2019/03/13; 13:30

EAST Search History

S39	262	S38 and (@ad<"20170725" @iad<"20170725")	IBM_TDB	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 13:30
S40	50	S39 and ((conceal\$3 encrypt\$3) near4 (id identifier identification))	IBM_TDB	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 13:30
S41	0	S39 and ((conceal\$3) near4 (id identifier identification))	IBM_TDB	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 13:30
S42	60	S39 and ((conceal\$3 encrypt\$3) near4 (subscription id identifier identification))	IBM_TDB	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 13:31
S43	0	S42 and (home near4 network near5 (identifier identification))	IBM_TDB	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 13:32
S44	11	S42 and (home near4 network)	IBM_TDB	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 13:32
S45	11	S44 and (server)	IBM_TDB	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 13:32
S46	11	S45 and (public private)	IBM_TDB	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 13:33
S47	0	S46 and (anchor)	IBM_TDB	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 13:33
S48	11	S46 and (security)	IBM_TDB	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 13:33
S49	266	(elliptic near4 curve near5 encryption near5 integrated near5 scheme)	IBM_TDB	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 13:33

file:///C:/Users/bho3/Documents/e-Red%20Folder/16200037/EASTSearchHistory.16200037_AccessibleVersion.htm[3/25/2019 12:31:27 PM]

			USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDS			16:16
S50	262	S49 and (@ad<"20170725" @rld<"20170725")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDS	OR	ON	2019/03/13; 16:16
S51	262	S50	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDS	OR	ON	2019/03/13; 16:16
S52	0	S51 and (null\$encryption near3 scheme)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDS	OR	ON	2019/03/13; 16:39
S53	0	S51 and (null\$encryption)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDS	OR	ON	2019/03/13; 16:49
S54	45	(null\$encryption)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDS	OR	ON	2019/03/13; 16:49
S55	3	(null\$encryption near3 scheme)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDS	OR	ON	2019/03/13; 16:49
S56	3	S55 and (@ad<"20170725" @rld<"20170725")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDS	OR	ON	2019/03/13; 16:49
S57	1	S56 and (authentica\$3 near4 server)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDS	OR	ON	2019/03/13; 16:49
S58	5	((null\$encryption (null near2 encryption)) near3 scheme)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDS	OR	ON	2019/03/13; 16:52
S59	0	S58 and (elliptic near4 curve near5 encryption near5 integrated near5 scheme)	US-PGPUB; USPAT; USOCR;	OR	ON	2019/03/13; 16:52

				FPRS; EPO; JPO; DERWENT; IBM_TDB			
S60	5	S68 and (@ad<"20170725" @rld<"20170725")		US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 17:06
S61	0	S60 and (elliptic near4 curve near5 encryption)		US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 17:10
S62	0	S60 and ((elliptic curve) near5 encryption)		US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 17:10
S63	1	S60 and (authentica\$3 near4 server)		US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 17:11
S64	3	S60 and (authentica\$3 server)		US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 17:11
S65	214	((null\$encryption (null near2 encryption)) near3 (algorithm scheme))		US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 17:14
S66	2	S65 and (elliptic near4 curve near5 encryption near5 integrated near5 scheme)		US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 17:14
S67	2	S66 and (@ad<"20170725" @rld<"20170725")		US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 17:14
S68	214	S65 and (@ad<"20170725" @rld<"20170725")		US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/03/13; 17:22
S69	96	S68 and (authentica\$3 near4 server)		US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2019/03/13; 17:22

EAST Search History

S70	1	S69 and (SUP1 (subcription near4 permanent near4 identifier))	DERWENT: IBM.TDB	FOR	ON	2019/03/13 17:22
			US-PGPUB: USPAT: USOCR: FPRS: EPO; JPO: DERWENT: IBM.TDB			

3/ 25/ 2019 12:31:24 PM
C:\Users\hho3\Documents\EAST\Workspaces\16200037.wsp



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/200,037	11/26/2018	Vesa TORVINEN	3602-1734US2

CONFIRMATION NO. 8611

PUBLICATION NOTICE



OC000000106953014

6449
ROTHWELL, FIGG, ERNST & MANBECK, P.C.
607 14th Street, N.W.
SUITE 800
WASHINGTON, DC 20005

Title:SUBSCRIPTION CONCEALED IDENTIFIER

Publication No.US-2019-0098502-A1

Publication Date:03/28/2019

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <https://portal.uspto.gov/pair/PublicPair>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/200,037	11/26/2018	Vesa TORVINEN	3602-1734US2	8611

6449 7590 02/22/2019
ROTHWELL, FIGG, ERNST & MANBECK, P.C.
607 14th Street, N.W.
SUITE 800
WASHINGTON, DC 20005

EXAMINER

ART UNIT	PAPER NUMBER
2642	

NOTIFICATION DATE	DELIVERY MODE
02/22/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTO-PAT-Email@rfem.com

<i>Decision Granting Request for Prioritized Examination (Track I)</i>	Application No. 16/200,037	Applicant(s) TORVINEN et al.	
	Examiner Liana Walsh	Art Unit OPET	AIA (First Inventor to File) Status Yes
1. THE REQUEST FILED <u>26 November 2018</u> IS GRANTED . The above-identified application has met the requirements for prioritized examination A. ☒ for an original nonprovisional application (Track I). B. ☐ for an application undergoing continued examination (RCE). 2. The above-identified application will undergo prioritized examination. The application will be accorded special status throughout its entire course of prosecution until one of the following occurs: A. filing a <u>petition for extension of time</u> to extend the time period for filing a reply; B. filing an <u>amendment to amend the application to contain more than four independent claims, more than thirty total claims</u>, or a multiple dependent claim; C. filing a <u>request for continued examination</u> ; D. filing a notice of appeal; E. filing a request for suspension of action; F. mailing of a notice of allowance; G. mailing of a final Office action; H. completion of examination as defined in 37 CFR 41.102; or I. abandonment of the application. Telephone inquiries with regard to this decision should be directed to Liana Walsh at (571)272-3206. In his/her absence, calls may be directed to Petition Help Desk at (571) 272-3282.			
/LIANA S WALSH/ Lead Paralegal Specialist, OPET			

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 16/200,037				
APPLICATION AS FILED - PART I										
(Column 1)		(Column 2)		SMALL ENTITY		OTHER THAN SMALL ENTITY				
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)			
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	300			
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	660			
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	760			
TOTAL CLAIMS (37 CFR 1.16(j))	23 minus 20 =	*			OR	x 100 =	300			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	4 minus 3 =	*				x 460 =	460			
APPLICATION SIZE FEE (37 CFR 1.16(s))		If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).					0.00			
							0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00			
				TOTAL		TOTAL	2480			
* If the difference in column 1 is less than zero, enter "0" in column 2.										
APPLICATION AS AMENDED - PART II										
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OTHER THAN SMALL ENTITY		
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)	RATE(\$)	ADDITIONAL FEE(\$)	
	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)	RATE(\$)	ADDITIONAL FEE(\$)	
	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.										



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/200,037	11/26/2018	Vesa TORVINEN	3602-1734US2

CONFIRMATION NO. 8611

INFORMAL NOTICE



6449
ROTHWELL, FIGG, ERNST & MANBECK, P.C.
607 14th Street, N.W.
SUITE 800
WASHINGTON, DC 20005

Date Mailed: 02/15/2019

INFORMATIONAL NOTICE TO APPLICANT

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

The item(s) indicated below are also required and should be submitted with any reply to this notice to avoid further processing delays.

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):
Vesa TORVINEN
Noamen BEN HENDA
David CASTELLANOS ZAMORA
Prajwol Kumar NAKARM
Pasi SAARINEN
Monica WIFVESSON

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/nton/



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
16/200,037	11/26/2018	2642	2640	3602-1734US2	23	4

CONFIRMATION NO. 8611
UPDATED FILING RECEIPT

6449
ROTHWELL, FIGG, ERNST & MANBECK, P.C.
607 14th Street, N.W.
SUITE 800
WASHINGTON, DC 20005



Date Mailed: 02/15/2019

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Vesa TORVINEN, Sauvo, FINLAND;
Noamen BEN HENDA, Stockholm, SWEDEN;
David CASTELLANOS ZAMORA, Madrid, SPAIN;
Prajwol Kumar NAKARMI, Sollentuna, SWEDEN;
Pasi SAARINEN, Jarfalla, SWEDEN;
Monica WIFVESSON, Lund, SWEDEN;

Applicant(s)

Telefonaktiebolaget LM Ericsson (publ), Stockholm, SWEDEN;

Assignment For Published Patent Application

Telefonaktiebolaget LM Ericsson (publ), Stockholm, SWEDEN

Power of Attorney: The patent practitioners associated with Customer Number 06449

Domestic Priority data as claimed by applicant

This application is a CON of PCT/EP2018/069432 07/17/2018
which claims benefit of 62/536,632 07/25/2017

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 12/14/2018

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 16/200,037**

Projected Publication Date: 03/28/2019

Non-Publication Request: No

Early Publication Request: No
Title

SUBSCRIPTION CONCEALED IDENTIFIER

Preliminary Class

455

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No. : 16/200037
First Named Inventor : Vesa TORVINEN
Filed : November 26, 2018
TC/A.U. : 2642
Examiner :
Docket No. : 3602-1734US2
Customer No. : 6449
Confirmation No. : 8611

RESPONSE TO NOTICE TO FILE MISSING PARTS

Mail Stop: Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

In response to the Notice to File Missing Parts mailed December 18, 2018, Applicant submits the following, which Applicant believes will satisfy the requirements specified in the Notice.

- Undiscounted Filing Fees Total: **\$160**
 - **\$160** Surcharge

Please charge the required fees in connection with this submission to Deposit Account No. 02-2135.

Respectfully submitted,

Date: February 12, 2019

By 

Brian S. Rosenbloom
Attorney for Applicants
Registration No. 41,276
ROTHWELL, FIGG, ERNST & MANBECK, p.c.
Suite 800, 607 14th Street, N.W.
Washington, D.C. 20005
Telephone: (202)783-6040
brosenbloom@rfem.com

Electronic Patent Application Fee Transmittal

Application Number:	16200037			
Filing Date:	26-Nov-2018			
Title of Invention:	SUBSCRIPTION CONCEALED IDENTIFIER			
First Named Inventor/Applicant Name:	Vesa TORVINEN			
Filer:	Brian S. Rosenbloom/Xania Steele			
Attorney Docket Number:	3602-1734US2			
Filed as Large Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
LATE FILING FEE FOR OATH OR DECLARATION	1051	1	160	160
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				160

Electronic Acknowledgement Receipt

EFS ID:	35124938
Application Number:	16200037
International Application Number:	
Confirmation Number:	8611
Title of Invention:	SUBSCRIPTION CONCEALED IDENTIFIER
First Named Inventor/Applicant Name:	Vesa TORVINEN
Customer Number:	6449
Filer:	Brian S. Rosenbloom/Xania Steele
Filer Authorized By:	Brian S. Rosenbloom
Attorney Docket Number:	3602-1734US2
Receipt Date:	12-FEB-2019
Filing Date:	26-NOV-2018
Time Stamp:	17:23:25
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	\$ 160
RAM confirmation Number	021319INTEFSW00003852022135
Deposit Account	022135
Authorized User	Xania Steele

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.21 (Miscellaneous fees and charges)

Lenovo Ex. 1009

Page 121

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Applicant Response to Pre-Exam Formalities Notice	3602-1734US2_Response-NOMP.pdf	45765	no	1
			5ab4c2612b33e0b1fe2ccb6b9d75b1f17b9b8099		
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30332	no	2
			4b45c9d5939145cefdc5a128f3ab15e360a68036		
Warnings:					
Information:					
Total Files Size (in bytes):			76097		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/200,037	11/26/2018	Vesa TORVINEN	3602-1734US2

CONFIRMATION NO. 8611

FORMALITIES LETTER



OC000000104485176

6449
ROTHWELL, FIGG, ERNST & MANBECK, P.C.
607 14th Street, N.W.
SUITE 800
WASHINGTON, DC 20005

Date Mailed: 12/18/2018

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing.

Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- Surcharge as set forth in 37 CFR 1.16(f) must be submitted.

The surcharge is due for any one of:

- late submission of the basic filing fee, search fee, or examination fee,
- late submission of inventor's oath or declaration,
- filing an application that does not contain at least one claim on filing, or
- submission of an application filed by reference to a previously filed application.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of this Notice to avoid abandonment is/are itemized below. No entity status discount is in effect. If applicant is qualified for small entity status, a written assertion of small entity status must be submitted to establish small entity status. (See 37 CFR 1.27). If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- \$ **160** surcharge.
- \$(**0**) previous unapplied payment amount.
- \$ **160** TOTAL FEE BALANCE DUE.

Items Required To Avoid Processing Delays:

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):

Vesa TORVINEN
Noamen BEN HENDA
David CASTELLANOS ZAMORA
Prajwol Kumar NAKARMI
Pasi SAARINEN
Monica WIFVESSON

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice".
<https://portal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html>

For more information about EFS-Web please call the USPTO Electronic Business Center at 1-866-217-9197 or visit our website at <http://www.uspto.gov/ebc>.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/lvongxay/

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 16/200,037				
APPLICATION AS FILED - PART I										
(Column 1)		(Column 2)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY				
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)			
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	300			
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	660			
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	760			
TOTAL CLAIMS (37 CFR 1.16(j))	23	minus 20 = * 3				x 100 =	300			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	4	minus 3 = * 1				x 460 =	460			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL		TOTAL	2480			
APPLICATION AS AMENDED - PART II										
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY		
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=		x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=		x	=
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE			TOTAL ADD'L FEE	
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=		x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=		x	=
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE			TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.										



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
16/200,037	11/26/2018	2491	2480	3602-1734US2	23	4

CONFIRMATION NO. 8611

FILING RECEIPT

6449

ROTHWELL, FIGG, ERNST & MANBECK, P.C.
607 14th Street, N.W.
SUITE 800
WASHINGTON, DC 20005



Date Mailed: 12/18/2018

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Vesa TORVINEN, Sauvo, FINLAND;
Noamen BEN HENDA, Stockholm, SWEDEN;
David CASTELLANOS ZAMORA, Madrid, SPAIN;
Prajwol Kumar NAKARMI, Sollentuna, SWEDEN;
Pasi SAARINEN, Jarfalla, SWEDEN;
Monica WIFVESSON, Lund, SWEDEN;

Applicant(s)

Telefonaktiebolaget LM Ericsson (publ), Stockholm, SWEDEN;

Assignment For Published Patent Application

Telefonaktiebolaget LM Ericsson (publ), Stockholm, SWEDEN

Power of Attorney: The patent practitioners associated with Customer Number 06449

Domestic Priority data as claimed by applicant

This application is a CON of PCT/EP2018/069432 07/17/2018
which claims benefit of 62/536,632 07/25/2017

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 12/14/2018

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 16/200,037**

Projected Publication Date: 03/28/2019

Non-Publication Request: No

Early Publication Request: No
Title

SUBSCRIPTION CONCEALED IDENTIFIER

Preliminary Class

713

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		16200037
	Filing Date		2018-11-26
	First Named Inventor	Vesa TORVINEN	
	Art Unit	2491	
	Examiner Name		
	Attorney Docket Number	3602-1734US2	

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20130003971	A1	2013-01-03	FORSBERG et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS								
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2016/209126	WO	A1	2016-12-29	TELEFONAKTIEBOLAG ET LM ERICSSON		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16200037
Filing Date	2018-11-26
First Named Inventor	Vesa TORVINEN
Art Unit	2491
Examiner Name	
Attorney Docket Number	3602-1734US2

1	International Search Report and Written Opinion dated November 7, 2018 issued in International Application No. PCT/EP2018/069432. (16 pages)	☐
2	Ericsson, "Clause 6.12.5 (NF discovery with SUCI)", 3GPP TSG SA WG3 (Security) Meeting #90bis; S-180824; (February 26-March 2, 2018); San Diego. (2 pages)	☐
3	Nokia, "UDM and SIDF discovery", 3GPP TSG SA WG3 (Security) Meeting #90Bis; S3-180767; (February 26-March 2, 2018); San Diego. (2 pages)	☐
4	3GPP TS 33.501 V0.2.0 (2017-05); 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Architecture and Procedures for 5G System (Release 15). (25 pages)	☐
5	3GPP TR 33.899 V1.2.0 (2017-06); 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on the security aspects of the next generation system (Release 14). (586 pages)	☐
6	AHOLA, K. et al., "5G Enablers for Network and System Security and Resilience", 5G-ENSURE, Deliverable D3.6; 5G-PPP security enablers open specifications (v2.0), (January 5, 2017). (294 pages)	☐
7	3GPP TS 23.003 V15.0.0 (2017-06); 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Numbering, addressing and identification (Release 15). (108 pages)	☐
8	3GPP TS 23.501 V1.0.0 (2017-06); 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System Architecture for the 5G System; Stage 2 (Release 15). (146 pages)	☐
9	3GPP TS 33.220 V15.0.0 (2017-06); 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (Release 15). (93 pages)	☐
10	ABOBA, B. et al., "The Network Access Identifier", Network Working Group; Request for Comments: 4282 (December 2005). (16 pages)	☐
11	SIMON, D. et al., "The EAP-TLS Authentication Protocol", Network Working Group; Request for Comments: 5216 (March 2008). (34 pages)	☐

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16200037
Filing Date	2018-11-26
First Named Inventor	Vesa TORVINEN
Art Unit	2491
Examiner Name	
Attorney Docket Number	3602-1734US2

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16200037
Filing Date	2018-11-26
First Named Inventor	Vesa TORVINEN
Art Unit	2491
Examiner Name	
Attorney Docket Number	3602-1734US2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Brian S. Rosenbloom/	Date (YYYY-MM-DD)	2018-12-06
Name/Print	Brian S. Rosenbloom	Registration Number	41276

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



(51) International Patent Classification:

H04W 12/02 (2009.01) H04W 8/26 (2009.01)
H04L 9/32 (2006.01) H04W 12/06 (2009.01)

(21) International Application Number:

PCT/SE2015/050728

(22) International Filing Date:

23 June 2015 (23.06.2015)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventors: NORRMAN, Karl; Sweden, Stigbergsgatan 32A, S-116 28 Stockholm (SE). NÄSLUND, Mats; Stopvägen 95, S-168 36 Bromma (SE). MATSSON, John; Garngård 5B, S-187 77 Täby (SE). CHENG, Yi; Högalidsvägen 9, S-172 37 Sundbyberg (SE).

(74) Agent: EGRELIUS, Fredrik; Ericsson AB, Patent Unit Kista DSM, S-16480 Stockholm (SE).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: METHODS, NETWORK NODES, MOBILE ENTITY, COMPUTER PROGRAMS AND COMPUTER PROGRAM PRODUCTS FOR PROTECTING PRIVACY OF A MOBILE ENTITY

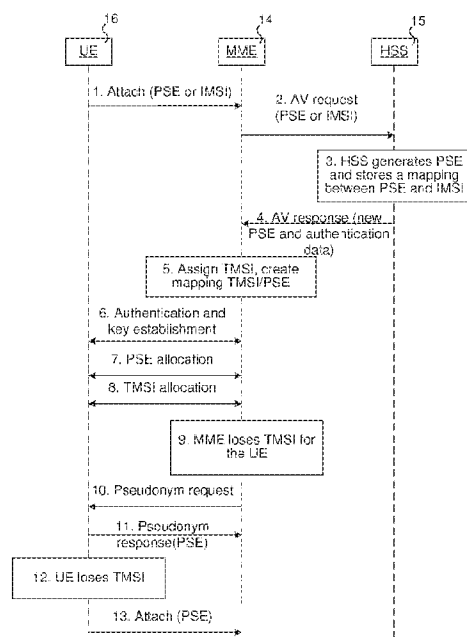


Fig. 3

(57) Abstract: A method (20) for a first network node (5, 15) of protecting confidentiality of a first identifier associated by the first network node (5, 15) with a subscription used by a mobile entity (6, 16) in a communications network (1, 10) is provided. The communications network (1, 10) comprises a home network (3, 13) of the mobile entity (6, 16) and a serving network (2, 4, 12, 14) serving the mobile entity (6, 16). The method (20) comprises the following steps performed by the first network node (5, 5), which is part of the home network (3, 13): receiving (21), from a second network node (4, 14) which is part of the serving network (2, 12), a first request for authentication information for the mobile entity (6, 16), the first request comprising the first identifier, generating (22) a first pseudonym associated with the first identifier, creating (23) a link between the first pseudonym and the first identifier, and sending (24), to the second network node (4, 14), the first pseudonym in response to the first request for authentication information for use as an identifier for the mobile entity (6, 16) in the serving network (2, 12). A method (70) for a second network node is also provided, and corresponding network nodes, computer programs and computer program products.

Methods, network nodes, mobile entity, computer programs and computer program products for protecting privacy of a mobile entity

Technical field

The technology disclosed herein relates generally to the field of communications systems and in particular to methods and means for protecting privacy of subscribers in such systems.

Background

In wireless communication there is inherently a risk of eavesdropping, i.e. that data sent from or to a user may be intercepted and used by an unintended user. Locations or traveling routes of a user in a mobile network could, for instance, be tracked by tracing to which cells the user is connected or through which cells the user is travelling, resulting in in privacy infringement.

It is known that the technical implementation of many trust models, including those used in mobile networks, may leave open the possibility for various types of attacks, from external hackers as well as malicious insiders. If, for example, a network operator's trust for its employees is betrayed, security is typically lost. Entities with access to interconnect networks, interconnecting home and visited networks, are often authorized to perform very sensitive operations on other entities and security thereof is therefore of high importance.

In recent years there has been much publicity around cases wherein attacks have been performed on networks supporting the operation of mobile communications systems. For example, attackers have quite easily obtained legal or illegal access to signaling system 7 (SS7) networks, and by using that access have been able to elicit privacy sensitive information such as subscribers' precise geographical location. However, attacks are not only performed via such gray-area access to interconnecting networks. There have also been various cases of actively compromising nodes in the mobile network core and vendors development environments.

Another type of attack comprises obtaining the identity of a mobile subscriber, e.g. International Mobile Subscriber Identity (IMSI) catchers. The IMSI catcher, in the simplest form, requests the long-term subscriber identity from a mobile terminal. Since this is a valid request in normal operations, the mobile terminal replies with its

long-term subscriber identity according to standardized protocols. The IMSI catchers can be used e.g. to keep track of who is moving in a certain area. In addition, more advanced IMSI catchers can eavesdrop on the traffic to and from the mobile terminal. Cellular standards do not address threats from such attack-devices, and it is a non-trivial issue since the IMSI requests may occur when there is no security context available to cryptographically protect the request.

A current solution for protecting the privacy of the subscriber's identity is based on a serving network assigning a temporary identity to the mobile terminal at regular intervals. The long-term identity is used only as a fallback mechanism or when a temporary identity has not yet been assigned. The long-term identity may be the mentioned IMSI and the temporary identity is then the Temporary Mobile Subscriber Identity (TMSI). There are also other temporary identifiers used, e.g. various Radio Network Temporary Identifiers (RNTIs) used locally for radio access specific parts, e.g. for identifying radio channels.

To avoid a lock-out of a mobile terminal when errors occur, e.g. when the serving network or the mobile terminal has lost the TMSI, the above mentioned fallback mechanism is provided, wherein the mobile terminal falls back to using the IMSI whenever the serving network so requests. This fallback is what the mentioned IMSI-catchers use to obtain the IMSI from the mobile terminals. The current way of protecting privacy does hence not provide any protection against an active attacker on the air-interface, claiming to be a legitimate network that has lost the temporary identity. Neither is there any protection against passive eavesdroppers who happen to be present when (legitimate or illegitimate) IMSI requests are made.

At the initial phases of Universal Mobile Telecommunications System (UMTS) and Long Term Evolution (LTE) standardization, some enhanced long-term identity protection mechanisms were discussed. The three options that were discussed included encrypting IMSI by a public key of the network, encrypting IMSI using a shared group key, and authenticating IMSI requests by the network.

The option of encrypting IMSI by a public key of the network was, eventually, dismissed due to the complexity and limited processing power for public key operations of mobile terminals that existed at the time. Further, this option may not protect against malicious insiders, e.g., from a roaming partner who could see a

business case in extracting and selling IMSIs and the corresponding location of mobile terminals.

The option of encrypting IMSI using a shared group key does not prevent other mobile terminals, who also know the group key, from obtaining the IMSI.

- 5 The third option, the authenticating IMSI requests by the network does not protect against passive (eavesdropping) attackers and requires complex key management associated with the serving network, e.g. a public key infrastructure (PKI).

Further, since the trust model assumes that anyone with access to the interconnecting network is trusted to behave well, the nodes in the serving network
10 will supply sensitive information such as the precise location of a subscriber when requested to do so by another node connected to the interconnecting network. As is evident from the multiple occurrences of various attacks, this trust model does no longer match reality. The privacy protection of the subscriber identity, being designed under the assumption that the trust model holds, is therefore ineffective.

- 15 The above mentioned problems occur also for other communications system. For example, systems using the Extensible Authentication Protocol (EAP) have various mechanisms to handle identifiers. As an example, when using the EAP-Authentication and Key Agreement (AKA) mechanism, there are occasions where the network issues identity requests that the terminal must accept and respond to. While
20 also here a scheme of temporary identities is supported, there are occasions during normal operation when there is no option but to disclose the long term identity. In the specific case of EAP-AKA, which is used in some Wireless Local Area Networks (WLAN), this identity will again reveal the IMSI. In other cases, long term identities may be disclosed in the form of user names encoded in "Issued-to" fields of public key
25 certificates, etc.

From the above it is clear that there is a need for improvements in view of handling of identifiers in order to prevent identification of subscribers and to protect their privacy.

Summary

- 30 An objective of the present disclosure is to address and solve or at least alleviate at least one of the above mentioned problems.

The objective is according to an aspect achieved by a method for a first network node (e.g. a home subscriber server, HSS) of protecting confidentiality of a first identifier associated by the first network node with a subscription used by a mobile entity in a communications network. The communications network comprises a home network of the mobile entity and a serving network serving the mobile entity. The method
5 comprises the following steps performed by a first network node which is part of the home network: receiving, from a second network node, which is part of the serving network, a first request for authentication information for the mobile entity, the first request comprising the first identifier, generating a first pseudonym associated with
10 the first identifier, creating a link between the first pseudonym and the first identifier, and sending, to the second network node, the first pseudonym in response to the first request for authentication information for use as an identifier for the mobile entity in the serving network.

An advantage of the method is that e.g. IMSI catchers are rendered less useful, since
15 they will only be able to catch a pseudonym, which in addition may be changed often. Further, nodes of the serving network will become less attractive as attack targets, since the IMSI will not be available to them. Still further, the method reduces the problem of almost any entity with access to an interconnecting network being able to request the precise location of a subscriber.

20 The objective is according to an aspect achieved by a computer program for a first network node for protecting confidentiality of a first identifier associated by the first network node with a subscription used by a mobile entity. The computer program comprises computer program code, which, when executed on at least one processor of the first network node causes the first network node to perform the method as above.

25 The objective is according to an aspect achieved by a computer program product comprising a computer program as above and a computer readable means on which the computer program is stored.

The objective is according to an aspect achieved by a method in a first network node for protecting confidentiality of a first identifier associated by the first network node
30 with a subscription used by a mobile entity in a communications network. The communications network comprises a home network of the mobile entity and a serving network serving the mobile entity. The first network node is part of the home

network and is configured to: receive, from a second network node, which is part of the serving network, a first request for authentication information for the mobile entity, the first request comprising the first identifier, generate a first pseudonym associated with the first identifier, create a link between the first pseudonym and the first identifier, and send, to the second network node, the first pseudonym in response to the first request for authentication information for use as an identifier for the mobile entity in the serving network.

The objective is according to an aspect achieved by a method for a second network node (e.g. a mobility management entity, MME) of protecting confidentiality of a first identifier associated by a first network node with a subscription used by a mobile entity in a communications network. The communications network comprises a home network of the mobile entity and a serving network serving the mobile entity. The method comprises the following steps, performed by the second network node, which is part of the serving network: sending, to the first network node, which is part of the home network, a first request for authentication information for the mobile entity, the first request comprising the first identifier, receiving, from the first network node, a first pseudonym associated with the first identifier in response to the first request, creating a link between a temporary identifier of the mobile entity and the first pseudonym, and using the first pseudonym as identifier of the mobile entity.

The objective is according to an aspect achieved by a computer program for a second network node for protecting confidentiality of a first identifier associated by a first network node with a subscription used by a mobile entity. The computer program comprises computer program code, which, when executed on at least one processor of the second network node causes the second network node to perform the method as above.

The objective is according to an aspect achieved by a computer program product comprising a computer program as above and a computer readable means on which the computer program is stored.

The objective is according to an aspect achieved by a second network node for protecting confidentiality of a first identifier associated by a first network node with a subscription used by a mobile entity in a communications network. The communications network comprises a home network of the mobile entity and a

serving network serving the mobile entity. The second network node is part of the serving network and is configured to: send, to a first network node, which is part of the home network, a first request for authentication information for the mobile entity, the first request comprising the first identifier, receive, from the first network
5 node, a first pseudonym associated with the first identifier in response to the first request, create a link between a temporary identifier of the mobile entity and the first pseudonym, and use the first pseudonym as identifier of the mobile entity.

The objective is according to an aspect achieved by a method for a mobile entity of a communications network of protecting confidentiality of a first identifier associated
10 with a subscription used by the mobile entity. The communications network comprises a home network of the mobile entity and a serving network serving the mobile entity. The method comprises sending to a second network node, which is part of the serving network, an attachment request, the attachment request comprising a first pseudonym previously generated for the mobile entity by a first
15 network node, which is part of the home network, or the first identifier in encrypted format, encrypted in the mobile entity, and receiving, from the second network node, a second pseudonym associated with the mobile entity in response to the attachment request.

The objective is according to an aspect achieved by a computer program for a mobile
20 entity of a communications network for protecting confidentiality of a first identifier associated with a subscription used by the mobile entity. The computer program comprises computer program code, which, when executed on at least one processor of the mobile entity causes the mobile entity to perform the method as above.

The objective is according to an aspect achieved by a computer program product
25 comprising a computer program as above and a computer readable means on which the computer program is stored.

The objective is according to an aspect achieved by a mobile entity of a communications network of protecting confidentiality of a first identifier associated with a subscription used by the mobile entity. The communications network
30 comprises a home network of the mobile entity and a serving network serving the mobile entity. The mobile entity is configured to: send to a second network node, which is part of the serving network, an attachment request, the attachment request

comprising a first pseudonym previously generated for the mobile entity by a first network node, which is part of the home network, or the first identifier in encrypted format, encrypted in the mobile entity, and receive, from the second network node, a second pseudonym associated with the mobile entity in response to the attachment request.

Further features and advantages of the embodiments of the present teachings will become clear upon reading the following description and the accompanying drawings.

Brief description of the drawings

Figure 1 illustrates schematically a general communications network in which embodiments according to the present teachings may be implemented.

Figure 2 illustrates schematically a basic LTE network in which embodiments according to the present teachings may be implemented.

Figure 3 is an exemplary sequence diagram illustrating an aspect according to the present teachings.

Figure 4 is an exemplary sequence diagram illustrating an aspect according to the present teachings.

Figure 5 summarizes exemplary ways of conveying a pseudonym from a home network to a mobile entity.

Figure 6 illustrates a flow chart over steps of an embodiment of a method in a first network node (e.g. HSS) in accordance with the present teachings.

Figure 7 illustrates schematically a communications network and means for implementing embodiments in accordance with the present teachings.

Figure 8 illustrates a first network node comprising function modules/software modules for implementing embodiments of the present teachings.

Figure 9 illustrates a flow chart over steps of an embodiment of a method in a second network node (e.g. MME) in accordance with the present teachings.

Figure 10 illustrates a second network node comprising function modules/ software modules for implementing embodiments of the present teachings.

Figure 11 illustrates a flow chart over steps of an embodiment of a method in a mobile entity in accordance with the present teachings.

- 5 Figure 12 illustrates schematically a mobile entity and means for implementing embodiments in accordance with the present teachings.

Figure 13 illustrates a mobile entity comprising function modules/ software modules for implementing embodiments of the present teachings.

Detailed description

- 10 In the following description, for purposes of explanation and not limitation, specific details are set forth such as particular architectures, interfaces, techniques, etc. in order to provide a thorough understanding. In other instances, detailed descriptions of well-known devices, circuits, and methods are omitted so as not to obscure the description with unnecessary detail. Same reference numerals refer to same or
15 similar elements throughout the description.

- Briefly, the present teachings provide, in different aspects and embodiments, privacy protection against compromised nodes of a serving network and malicious insiders as well as IMSI catchers by not providing the IMSI to the serving network, and instead providing a pseudonym which may be regularly updated. Examples of such nodes of
20 the serving network comprise Mobile Switching Center (MSC), Serving GPRS support node (SGSN), Mobility Management Entity (MME), etc.

- If the serving network node (e.g. MME) is nevertheless compromised, an attacker will only get access to the pseudonym and cannot easily deduce to which IMSI the pseudonym belongs. In addition, when a serving network node loses the TMSI or the
25 pseudonym for a given mobile terminal, it will not request the IMSI from the mobile terminal, but rather request the pseudonym. However, it is noted that such pseudonym request may technically be implemented as a standard IMSI request, but the response from the mobile terminal comprises the pseudonym instead of the IMSI. Depending on implementation, the serving network node may issue a conventional
30 IMSI request, but receive in response an encrypted IMSI or a pseudonym. An

advantage of such embodiments is transparency to the serving network, if the pseudonym is formatted according to the same principles as an IMSI. Alternatively, the serving network node may send a new type of request, a "pseudonym request", and receive in response the pseudonym. Since the mobile terminal does not send the
5 IMSI, at least not unencrypted, an IMSI catcher will not be able to obtain anything else than the pseudonym.

The described mechanism does not completely protect against IMSI catchers, which could catch the IMSI of a mobile terminal not yet having a pseudonym in the visited network and doing an attach request to an MME. However, the mechanism can be
10 combined with other security measures, such as the above-mentioned encryption of IMSI. An example of such encryption comprises encrypting a mobile subscription identification number (MSIN) part of the IMSI using a public key of the home network operator before sending it from the mobile terminal to the serving network. The serving network can still route the message to the correct home network based
15 on the Mobile Network Code (MNC) and Mobile Country Code (MCC) parts of the IMSI, which parts can be left in clear text. It is noted that this particular encryption does not prevent the problem of misbehaving serving network nodes (e.g. MMEs). The present disclosure does that, so the two parts provides complete protection in a complementary way.

20 A general objective of the present teachings is to address at least one or some of the disadvantages with the prior art solutions described in the background section. The various steps described below in connection with the figures should primarily be understood in a logical sense, while each step may involve the communication of one or more specific messages depending on the implementation and protocols used.

25 Embodiments according to the present teachings relate, in general, to the field of providing privacy for subscribers and other users in a communications network. In particular, embodiments are described for generating a pseudonym in a home network and using this pseudonym for identifying a mobile entity used by a subscriber in a serving network. Thereby, the long-term identity of the subscriber will
30 remain hidden from the serving network as well as entities eavesdropping on communication between the serving network and the mobile entity.

The disclosed mechanism applies to general communications networks where the subscriber can roam into a serving network which may be controlled by another (separate) legal entity than the entity controlling the subscriber's home network. As particular examples, the disclosed mechanism is applicable for instance in LTE,
5 Wideband Code Division Multiple Access (WCDMA) and Global System for Mobile Communications (GSM) networks CDMA/CDMA2000 defined by 3GPP2, or access technologies such as those of the IEEE 802.11 (WLAN) or 802.16 (WiMAX) families, etc. In the following, aspects and embodiments according to the present teachings are described in the context of LTE, but as will be appreciated by a person skilled in the
10 art, the teachings are applicable to a general communications network, such as illustrated in figure 1.

Figure 1 illustrates schematically a general communications network 1 comprising a home network 3 controlled by a home-operator and a serving network 2 controlled by a serving operator. It is noted that the home-operator and serving operator may be
15 the same entity. The serving network 2 may also be denoted visited network, e.g. when the serving operator is a different entity than the home-operator. A subscriber operating a mobile entity 6 has a subscription or is otherwise registered as a user with the home-operator. The subscriber, e.g. a roaming subscriber, has typically no direct business relation with the serving operator, e.g. need not be a subscriber also with the
20 serving operator. However, it is noted that the serving network 12 and the home network 3, 13 may belong to the same operator.

In the serving network 2 a serving function 4 is controlling the mobile entity 6 operated by the subscriber, e.g. in view of authentication, bearer activation and deactivation, allocation of temporary identities for the mobile entity 6. The serving
25 network may comprise a number of base stations, e.g. evolved Node B in case of LTE, providing wireless communication for the mobile entity 6 in one or more cells. The serving function 4 is connected to a home function 5 in the home network 3. The home function 5 may comprise a node comprising or having access to user and/or subscriber-related information, information on subscriptions such as subscriber
30 credentials, available services, mobility management information etc.

Figure 2 schematically illustrates a basic LTE network 10, comprising a mobile entity 16 operated by a subscriber, nodes such as a Mobility Management Entity (MME) 14

of a serving network 12, controlling the mobile entity's 16 access via the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) 17, and a Home Subscription Server (HSS) 15 of the home network 3, 13. E-UTRA is the air interface of LTE, over which the mobile entity 16 communicates with eNodeBs. E-UTRAN is a combination
5 of E-UTRA, UEs and eNnodeBs, generally indicated at reference numeral 17. The MME 14 is an example on the serving function 4 mentioned with reference to figure 1, while the HSS 15 is an example on the home function 5. The eNodeBs of the E-UTRAN 17 communicates with the MME 14 over an S1 interface. The MME 14 in turn communicates with the HSS 15 over an S6a interface. It is noted that the UE 16
10 comprises mobile equipment (ME) and a Universal Subscriber Identity Module (USIM), and the ME typically has an identifier, e.g. International Mobile Station Equipment Identity (IMEI), enabling the communications network to identify the device. The UE 16 also comprises an identifier, e.g. the IMSI associated with a subscription tied to the UE 16, the subscription allowing the UE 16 to be used for
15 obtaining services from the communications network. The UE user identifier (e.g. IMSI) is typically provided on a removable card, e.g. Universal Integrated Circuit Card (UICC) card, while the ME identifier (e.g. IMEI) can be found in or on the ME 16.

It is noted that when the subscription/IMSI is associated with a removable card such
20 as UICC, the ME part of the UE 16 may in principle change over time due to so called "plastic roaming"; when the user/ subscriber simply moves the UICC from one ME to another. Such plastic roaming does not affect the principles of the invention. It is not possible to maintain service while the UICC is moved from one ME 16 to another, and the description below relates to steps and methods occurring while the UICC is
25 inserted into a specific ME 16.

Figure 3 is an exemplary sequence diagram illustrating an aspect according to the present teachings. In the disclosed mechanism, a pseudonym is used to protect the privacy of the long-term subscriber identity in the LTE environment. In the following, the mobile entity 16 is represented and exemplified by a user equipment (UE) 16.

30 At arrow 1, the UE 16 performs an attach procedure to the MME 14 when the UE 16 registers to the serving network 12. If the UE 16 has access to a TMSI, the UE 16 may use it in an attach request of the attach procedure. The mechanism according to the

present teachings interacts well with this existing TMSI mechanism (not shown in figure 3). If no TMSI is available, the UE 16 may identify itself using a pseudonym (PSE) instead of the IMSI, as will be explained below. Further, the TMSI may be mapped to/from the pseudonym PSE rather than to/from the IMSI. Thus, as a principle, whenever identification by means IMSI would normally be required, the PSE is used instead. Only the home network 13, e.g. the HSS 15 thereof, and the UE 16 know the mapping between the PSE and IMSI. While the MME 14 knows the mapping between PSE and TMSI, it thus does not know the mapping between TMSI and IMSI. This is in contrast to today's systems where also the MME 14 knows the mapping between TMSI and IMSI. In the disclosed mechanism, the IMSI is hidden from the serving network 12, including the MME 14.

In the case that the UE 16 does not yet have a PSE, it may need to use its long-term identity IMSI instead. As mentioned briefly, encryption of the IMSI by a public key of the home network 13 may in such cases be used to prevent the IMSI from being eavesdropped during transit of the IMSI from the UE 16 to the HSS 15. The UE 16 may for instance encrypt part of the IMSI, e.g. encrypt the MSIN part of the IMSI using the public key of the home network 13 whereas MCC and MNC parts of the IMSI may be kept un-encrypted. The serving network 12, in particular the MME 14 thereof, is then not provided any information about the UE 16 and hence not about its subscriber, besides the identity of the home network of the subscriber. In a broadest embodiment of the present teachings, the initial use of un-encrypted IMSI may also be used, thereafter relying on the privacy protection provided by the pseudonym PSE. In the following, the term "encrypted IMSI" is used, and the term encompasses cases wherein the entire IMSI is encrypted as well as cases wherein only part of the IMSI is encrypted.

Upon reception of the attach request, the MME 14 requests an Authentication Vector (AV) from the HSS 15 (arrow 2). The AV request comprises the PSE or the encrypted IMSI as sent by the UE 16. The HSS 15 may then use the pseudonym PSE (or IMSI after decryption) to allocate or generate a new pseudonym PSE (box indicated at reference numeral 3). The new pseudonym is preferably chosen to be distinct from other pseudonyms, currently associated with other subscribers. In some embodiments, the pseudonym PSE may be chosen to have the same format as an IMSI, e.g. being structurally composed of MCC, MNC and MSIN fields. In such case,

MCC and MNC may be identical to the corresponding sub-fields of the IMSI and only the MSIN part carries the pseudonym information. Further, still with reference to box 3, the HSS 15 creates a link between the generated pseudonym PSE and the long-term identity IMSI, e.g. a mapping between them. The HSS stores the created link or the mapping or makes the created link/mapping otherwise retrievable for future use, e.g. by sending it for storage elsewhere.

The HSS 15 includes the new pseudonym PSE (or the old pseudonym, in a new was not generated) together with the AV in a response (arrow 4) to the MME 14. In any case, a PSE (old or new) takes the place of what conventionally would be the IMSI.

When, in box indicated at reference numeral 5, the MME 14 receives the AV from the HSS 15, the MME 14 can use the AV to authenticate and assign a Temporary IMSI (TMSI) to the UE 16. The MME 14 further creates a mapping between the assigned TMSI and the pseudonym PSE received from the HSS 15. It is noted that the MME 14 does not know the long-term identity of the subscription associated with the UE 16, i.e., the IMSI stored on the Universal Subscriber Identity Module (USIM) (or corresponding card, device or the like of the UE).

There is, as indicated by double-headed arrow 6, authentication and key establishment signaling between the UE 16 and the MME 14 (typically via intermediate node(s) such as gateways and eNodeBs). Generally, the purpose of the AKA procedure is to provide mutual authentication between the UE 16 and the serving network 12.

According to the present teachings, the MME 14 also transfers the pseudonym PSE to the UE 16 (double-headed arrow 7), which the UE 10 may be configured to acknowledge receipt of. "Transfer" is in this context understood as being provided to the UE 16, typically via intermediate nodes such as eNodeBs. This may be done in the same procedure as the TMSI allocation procedure (double-headed arrow 8). It may alternatively be done by the HSS 15 including the pseudonym PSE as a new information element that is transferred together with authentication information (exemplified by AUTN and RAND) from the HSS 15 to the UE 16 (again via intermediate nodes). This is disclosed and described in more detail with reference to figure 4. The pseudonym PSE may, in some embodiments, be included as part of

AUTN or RAND. The pseudonym PSE would preferably be encrypted from the HSS 15 to the UE 16.

In case the MME 14 would, for any reason, loose the pseudonym PSE or TMSI for a given UE 16 (box indicated at reference numeral 9), the MME 14 may request the pseudonym PSE from the UE 16 (arrow 10). The UE 16 in turn replies with the pseudonym PSE (arrow 11). In a regular LTE network and according to prior art, the MME 14 would in this situation have to request the IMSI from the UE 16 and the UE 16 would then risk revealing it to potential eavesdroppers since it would have to be sent in clear text. In case the UE 16 loses the TMSI (box indicated at reference numeral 12), it can re-attach (arrow 13) to the network using the pseudonym PSE as the identifier just as it did in the first step, and thereby avoiding revealing the IMSI.

According to an aspect of the present teachings, the MME 14 may request any context information related to a mobile subscriber or mobile entity 16 from the HSS 15 using the pseudonym PSE. The MME 14 may even send the request to a different node than an HSS 15. An MME 14 may for instance send the request to another MME which, for some reason, may have knowledge about the user and the user's pseudonym PSE. An example of such situation, wherein a first MME could send a request to a second MME, comprises when a UE 16 has moved into a service area covered by the second MME. In that case the UE 16 will present the MME in the new service area with the pseudonym PSE, for example in a Tracking Area Update message. The second MME in the new service area would then, based on the pseudonym PSE, request the security context for the UE 16 from the first MME serving the service area to which the UE 16 was previously connected.

Figure 4 is an exemplary sequence diagram illustrating an aspect according to the present teachings. In particular, a message sequence diagram is shown illustrating how the authentication in LTE may be augmented in order to provide the UE 16 with the pseudonym PSE during the authentication procedure (schematically illustrated at arrow 6 of figure 3). When the UE 16, at arrow 1, attaches to the MME 14 of a serving network 12 it may use the pseudonym PSE or the encrypted IMSI. The MME 14 then sends (arrow 2) the AV request to the HSS 15, the request comprising the pseudonym PSE or the encrypted IMSI, whichever it received from the UE 16. The HSS 15 sends in response (arrow 3), to the MME 1, the AV response and include in this response a

new information element: the pseudonym PSE. The response may comprise the conventional AV response message comprising information elements AUTN and RAND, KASME, XRES, with the new information element pseudonym PSE added. The pseudonym PSE may be encrypted, as mentioned earlier. The conventional authentication vector comprises these four parameters: a random number (RAND),
5 an authentication token (AUTN), an expected user response (XRES) and an intermediate access security management entity key (KASME). The MME 14 sends (arrow 4) an authentication request to the UE 16 including the RAND, AUTN in conventional way, and also the PSE. The UE 16 responds (arrow 5) to the
10 authentication request in conventional way, e.g. calculates a response parameter RES based on AUTN and RAND, and now also has the pseudonym PSE, which it may use to authenticate itself in the serving network 12 in subsequent message exchanges.

The HSS 15 may generate the pseudonym PSE by randomly or pseudo-randomly generating a string. As another alternative, the HSS 15 may generate the pseudonym
15 by encrypting the IMSI (or parts thereof, e.g. the MSIN) using a time dependent key with an encryption algorithm such as according to Advanced Encryption Standard (AES) in counter mode. The term time-dependent is here only intended to mean that different keys may be used at different times, it does not necessarily imply that time is a parameter used in the derivation of the key even though this may be the case.
20 Optionally, the HSS 15 may generate the pseudonym by inputting the IMSI and a time dependent parameter into a hash function, such as e.g. Secure Hash Algorithm-256 (SHA-256) or SHA-1, or a key derivation function, such as e.g. Hash Message Authentication Code-SHA-256 (HMAC-SHA-256). The pseudonym PSE may thus have a format compatible with the IMSI format is so desired, i.e. it may comprise
25 sub-fields equivalent to the MCC, MNC and MSIN.

In other embodiments, the HSS 15, or more generally a database server handling the user's subscription, may generate the pseudonym in accordance with what has been described, but using a different long-term identity than the IMSI. It could for example be a Network Access Identifier, an IP Multimedia Subsystem (IMS)
30 Multimedia Public Identity (IMPU) or IP Multimedia Private Identity (IMPI) a social network login identifier (e.g. Facebook login identifier), or some username. This provides a convenient way to integrate use of non-SIM based identities, since the format of the generated pseudonym PSE, being e.g. a bit string, can easily be made to

be indifferent to the format of the underlying long-term identity, irrespective of it being the IMSI, Facebook ID, or something else.

A common way to handle both IMSI/USIM-based identifies as well as non-IMSI/USIM identifiers within the same framework is in the context of the EAP
5 protocol. In EAP, the network may request user/subscriber identity using the message EAP-Request/Identity and the user/subscriber (called "peer" in EAP terminology) provides it in an EAP-Response/Identity message. EAP suffers from the same problems as discussed above and there may be situations where an UE 16 using EAP will be forced to reveal its long-term identifier. If, for example, EAP-AKA is used,
10 this long-term identifier will again be the IMSI. While some EAP methods provide so called pseudonyms, it should be noted that these are not accessible to intermediary networks such as a serving network 12. Therefore, when the serving network needs to perform e.g. mobility management, some other identifier will be needed and that identifier could still leak information about the user/subscriber.

15 The present teachings may be applied also in such contexts. Considering, for example, a situation wherein the UE 16 is a WLAN terminal accessing a serving network 12 over WLAN. The node corresponding to the MME 14 may now instead be the WLAN Access Point or a PDG (Packet Data Gateway). The node in the home network 13 corresponding to the HSS 15 may still be a HSS or more generally, an
20 Authentication, Authorization and Accounting (AAA)/EAP server. In this case, when the UE 16 receives an EAP-Request/Identity message, it may include a previously assigned pseudonym PSE (or an encrypted long-term identifier such as IMSI) in the corresponding EAP-Response/Identity. Using the present teachings renders it possible to make the same pseudonym PSE available to the serving network 12, e.g.
25 for mobility management purposes. For example, the PSE could be included in Diameter or Radius protocol based signaling between nodes of the home network 13 and the serving network 12. Other handling/updates of PSE are analogous to what has just been described.

According to yet another aspect, the HSS 15 calculates the pseudonym PSE based on
30 the RAND used in the Authentication and Key Agreement (AKA) protocol and/or based on a key derived in one or more steps from the RAND, e.g., in LTE the Key Access Security Management Entity (KASME) key. Since the UE 16 can calculate the

same pseudonym PSE from the received RAND and/or KASME, the MME 14 does not need to send the pseudonym PSE to the UE 16 over the air interface.

In yet another embodiment, the HSS 15 may calculate the PSE from the SQN xor AK field which is present in the AUTN. The SQN is the sequence number associated with the authentication vector, and AK is the anonymity key associated with the authentication vector. It is noted that SQN xor AK is unique for each new authentication vector. A reason for not using SQN directly is that, if the authentication key AK is not equal to all zeroes, the SQN is only visible/accessible inside the USIM. The SQN is not visible in the actual UE 16 and can hence not be used by the UE 16 to calculate PSE. This is not a problem since the SQN xor AK is statistically unique for each authentication vector.

The HSS 15 and/or the UE 16 may lose the pseudonym PSE. This can occur, e.g., due to a re-start of the HSS 15. When this happens, the UE 16 would not be able to present the pseudonym PSE as an identifier anymore and would have to rely on sending the long-term identity, the IMSI. The disclosed mechanism provides a solution for this situation as well. As explained in the background section, the UE 16 can send the long-term identity encrypted with the home network's (e.g. HSS's 15) public key to break free from this dead lock, and get a new pseudonym PSE according to the procedure described with reference to figure 3.

Other parameters than those explicitly mentioned herein may be input to a Key Derivation Functions (KDF), Message Authentication Codes (MAC) and any other functions in all instances described herein. The parameters may be put in a different order than explicitly mentioned. The parameters may be transformed before being input to the function. For example, a set of parameters $P_1, P_2, \dots, P_n$, for some nonnegative integer n , could be transformed by first being run through a second function f and the result of that, i.e., $f(P_1, P_2, \dots, P_n)$, being input to the function.

An exemplary embodiment of the key derivation is when the parameter P_1 is first transformed before being input to a KDF to calculate a key called "output_key":
$$\text{output_key} = \text{KDF}(f(P_1), \text{some other parameter}),$$
 where f is some arbitrary function or chain of functions. The input "some other parameter" could be 0, 1 or more other parameters, e.g., used to bind the key to a certain context. Sometimes, the notation "..." may be used as a synonym for "some other parameter". Parameters may be input

as separate parameters or may be concatenated together and then input in one single input to the KDF. Even in the presence of things like these, the core of the idea remains the same.

It is noted that the present teachings are also applicable when IMSI identifiers are used within Extensible Authentication Protocol (EAP)-AKA.

Figure 5 summarizes some of the above aspects according to the present teachings, and in particular five exemplary ways of conveying a pseudonym from a home network 13, in particular the HSS 15 thereof, to a mobile entity 16.

A first option, indicated at a), is that the HSS 15 simply sends the pseudonym, PSE, to the UE 16 via the MME 14. That is, the MME 14 merely acts as a middle-hand and conveys the PSE, that is receives from the HSS 15, to the UE 16.

A second option, indicated at b) is that the HSS 15 uses a function f taking some information "info" as input to calculate the PSE. The HSS 15 then sends the information "info" to the MME 14, which has the function f and having received the info may calculate the PSE for the UE 16 and store it as identifier of the UE 16. The MME 14 then sends the "info" to the UE 16, which also has the function f and can calculate the PSE and use for identifying itself in the serving network 12. The "info" may for instance comprise the RAND, KASME, cipher key (CK) or integrity key (IK) or any other key or set of keys that have been described. The USIM of the UE 16 computes the cipher key CK and the integrity key IK as a function of RAND in the conventional authentication responses.

A third option, indicated at c) is that the HSS 15 again uses a function f taking some information "info" as input to calculate the PSE. The HSS 15 then sends the information "info" to the MME 14, which has the function f and having received the info may calculate the PSE for the UE 16 and store it as identifier of the UE 16. The MME 14 then sends the PSE (instead of "info" as in the second option) to the UE 16, which thus receives the PSE and may use it identifying itself in the serving network 12. In this case, the UE 16 does not have to have the function f .

A fourth option, indicated at d) is that the HSS 15 once again uses a function f taking some information "info" as input to calculate the PSE. The HSS 15 then sends the information "info" along with the PSE to the MME 14. In this option though, the

MME 14 does not have the function f but may store the PSE as an identifier of the UE 16 having received it from the HSS 15. The MME 14 forwards the "info" to the UE 16, which has the function f and may calculate the PSE having received the "info" from the MME 14. The UE 16 may then use the PSE for identifying itself in the serving network 12.

A fifth option, indicated at e) is that the HSS 15 uses a function f taking some information "info" as input to calculate the PSE. The HSS 15 then sends the information "info" along with the PSE to the MME 14. The MME 14 stores the PSE for the UE 16 and also forwards the PSE to the UE 16. The MME 14 nor the UE 16 needs to have the function f in this case.

In view of backwards compatibility issues, it is possible that some aspects of the present teachings may be introduced and implemented only starting with a new generation of networks, e.g. with the fifth generation, 5G. If implementing the present teachings in legacy networks, a vast amount of legacy nodes would have to be updated, preferably simultaneously in order to keep the networks running. Fallbacks for allowing use of legacy authentication would have to be implemented. This may lead to possibilities of downgrade attacks where the network and/or the devices are fooled into believing they must refrain from using the herein disclosed enhanced privacy method due to the (incorrect) belief that the other party does not support it. If on the other hand the present teachings are implemented for 5G and onwards, it may be assumed that all entities supporting the 5G radio interface will also support implementation of the present teachings and no backwards compatibility problems would arise. For instance, the mobile entities would not respond to requests from visited networks for its long-term identity, but would instead use only the pseudonym and/or would only provide an encrypted IMSI.

The various embodiments and features that have been described may be combined in different ways, examples of which are given in the following with reference first to figure 6.

Figure 6 illustrates a flow chart over steps of an embodiment of a method for a first network node (e.g. HSS) in accordance with the present teachings. The method may be performed in a first network node for protecting confidentiality of a first identifier associated by the first network node with a subscription used by a

mobile entity 6, 16 in a communications network 1, 10. The first network node 5, 15 may for instance comprise a home network function, such as a HSS. The communications network 1, 10 comprises a home network 3, 13 of the mobile entity 6, 16 and a serving network 2, 4, 12, 14 serving the mobile entity 6, 16. As described
5 earlier (e.g. in relation to figure 5), in some embodiments a pseudonym is explicitly communicated from the home network function 5, 15 to the serving network 2, 4, 12, 14 whereas in other embodiments, only "info" from which the pseudonym can be derived is communicated. "Pseudonym" may hence also, in the following, be interpreted as information corresponding to a pseudonym, e.g. information from
10 which a pseudonym is derived.

The method 20 comprises the following steps performed by the first network node 5, 15, which is part of the home network 3, 13:

- Receiving 21, from a second network node 4, 14, which is part of the serving network 2, 12, a first request for authentication information for the mobile entity 6, 16, the
15 first request comprising the first identifier. The first identifier may for instance comprise an IMSI of the mobile entity 6, 16 in encrypted format (encrypted IMSI).
- Generating 22 a first pseudonym associated with the first identifier.
- Creating 23 a link between the first pseudonym and the first identifier. The creating 23 may for instance comprise creating a mapping between the first pseudonym and
20 the first identifier.
- Sending 24, to the second network node 4, 14, the first pseudonym in response to the first request for authentication information for use as an identifier for the mobile entity 6, 16 in the serving network 2, 12. The second network node 4, 14 may use the first identifier in different ways, e.g. in order to keep track of mobility of the mobile
25 entity 6, 16 and request contexts associated with the mobile entity 6, 16 from other nodes by using the first identifier.

An advantage provided by the method 20 is that an increased protection of the privacy of the user or subscriber of the mobile entity 6, 16 is enabled. The serving network 2, 12, e.g. a second network node 4, 14 such as a mobility management entity
30 thereof, is provided only with a pseudonym of the mobile entity 6, 16 and not any information about the actual identity of the mobile entity 6, 16 which in turn could

reveal information about the user of the mobile entity 6, 16. It would also be difficult for an attacker that intercepts this information to deduce any information about the user of the mobile entity (or about the subscription tied to the mobile entity, which in turn could give information about the user).

5 In an embodiment, the method 20 comprises:

- receiving, from the second network node 4, 14, a second request for authentication information for the mobile entity 6, 16, the second request comprising the first pseudonym associated with the first identifier,
- generating a second pseudonym associated with the first identifier,
- 10 - updating the link between the first pseudonym and the first identifier to a link between the second pseudonym and the first identifier, and
- sending, to the second network node 4, 14, the second pseudonym in response to the second request for authentication information.

The second network node 4, 14 may have received the first pseudonym from the
15 mobile entity 6, 16 e.g. as a message of an attachment procedure, and then turned to the home network 3, 13, in particular the first network node 5, 15 thereof, in order to authenticate the mobile entity 6, 16. In response to receiving the second request the home network 3, 13, e.g. the first network node 5, 15 thereof, generates a second
20 pseudonym associated with the first identifier, and sends it to the serving network 2, 12, e.g. the second network node 4, 14 thereof. The existing link between the first pseudonym and the first identifier is updated by the first network node 5, 15 to a link between the second pseudonym and the first identifier. An attacker having captured the first pseudonym has then no use of it, as it no longer is used by the communications network. The pseudonym may thus be updated frequently, which
25 makes the privacy protection provided by the method 20 even more secure.

In various embodiments, the first identifier comprises a long-term identity associated with a subscription used by the mobile entity 6, 16, such as the IMSI of the mobile entity 6, 16, preferably encrypted IMSI or a third (old) pseudonym previously generated for the mobile entity 6, 16. The IMSI may be encrypted in the mobile entity
30 6, 16 using e.g. a public key associated with the home network 3, 13; the public key

may be specific for the first network node 3, 13 or generic for the entire home network 3, 13,.

In an embodiment, the first identifier comprises an IMSI in encrypted format and the receiving 21 comprises receiving and decrypting the first identifier. The first
5 identifier, e.g. IMSI, may have been encrypted at the mobile entity 6, 16 by use of a public key associated with the home network 3, 13. The identity of the mobile entity 6, 16 and user thereof is thereby protected all the way from the mobile entity 6, 16 to the first network node 5, 15 in the home network 3, 13, preventing the identity to be captured over the air interface between the mobile entity 6, 16 and the second
10 network node 4, 14 of the serving network 2, 12.

In an embodiment, the sending 24 of the first pseudonym to the serving network 2, 12, in particular to the second network node 4, 14 thereof, comprises encrypting the first pseudonym and sending the encrypted first pseudonym for transferal by the serving network 2, 4, 12, 14 to the mobile entity 6, 16. When the first network node 5,
15 15 encrypts the first pseudonym before sending it to the second network node 4, 14 (of the serving network 2, 12), the second network node 4, 14 merely conveys it to the mobile entity 6, 16, which may decrypt it. This provides an even higher degree of protection of the privacy.

In various embodiments, the generating 22 comprises selecting a random number or
20 a pseudo random number, or applying a cryptographic function to at least a long-term identity associated with a subscription used by the mobile entity 6, 16, wherein the cryptographic function comprises one of: encryption function, a hash function or a key derivation function. Many different options are thus available for generating the pseudonyms.

25 The method 20 may be performed in a single node or in a distributed manner, wherein different steps are performed by different network nodes or other entities. It is noted that the steps of the method 20 may be performed by different (logical) entities arranged in a single network node or distributed over several network nodes. The method 20' may hence be performed in a communications network 1, 10 for
30 protecting confidentiality of a first identifier associated by a first network node (5, 15) with a subscription used by a mobile entity 6, 16. The communications network 1, 10

comprises a home network 3, 13 of the mobile entity 6, 16 and a serving network 2, 4, 12, 14 serving the mobile entity 6, 16.

The method 20' comprises receiving 21', in the home network 3, 5; 13, 15, a first request for authentication information for the mobile entity 6, 16 from the serving
5 network, the first request comprising the first identifier; generating 22', in the home network 3, 5; 13, 15, a first pseudonym associated with the first identifier, creating 23' a link between the first pseudonym and the first identifier, and sending 24', to the serving network 2, 4; 12, 14, the first pseudonym in response to the first request for authentication information for use as an identifier for the mobile entity 6, 16 in the
10 serving network 2, 12.

Figure 7 illustrates schematically a communications network 1, 10 and means for implementing embodiments in accordance with the present teachings. A first network node 5, 15 (e.g. HSS) of a communications network is illustrated schematically in which the method as described e.g. with reference to figure 6 may be
15 implemented.

The first network node 5, 15 comprises a processor 30 comprising any combination of one or more of a central processing unit (CPU), multiprocessor, microcontroller, digital signal processor (DSP), application specific integrated circuit etc. capable of executing software instructions stored in a memory 31 which can thus be a computer
20 program product 31. The processor 30 can be configured to execute any of the various embodiments of the method for instance as described in relation to figure 6.

The memory 31 can be any combination of read and write memory (RAM) and read only memory (ROM), Flash memory, magnetic tape, Compact Disc (CD)-ROM, digital versatile disc (DVD), Blu-ray disc etc. The memory 31 may also comprise
25 persistent storage, which, for example, can be any single one or combination of magnetic memory, optical memory, solid state memory or even remotely mounted memory.

The first network node 5, 15 also comprises an input/output device 33 (indicated by I/O in figure 7) for communicating with other entities, e.g. with network nodes of
30 visited network 4, 14 of the mobile entity 6, 16 and with other network nodes in the

home network 3, 13, which the first network node 5, 15 is part of. Such input/output device 33 of the first network node 5, 15 may comprise a communication interface.

The first network node 5, 15 may also comprise additional processing circuitry, schematically indicated at reference numeral 34, for implementing the various
5 embodiments according to the present teachings.

The present teachings provide computer programs 32 for the first network node 5, 15. The computer programs 32 comprises computer program code, which, when executed on at least one processor 30 on the first network node 5, 15 causes the first network node 5, 15 to perform the method 20 according to any of the described
10 embodiments thereof.

The present disclosure also encompasses computer program products 31 comprising a computer program 32 for implementing the embodiments of the method as described, and a computer readable means on which the computer program 32 is stored. The computer program product 31 may, as mentioned earlier, be any
15 combination of random access memory (RAM) or read only memory (ROM), Flash memory, magnetic tape, Compact Disc (CD)-ROM, digital versatile disc (DVD), Blu-ray disc etc.

A first network node 5, 15 (e.g. HSS) is provided for protecting confidentiality of a first identifier associated by a first network node (5, 15) with a subscription used by a
20 mobile entity 6, 16 in a communications network 1, 10. The communications network 1, 10 comprises a home network 3, 13 of the mobile entity 6, 16 and a serving network 2, 4, 12, 14 serving the mobile entity 6, 16. The first network node 5, 15 is part of the home network 3, 13 and is configured to:

- receive, from a second network node 4, 14, which is part of the serving network 2,
25 12, a first request for authentication information for the mobile entity 6, 16, the first request comprising the first identifier,
- generate a first pseudonym associated with the first identifier,
- create a link between the first pseudonym and the first identifier, and

- send, to the second network node 4, 14, the first pseudonym in response to the first request for authentication information for use as an identifier for the mobile entity 6, 16 in the serving network 2, 12.

5 The first network node 5, 15 may be configured to perform the above steps e.g. by comprising one or more processors 30 and memory 31, the memory 31 containing instructions executable by the processor 30, whereby the first network node 5, 15 is operative to perform the steps. In case of several processors 30 (not illustrated), they may be configured to perform all steps of the method 20 or only part of the steps.

In an embodiment, the first network node 5, 15 is configured to:

- 10 - receive, from the second network node 4, 14, a second request for authentication information for the mobile entity 6, 16, the second request comprising the first pseudonym associated with the first identifier, and
- generate a second pseudonym associated with the first identifier,
- update the link between the first pseudonym and the first identifier to a link
- 15 between the second pseudonym and the first identifier, and
- send, to the second network node 4, 14, the second pseudonym in response to the second request for authentication information.

In various embodiments, the first identifier comprises a long-term identity associated with a subscription used by the mobile entity 6, 16 or a third (old) pseudonym

20 previously generated for the mobile entity 6, 16.

In an embodiment, the first identifier comprises an identifier in encrypted format, and wherein the first network node 5, 15 is configured to receive and decrypt the encrypted first identifier.

In an embodiment, the first network node 5, 15 is configured to encrypt the first

25 pseudonym and to send the encrypted first pseudonym for transferal by the serving network 2, 4, 12, 14 to the mobile entity 6, 16.

In an embodiment, the first network node 5, 15 is configured to generate by selecting a random number or a pseudo random number, or applying a cryptographic function

to a long-term identity associated with a subscription used by the mobile entity 6, 16, wherein the cryptographic function comprises one of: encryption function, a hash function or a key derivation function.

5 The computer program products, or the memories, comprises instructions executable by the processor 30. Such instructions may be comprised in a computer program, or in one or more software modules or function modules.

Figure 8 illustrates a first network node comprising function modules/software modules for implementing embodiments of the present teachings. In an aspect, means are provided, e.g. function modules or units, that can be implemented using
10 software instructions such as computer program executing in a processor and/or using hardware, such as application specific integrated circuits, field programmable gate arrays, discrete logical components etc., or any combination thereof.

A first network node of protecting confidentiality of a first identifier associated by the first network node with a subscription used by a mobile entity in a communications
15 network is provided. The communications network comprises a home network of the mobile entity and a serving network serving the mobile entity. The first network node comprises a first unit 101 for receiving, from a second network node of the serving network, a first request for authentication information for the mobile entity, the first request comprising the first identifier. Such first unit 101 may for instance comprise a
20 network interface and/or processing circuitry for receiving such information.

The first network node comprises a second unit 102 for generating a first pseudonym associated with the mobile entity. Such second unit 102 may comprise various processing circuitry, e.g. processing circuitry, adapted generate the first pseudonym by using program code stored in memory.

25 The first network node comprises a third unit 103 for creating a link between the first pseudonym and the first identifier. Such third unit 103 may comprise various processing circuitry, e.g. processing circuitry, adapted to create the link by using program code stored in memory.

The first network node comprises a fourth unit 104 for sending, to the second
30 network node, the first pseudonym in response to the first request for authentication information for use as an identifier for the mobile entity in the serving network. Such

fourth unit 104 may for instance comprise a network interface and/or processing circuitry for sending such information.

Figure 9 illustrates a flow chart over steps of an embodiment of a method in a second network node in accordance with the present teachings.

5 The method 70 of protecting confidentiality of a first identifier associated by a first network node 5, 15 with a subscription used by of a mobile entity 6, 16 in a communications network 1, 10 may be performed in a second network node 4, 14 (e.g. MME). The communications network 1, 10 comprises a home network 3, 13 of the mobile entity 6, 16 and a serving network 2, 12 serving the mobile entity 6, 16. The
10 method 70 comprises the following steps, performed by the second network node 4, 14, which is part of the serving network 2, 12:

- Sending 71, to the first network node 5, 15 (e.g. HSS), which is part of the home network 3, 13, a first request for authentication information for the mobile entity 6, 16, the first request comprising the first identifier.
- 15 - Receiving 72, from the first network node 5, 15, a first pseudonym associated with the first identifier in response to the first request.
- Creating 73 a link between a temporary identifier of the mobile entity 6, 16 and the first pseudonym. The creating 73 a link between a temporary identifier of the mobile entity 6, 16 may comprise or be preceded by a step of assigning a temporary identifier
20 to the mobile entity.
- Using 74 the first pseudonym as identifier of the mobile entity 6, 16. The second network node 4, 14 may use the first pseudonym as identifier as well as the temporary identifier.

In an embodiment, the method 70 comprises, prior to the sending 71, receiving from
25 the mobile entity 6, 16 an attachment request comprising the first identifier, wherein the first identifier comprises an identifier in encrypted format, encrypted by the mobile entity 6, 16.

In an embodiment, the method 70 comprises assigning the temporary identifier to the mobile entity 6, 16.

In an embodiment, the method 70 comprises requesting, from the mobile entity 6, 16, the first pseudonym in response to determining that the temporary identifier has been lost.

In an embodiment, the receiving 72 comprises receiving the first pseudonym encrypted and the using 74 comprises conveying the encrypted first pseudonym to the mobile entity 6, 16 for use in the authenticating of the mobile entity 6, 16. In other embodiments, the second network node 4, 14 decrypts the first pseudonym before conveying it to the mobile entity 6, 16.

In various embodiments, the method 70 comprises:

- receiving, from a third network node, which is part of a second serving network to which the mobile entity 6, 16 is to be handed over to, a request for the first pseudonym, and
- sending, in response to the request, the first pseudonym to the third network node.

It is noted that the request from the third network node may typically comprise also request for other information besides the first pseudonym, e.g. information such as security context.

The method 70 may be performed in a single node or in a distributed manner, wherein different steps are performed by different network nodes or other entities. It is noted that the steps of the method 70 may be performed by different (logical) entities arranged in a single network node or distributed over several network nodes. The method 70' may hence be performed in a communications network 1, 10 for protecting confidentiality of a first identifier associated by a first network node 5, 15 with a subscription used by a mobile entity 6, 16. The communications network 1, 10 comprises a home network 3, 13 of the mobile entity 6, 16 and a serving network 2, 4, 12, 14 serving the mobile entity 6, 16. The method 70' comprises sending 71', from the serving network 2, 4, 12, 14 to the home network 3, 5, 13, 15, a first request for authentication information for the mobile entity 6, 16, the first request comprising the first identifier; receiving 72', from the home network 3, 5, 13, 15, a first pseudonym associated with the first identifier in response to the first request; creating 73' a link between a temporary identifier of the mobile entity 6, 16 and the

first pseudonym; and using 74' the first pseudonym as identifier of the mobile entity 6, 16.

Referring again to figure 7, a second network node 4, 14 of a communications network is also illustrated schematically in which the method as described e.g. with
5 reference to figure 9 may be implemented.

The second network node 4, 14 comprises a processor 50 comprising any combination of one or more of a central processing unit (CPU), multiprocessor, microcontroller, digital signal processor (DSP), application specific integrated circuit etc. capable of executing software instructions stored in a memory 51 which can thus
10 be a computer program product 51. The processor 50 can be configured to execute any of the various embodiments of the method for instance as described in relation to figure 9.

The memory 51 can be any combination of read and write memory (RAM) and read only memory (ROM), Flash memory, magnetic tape, Compact Disc (CD)-ROM,
15 digital versatile disc (DVD), Blu-ray disc etc. The memory 31 may also comprise persistent storage, which, for example, can be any single one or combination of magnetic memory, optical memory, solid state memory or even remotely mounted memory.

The second network node 4, 14 also comprises an input/output device 43 (indicated
20 by I/O in figure 7) for communicating with other entities, e.g. with network nodes of the home network 3, 13 of the mobile entity 6, 16 and with other network nodes in the serving network 12, which the second network node 4, 14 is part of. Such input/output device 43 of the second network node 4, 14 may comprise a communication interface.

25 The second network node 4, 14 may also comprise additional processing circuitry, schematically indicated at reference numeral 54, for implementing the various embodiments according to the present teachings.

The present teachings provide computer programs 52 for the second network node 4, 14. The computer programs 52 comprises computer program code, which, when
30 executed on at least one processor 50 on the second network node 4, 14 causes the

second network node 4, 14 to perform the method 70 according to any of the described embodiments thereof.

The present disclosure also encompasses computer program products 51 comprising a computer program 52 for implementing the embodiments of the method as
5 described, and a computer readable means on which the computer program 52 is stored. The computer program product 31 may, as mentioned earlier, be any combination of random access memory (RAM) or read only memory (ROM), Flash memory, magnetic tape, Compact Disc (CD)-ROM, digital versatile disc (DVD), Blu-ray disc etc.

10 A second network node 4, 14 is provided for protecting confidentiality of a first identifier associated by a first network node 5, 15 with a subscription used by a mobile entity 6, 16 in a communications network 1, 10. The communications network 1, 10 comprises a home network 3, 13 of the mobile entity 6, 16 and a serving network 2, 12 serving the mobile entity 6, 16. The second network node 4, 14 is part of the
15 serving network 2, 12 and is configured to:

- Send, to the first network node 5, 15, which is part of the home network 3, 13, a first request for authentication information for the mobile entity 6, 16, the first request comprising the first identifier.

- Receive, from the first network node 5, 15, a first pseudonym associated with the
20 first identifier in response to the first request.

- Create a link between a temporary identifier of the mobile entity 6, 16 and the first pseudonym.

- Use the first pseudonym as identifier of the mobile entity 6, 16.

The second network node 4, 14 may be configured to perform the above steps e.g. by
25 comprising one or more processors 50 and memory 51, the memory 51 containing instructions executable by the processor 50, whereby the second network node 4, 14 is operative to perform the steps. In case of several processors 50 (not illustrated) they may be configured to perform all steps of the method 70 or only part of the steps.

In an embodiment, the second network node 4, 14 is configured to, prior to the sending, receive from the mobile entity 6, 16 an attachment request comprising the first identifier, wherein the first identifier comprises an identifier in encrypted format, encrypted by the mobile entity 6, 16.

- 5 In an embodiment, the second network node 4, 14 is configured to assign the temporary identifier to the mobile entity 6, 16.

In an embodiment, the second network node 4, 14 is configured to request, from the mobile entity 6, 16, the first pseudonym in response to determining that the temporary identifier has been lost.

- 10 In an embodiment, the second network node 4, 14 is configured to receive by receiving the first pseudonym encrypted and configured to use by conveying the encrypted first pseudonym to the mobile entity 6, 16 for use in the authenticating of the mobile entity 6, 16.

In an embodiment, the second network node 4, 14 is configured to:

- 15 - receive, from third network node, which is part of a second serving network to which the mobile entity 6, 16 is to be handed over, a request for the first pseudonym, and
- send, in response to the request, the first pseudonym to the third network node.

- 20 Figure 10 illustrates a second network node comprising function modules/ software modules for implementing embodiments of the present teachings.

- In an aspect, means are provided, e.g. function modules or units, that can be implemented using software instructions such as computer program executing in a processor and/or using hardware, such as application specific integrated circuits, field programmable gate arrays, discrete logical components etc., or any combination
- 25 thereof.

A second network node for protecting confidentiality of a first identifier associated by a first network node 5, 15 with a subscription used by a mobile entity in a communications network is provided. The communications network comprises a home network of the mobile entity and a serving network serving the mobile entity.

The second network node comprises a first unit 111 for sending, to the first network node of the home network, a first request for authentication information for the mobile entity, the first request comprising the first identifier. Such first unit 111 may for instance comprise processing circuitry for sending such request.

- 5 The second network node comprises a second unit 112 for receiving, from the first network node, a first pseudonym associated with the first identifier in response to the first request. Such second unit 112 may comprise various processing circuitry, e.g. processing circuitry, for receiving such information.

- 10 The second network node comprises a third unit 113 for creating a link between a temporary identifier of the mobile entity and the first pseudonym. Such third unit 113 may comprise various processing circuitry, e.g. processing circuitry, adapted to create the link by using program code stored in memory.

- The second network node comprises a fourth unit 114 for using the first pseudonym as identifier of the mobile entity. Such fourth unit 114 may for instance comprise
15 various processing circuitry, e.g. processing circuitry, adapted for such use by using program code stored in memory.

Figure 11 illustrates a flow chart over steps of an embodiment of a method in a mobile entity in accordance with the present teachings.

- The method 80 may be performed in a mobile entity 6, 16 of a communications
20 network 1, 10 for protecting confidentiality of a first identifier associated with a subscription used by the mobile entity 6, 16. The communications network 1, 10 comprises a home network 3, 13 of the mobile entity 6, 16 and a serving network 2, 12 serving the mobile entity 6, 16. The method 80 comprises:

- Sending 81 to a second network node 4, 14, which is part of the serving network 2, 4,
25 12, 14 an attachment request, the attachment request comprising a first pseudonym (an old pseudonym) previously generated for the mobile entity 6, 16 by a first network node 5, 15, which is part of the home network 3, 13 or the first identifier in encrypted format, encrypted in the mobile entity 6, 16. The mobile entity 6, 16 may for instance encrypt a long-term identifier thereof, e.g. IMSI, the first time it attaches
30 to the serving network 2, 12, and if it subsequently needs to authenticate itself

towards the serving network 2, 12, then it may send the pseudonym PSE that it has been provided e.g. by the HSS 15.

- Receiving 82, from the second network node 4, 14, a second pseudonym (a new pseudonym) associated with the mobile entity 6, 16 in response to the attachment request.

In an embodiment, the method 80 comprises receiving, from the second network node 4, 14, a request for the second pseudonym and sending, in response thereto, the second pseudonym to the second network node 4, 14. The mobile entity 6, 16 may create a link between a temporary identifier identifying the mobile entity 6, 16 and the second pseudonym.

Figure 12 illustrates schematically a mobile entity and means for implementing embodiments in accordance with the present teachings.

The mobile entity 6, 16 comprises a processor 90 comprising any combination of one or more of a central processing unit (CPU), multiprocessor, microcontroller, digital signal processor (DSP), application specific integrated circuit etc. capable of executing software instructions stored in a memory 91 which can thus be a computer program product 91. The processor 90 can be configured to execute any of the various embodiments of the method for instance as described in relation to figure 11.

The memory 91 can be any combination of read and write memory (RAM) and read only memory (ROM), Flash memory, magnetic tape, Compact Disc (CD)-ROM, digital versatile disc (DVD), Blu-ray disc etc. The memory 91 may also comprise persistent storage, which, for example, can be any single one or combination of magnetic memory, optical memory, solid state memory or even remotely mounted memory.

The mobile entity 6, 16 also comprises an input/output device 93 (indicated by I/O in figure 12) for communicating with other entities, e.g. with network nodes of the currently serving network 12 of the mobile entity 6, 16. Such input/output device 93 of the mobile entity 6, 16 may comprise a wireless communication interface, antennas, processing circuitry 95 and/or devices for reception and transmission of wireless signaling.

The mobile entity 6, 16 may comprise a subscriber identity module (SIM) 96, also denoted SIM card, or a USIM card, or any other type of card or device or software for accessing the communications network 1, 10.

The mobile entity 6, 16 may also comprise additional processing circuitry,
5 schematically indicated at reference numeral 94, for implementing the various embodiments according to the present teachings.

The present teachings provide computer programs 92 for the mobile entity 6, 16. The computer programs 92 comprises computer program code, which, when executed on at least one processor 90 on the mobile entity 6, 16 causes mobile entity 6, 16 to
10 perform the method 80 according to any of the described embodiments thereof.

The present disclosure also encompasses computer program products 91 comprising a computer program 92 for implementing the embodiments of the method as described, and a computer readable means on which the computer program 92 is stored. The computer program product 91 may, as mentioned earlier, be any
15 combination of random access memory (RAM) or read only memory (ROM), Flash memory, magnetic tape, Compact Disc (CD)-ROM, digital versatile disc (DVD), Blu-ray disc etc.

A mobile entity 6, 16 is provided for use in a communications network 1, 10 for protecting confidentiality of a first identifier associated with a subscription used by
20 the mobile entity 6, 16. The communications network 1, 10 comprises a home network 3, 13 of the mobile entity 6, 16 and a serving network 2, 12 serving the mobile entity 6, 16. The mobile entity 6, 16 is configured to:

- send to a second network node 4, 14, which is part of the serving network 2, 4, 12, 14 an attachment request, the attachment request comprising a first pseudonym (an old
25 pseudonym) previously generated for the mobile entity 6, 16 by a first network node 5, 15, which is part of the home network 3, 13 or the first identifier in encrypted format, encrypted in the mobile entity 6, 16, and

- receive, from the second network node 4, 14, a second pseudonym (a new pseudonym) associated with the mobile entity 6, 16 in response to the attachment
30 request.

The mobile entity 6, 16 may be configured to perform the above steps e.g. by comprising one or more processors 90 and memory 91, the memory 91 containing instructions executable by the processor 90, whereby the mobile entity 6, 16 is operative to perform the steps.

- 5 In an embodiment, the mobile entity 6, 16 is configured to receive, from the second network node 4, 14, a request for the second pseudonym and sending, in response thereto, the second pseudonym to the second network node 4, 14.

Figure 13 illustrates a mobile entity comprising function modules/ software modules for implementing embodiments of the present teachings.

- 10 In an aspect, means are provided, e.g. function modules or units, that can be implemented using software instructions such as computer program executing in a processor and/or using hardware, such as application specific integrated circuits, field programmable gate arrays, discrete logical components etc., or any combination thereof.
- 15 A mobile entity is provided for use in a communications network for protecting confidentiality of a first identifier associated with a subscription used by the mobile entity. The communications network comprises a home network of the mobile entity and a serving network serving the mobile entity. The mobile entity comprises a first unit 121 for sending to a second network node of the serving network an attachment
- 20 request, the attachment request comprising a first pseudonym previously generated for the mobile entity by a first network node of the home network or the first identifier in encrypted format, encrypted in the mobile entity. Such first unit 121 may for instance comprise processing circuitry for sending such request.

- The mobile entity comprises a second unit 122 for receiving, from the second network
- 25 node, a second pseudonym associated with the mobile entity in response to the attachment request. Such second unit 122 may comprise various processing circuitry for receiving such pseudonym.

- The invention has mainly been described herein with reference to a few embodiments. However, as is appreciated by a person skilled in the art, other
- 30 embodiments than the particular ones disclosed herein are equally possible within the scope of the invention, as defined by the appended patent claims.

Claims

1. A method (20) for a first network node (5, 15) of protecting confidentiality of a first identifier associated by the first network node (5, 15) with a subscription used by a mobile entity (6, 16) in a communications network (1, 10), the communications network (1, 10) comprising a home network (3, 13) of the mobile entity (6, 16) and a serving network (2, 4, 12, 14) serving the mobile entity (6, 16), the method (20) comprising the following steps performed by the first network node (5, 15), which is part of the home network (3, 13):
- receiving (21), from a second network node (4, 14), which is part of the serving network (2, 12), a first request for authentication information for the mobile entity (6, 16), the first request comprising the first identifier,
 - generating (22) a first pseudonym associated with the first identifier,
 - creating (23) a link between the first pseudonym and the first identifier, and
 - sending (24), to the second network node (4, 14), the first pseudonym in response to the first request for authentication information for use as an identifier for the mobile entity (6, 16) in the serving network (2, 12).
2. The method (20) as claimed in claim 1, comprising:
- receiving, from the second network node (4, 14), a second request for authentication information for the mobile entity (6, 16), the second request comprising the first pseudonym associated with the first identifier,
 - generating a second pseudonym associated with the first identifier,
 - updating the link between the first pseudonym and the first identifier to a link between the second pseudonym and the first identifier, and
 - sending, to the second network node (4, 14), the second pseudonym in response to the second request for authentication information.
3. The method (20) as claimed in any of the preceding claims, wherein the first identifier comprises a long-term identity associated with a subscription used by the

mobile entity (6, 16) or a third pseudonym previously generated for the mobile entity (6, 16).

4. The method (20) as claimed in any of the preceding claims, wherein the first identifier comprises an identifier in encrypted format and wherein the receiving (21)

5 comprises receiving and decrypting the first identifier.

5. The method (20) as claimed in any of the preceding claims, wherein the generating (22) comprises selecting a random number or a pseudo random number, or applying a cryptographic function to a long-term identity associated with a subscription used by the mobile entity (6, 16), wherein the cryptographic function comprises one of:

10 encryption function, a hash function or a key derivation function.

6. A computer program (32) for first network node (5, 15) for protecting confidentiality of a first identifier associated by the first network node (5, 15) with a subscription used by a mobile entity (6, 16), the computer program (32) comprising computer program code, which, when executed on at least one processor of the

15 communications network (1, 10) causes the first network node (5, 15) to perform the method (20) according to any one of claims 1-5.

7. A computer program product (31, 41) comprising a computer program (32, 42) as claimed in claim 6 and a computer readable means on which the computer program (32, 42) is stored.

20 8. A first network node (5, 15) for protecting confidentiality of a first identifier associated by the first network node (5, 15) with a subscription used by a mobile entity (6, 16) in a communications network (1, 10), the communications network (1, 10) comprising a home network (3, 13) of the mobile entity (6, 16) and a serving network (2, 4, 12, 14) serving the mobile entity (6, 16), the first network node (5, 15),

25 which is part of the home network (3, 13) and being configured to:

- receive, from a second network node (4, 14), which is part of the serving network (2, 12), a first request for authentication information for the mobile entity (6, 16), the first request comprising the first identifier,

- generate a first pseudonym associated with the mobile entity (6, 16),

- create a link between the first pseudonym and the first identifier, and
 - send, to the second network node (4, 14), the first pseudonym in response to the first request for authentication information for use as an identifier for the mobile entity (6, 16) in the serving network (2, 12).
- 5 9. The first network node (5, 15) as claimed in claim 8, configured to:
- receive, from the second network node (4, 14), a second request for authentication information for the mobile entity (6, 16), the second request comprising the first pseudonym associated with the first identifier, and
 - generate a second pseudonym associated with the first identifier,
- 10 - update the link between the first pseudonym and the first identifier to a link between the second pseudonym and the first identifier, and
- send, to the second network node (4, 14), the second pseudonym in response to the second request for authentication information.
10. The first network node (5, 15) as claimed in claim 8 or 9, wherein the first
- 15 identifier comprises a long-term identity associated with a subscription used by the mobile entity (6, 16) or a third pseudonym previously generated for the mobile entity (6, 16).
11. The first network node (5, 15) as claimed in claim 8, wherein the first identifier comprises an identifier, in encrypted format, wherein the first network node (5, 15) is
- 20 configured to receive and decrypt the first identifier.
12. The first network node (5, 15) as claimed in any of claims 8-11, configured to generate by selecting a random number or a pseudo random number, or applying a cryptographic function to a long-term identity associated with a subscription used by the mobile entity (6, 16), wherein the cryptographic function comprises one of:
- 25 encryption function, a hash function or a key derivation function.
13. A method (70) for a second network node (4, 14) of protecting confidentiality of a first identifier associated by a first network node (5, 15) with a subscription used by a mobile entity (6, 16) in a communications network (1, 10), the communications

network (1, 10) comprising a home network (3, 13) of the mobile entity (6, 16) and a serving network (2, 12) serving the mobile entity (6, 16), the method (70) comprising the following steps, performed by the second network node (4, 14), which is part of the serving network (2, 12):

- 5 - sending (71), to the first network node (5, 15), which is part of the home network (3, 13), a first request for authentication information for the mobile entity (6, 16), the first request comprising the first identifier,
- receiving (72), from the first network node (5, 15), a first pseudonym associated with the first identifier in response to the first request,
- 10 - creating (73) a link between a temporary identifier of the mobile entity (6, 16) and the first pseudonym, and
- using (74) the first pseudonym as identifier of the mobile entity (6, 16).

14. The method (70) as claimed in claim 13, comprising, prior to the sending (71), receiving from the mobile entity (6, 16) an attachment request comprising the first
15 identifier, wherein the first identifier comprises an identifier in encrypted format, encrypted by the mobile entity (6, 16).

15. The method (70) as claimed in claim 13 or 14, comprising assigning the temporary identifier to the mobile entity (6, 16).

16. The method (70) as claimed in any of claims 13-15, comprising requesting, from
20 the mobile entity, (6, 16), the first pseudonym in response to determining that the temporary identifier has been lost.

17. The method (70) as claimed in any of claims 13-16, wherein the receiving (72) comprises receiving the first pseudonym in encrypted format and the using (74) comprises conveying the encrypted first pseudonym to the mobile entity (6, 16) for
25 use in the authenticating of the mobile entity (6, 16).

18. The method (70) as claimed in any of claims 13-17, comprising:

- receiving, from a third network node, which is part of a second serving network to which the mobile entity (6, 16) is to be handed over, a request for the first pseudonym, and

- sending, in response to the request, the first pseudonym to the third network node.

5 19. A computer program (52) for a second network node (4, 14) for protecting confidentiality of a first identifier associated by a first network node (5, 15) with a subscription used by a mobile entity (6, 16), the computer program (52) comprising computer program code, which, when executed on at least one processor of the second network node (4, 14) causes second network node (4, 14) to perform the
10 method (70) according to any one of claims 13-18.

20. A computer program product (51) comprising a computer program (52) as claimed in claim 19 and a computer readable means on which the computer program (52) is stored.

15 21. A second network node (4, 14) for protecting confidentiality of a first identifier associated by a first network node (5, 15) with a subscription used by a mobile entity (6, 16) in a communications network (1, 10), the communications network (1, 10) comprising a home network (3, 13) of the mobile entity (6, 16) and a serving network (2, 12) serving the mobile entity (6, 16), the second network node (4, 14), which is part of the serving network (2, 12) and being configured to:

20 - send, to the first network node (5, 15), which is part of the home network (3, 13), a first request for authentication information for the mobile entity (6, 16), the first request comprising the first identifier,

- receive, from the first network node (5, 15), a first pseudonym associated with the first identifier in response to the first request,

25 - create a link between a temporary identifier of the mobile entity (6, 16) and the first pseudonym, and

- use the first pseudonym as identifier of the mobile entity (6, 16).

22. The second network node (4, 14) as claimed in claim 21, configured to, prior to the sending, receive from the mobile entity (6, 16) an attachment request comprising

the first identifier, wherein the first identifier comprises an identifier in encrypted format, encrypted by the mobile entity (6, 16).

23. The second network node (4, 14) as claimed in claim 21 or 22, configured to assign the temporary identifier to the mobile entity (6, 16).

5 24. The second network node (4, 14) as claimed in any of claims 21-23, configured to request, from the mobile entity (6, 16), the first pseudonym in response to determining that the temporary identifier has been lost.

25. The second network node (4, 14) as claimed in any of claims 21-24, configured to receive by receiving the first pseudonym encrypted and configured to use by
10 conveying the encrypted first pseudonym to the mobile entity (6, 16) for use in the authenticating of the mobile entity (6, 16).

26. The second network node (4, 14) as claimed in any of claims 21-25, configured to:

- receive, from third network node, which is part of a second serving network to which the mobile entity (6, 16) is to be handed over, a request for the first
15 pseudonym, and

- send, in response to the request, the first pseudonym to the third network node.

27. A method (80) for a mobile entity (6, 16) of a communications network (1, 10) of protecting confidentiality of a first identifier associated with a subscription used by the mobile entity (6, 16), the communications network (1, 10) comprising a home
20 network (3, 13) of the mobile entity (6, 16) and a serving network (2, 12) serving the mobile entity (6, 16), the method (80) comprising:

- sending (81) to a second network node (4, 14), which is part of the serving network (2, 4, 12, 14) an attachment request, the attachment request comprising a first pseudonym previously generated for the mobile entity (6, 16) by a first network node
25 (5, 15), which is part of the home network (3, 13) or the first identifier in encrypted format, encrypted in the mobile entity (6, 16), and

- receiving (82), from the second network node (4, 14), a second pseudonym associated with the mobile entity (6, 16) in response to the attachment request.

28. The method (80) as claimed in claim 27, comprising receiving, from the second network node (4, 14), a request for the second pseudonym and sending, in response thereto, the second pseudonym to the second network node (4, 14).

29. A computer program (92) for a mobile entity (6, 16) of a communications network (1, 10) for protecting confidentiality of a first identifier associated with a subscription used by the mobile entity (6, 16), the computer program (92) comprising computer program code, which, when executed on at least one processor of the mobile entity (6, 16) causes the mobile entity (6, 16) to perform the method (90) according to any one of claims 27-28.

30. A computer program product (91) comprising a computer program (92) as claimed in claim 29 and a computer readable means on which the computer program (92) is stored.

31. A mobile entity (6, 16) of a communications network (1, 10) for protecting confidentiality of a first identifier associated with a subscription used by the mobile entity (6, 16), the communications network (1, 10) comprising a home network (3, 13) of the mobile entity (6, 16) and a serving network (2, 12) serving the mobile entity (6, 16), the mobile entity (6, 16) being configured to:

- send to a second network node (4, 14), which is part of the serving network (2, 4, 12, 14) an attachment request, the attachment request comprising a first pseudonym previously generated for the mobile entity (6, 16) by a first network node (5, 15), which is part of the home network (3, 13) or the first identifier in encrypted format, encrypted in the mobile entity (6, 16), and

- receive, from the second network node (4, 14), a second pseudonym associated with the mobile entity (6, 16) in response to the attachment request.

32. The mobile entity (6, 16) as claimed in claim 31, configured to receive, from the second network node (4, 14), a request for the second pseudonym and sending, in response thereto, the second pseudonym to the second network node (4, 14).

33. A method (20') for a communications network (1, 10) of protecting confidentiality of a first identifier associated by a first network node (5, 15) with a subscription used by a mobile entity (6, 16), the communications network (1, 10) comprising a home

network (3, 13) of the mobile entity (6, 16) and a serving network (2, 4, 12, 14) serving the mobile entity (6, 16), the method (20') comprising:

- receiving (21'), in the home network (3, 5; 13, 15), a first request for authentication information for the mobile entity (6, 16) from the serving network, the first request comprising the first identifier,
- generating (22'), in the home network (3, 5; 13, 15), a first pseudonym associated with the first identifier,
- creating (23') a link between the first pseudonym and the first identifier, and
- sending (24'), to the serving network (2, 4; 12, 14), the first pseudonym in response to the first request for authentication information for use as an identifier for the mobile entity (6, 16) in the serving network (2, 12).

34. A method (70') for a communications network (1, 10) of protecting confidentiality of a first identifier associated by a first network node (5, 15) with a subscription used by a mobile entity (6, 16), the communications network (1, 10) comprising a home network (3, 13) of the mobile entity (6, 16) and a serving network (2, 12) serving the mobile entity (6, 16), the method (70') comprising:

- sending (71'), from the serving network (2, 4, 12, 14) to the home network (3, 5, 13, 15), a first request for authentication information for the mobile entity (6, 16), the first request comprising the first identifier,
- receiving (72'), from the home network (3, 5; 13, 15), a first pseudonym associated with the first identifier in response to the first request,
- creating (73') a link between a temporary identifier of the mobile entity (6, 16) and the first pseudonym, and
- using (74') the first pseudonym as identifier of the mobile entity (6, 16).

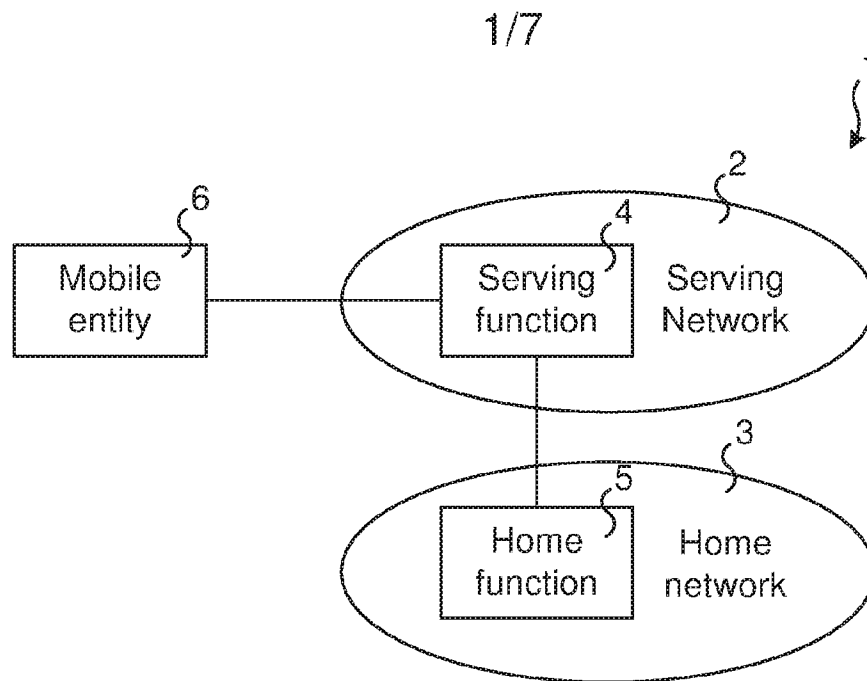


Fig. 1

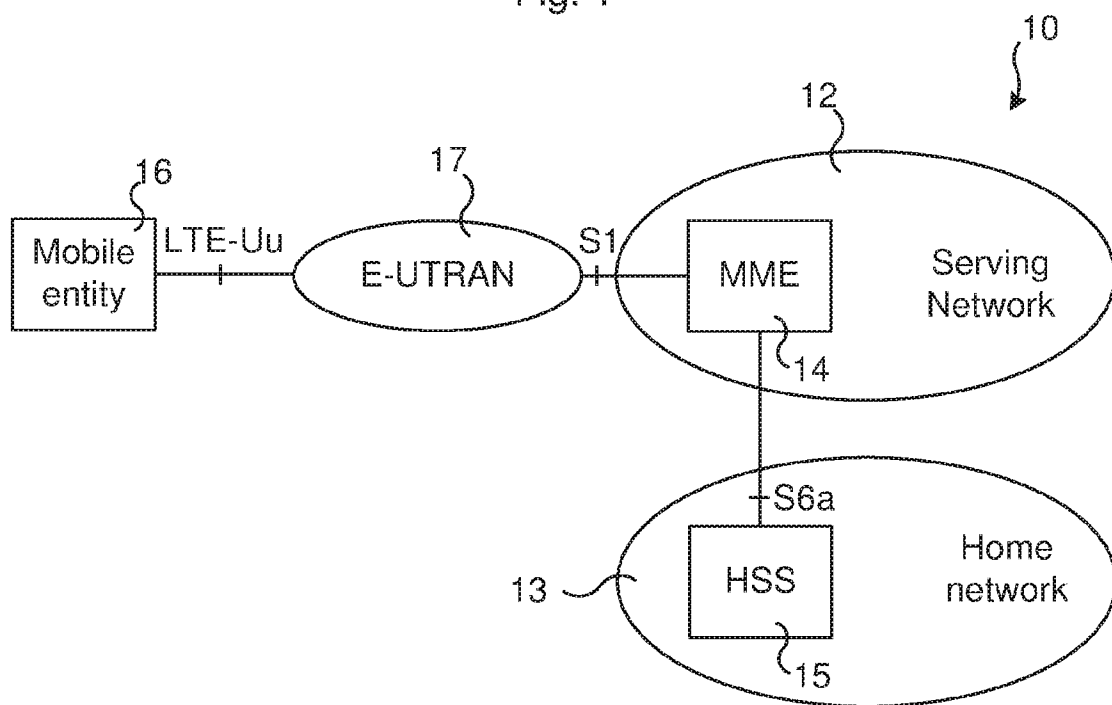


Fig. 2

2/7

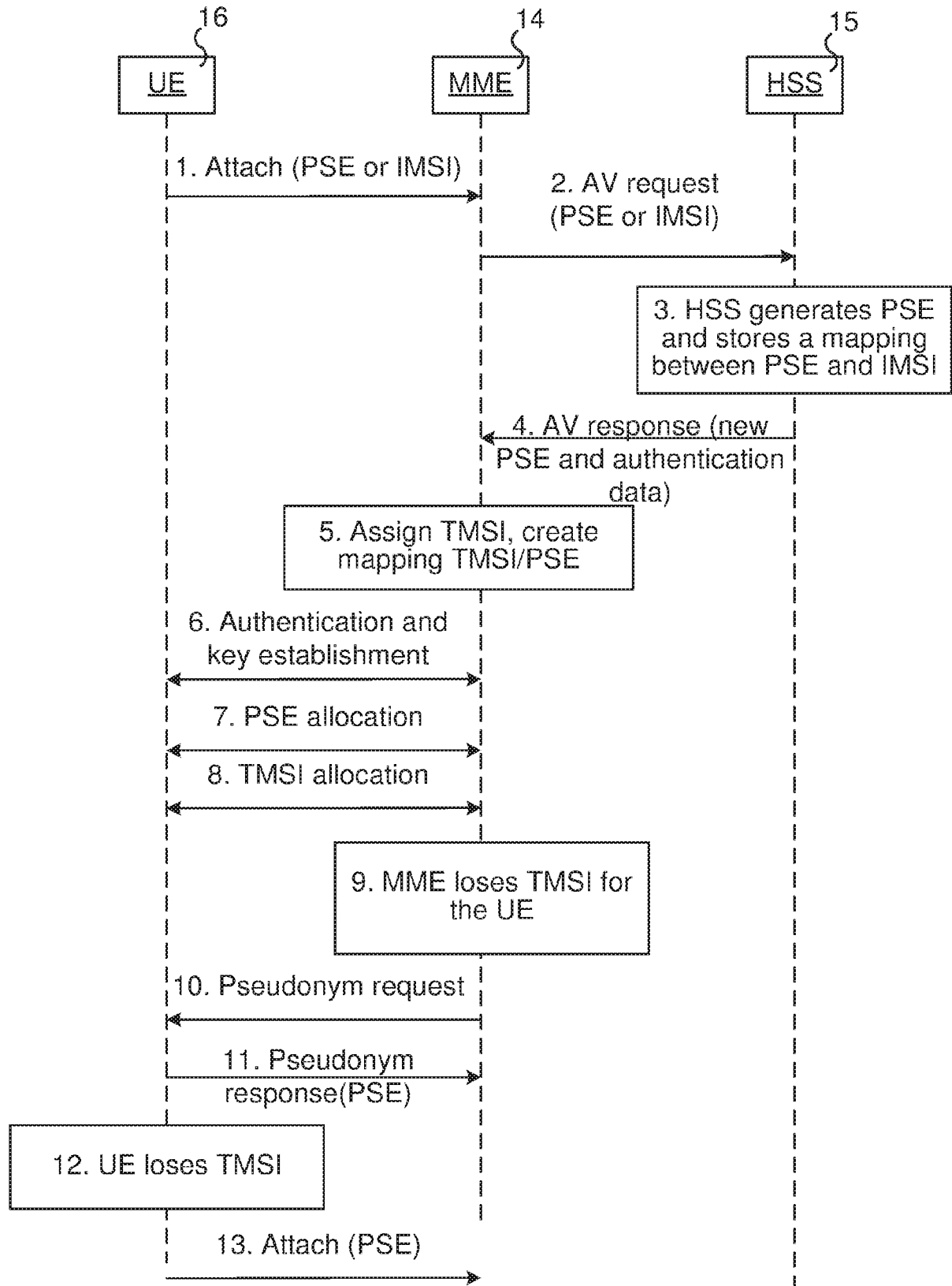


Fig. 3

3/7

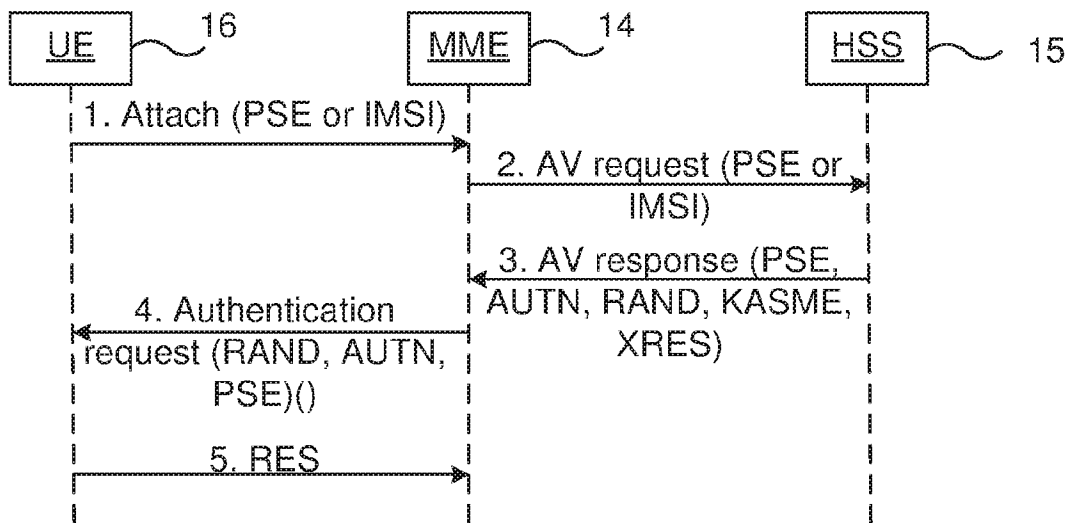


Fig. 4

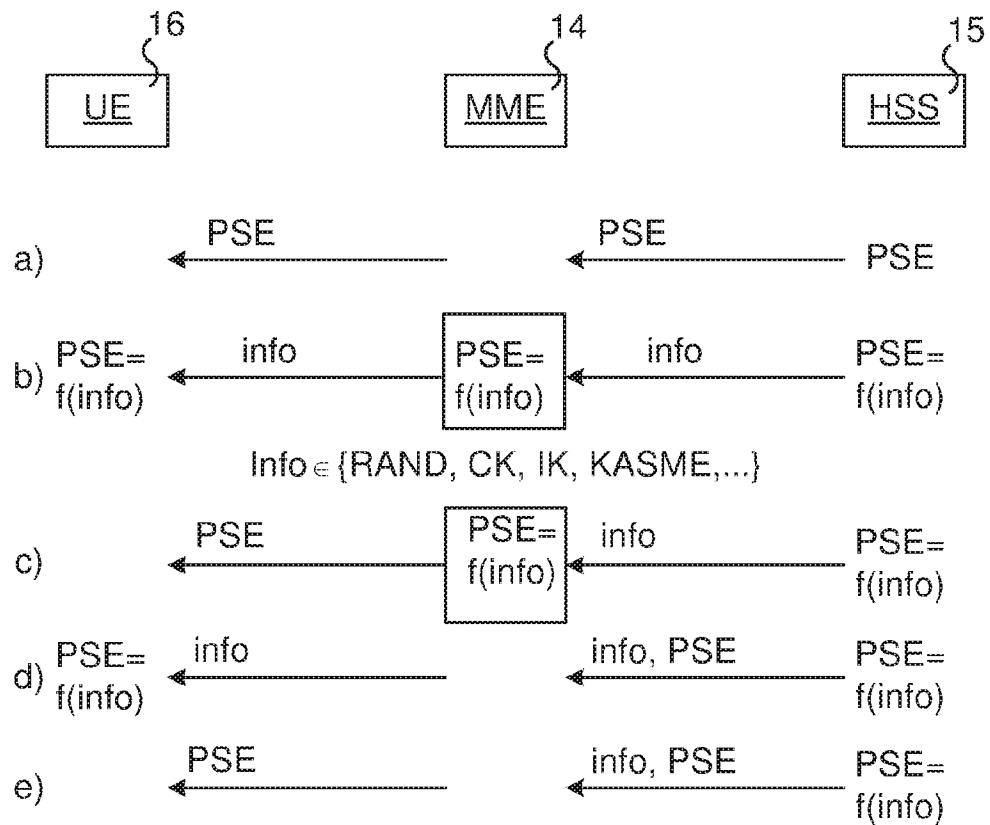


Fig. 5

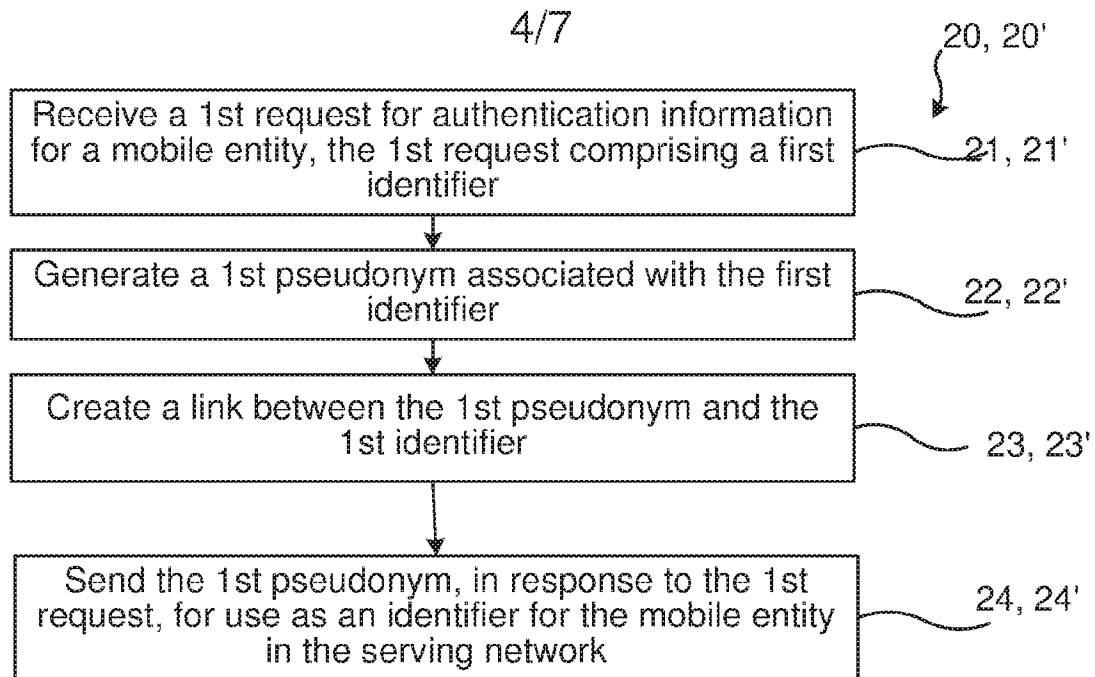


Fig. 6

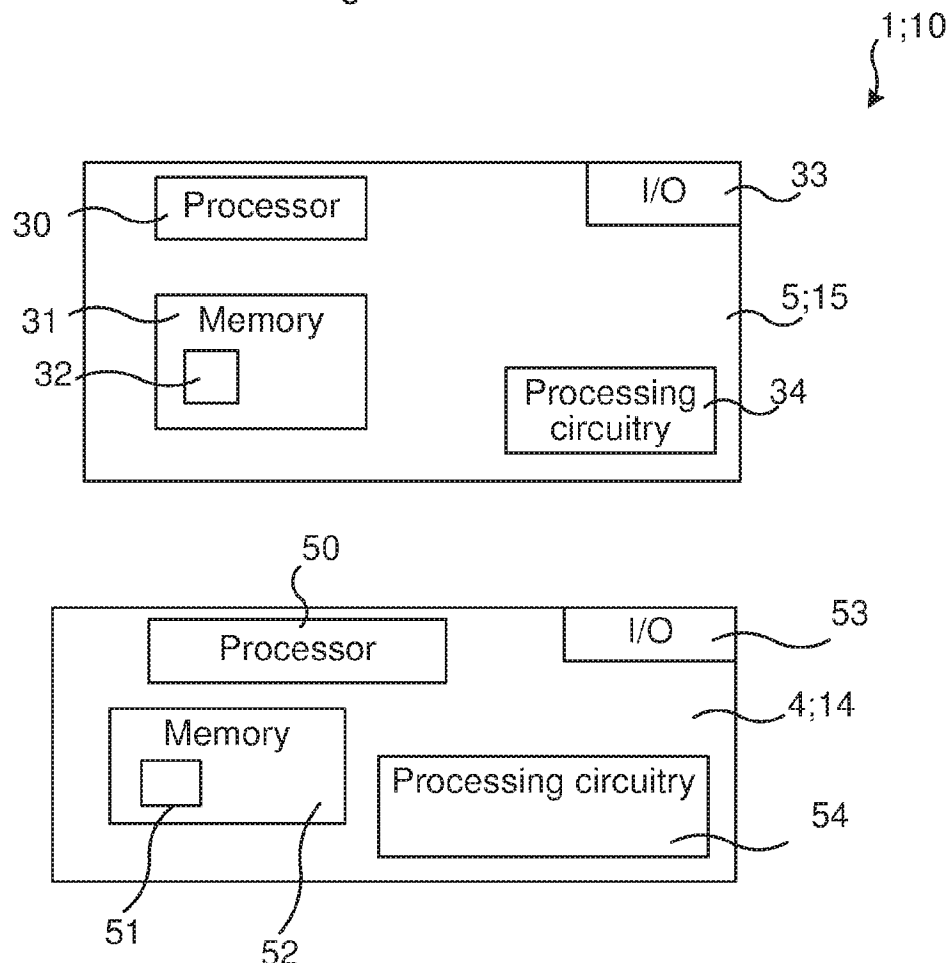


Fig. 7

5/7

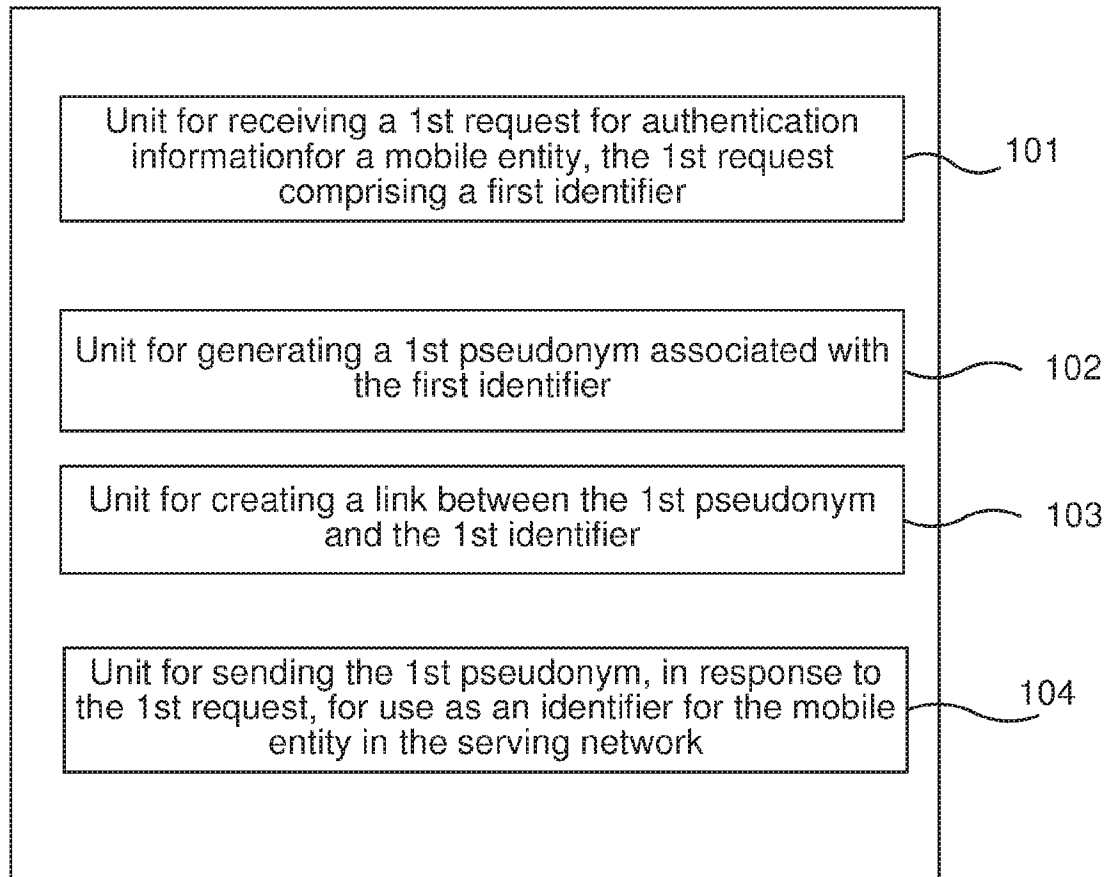


Fig. 8

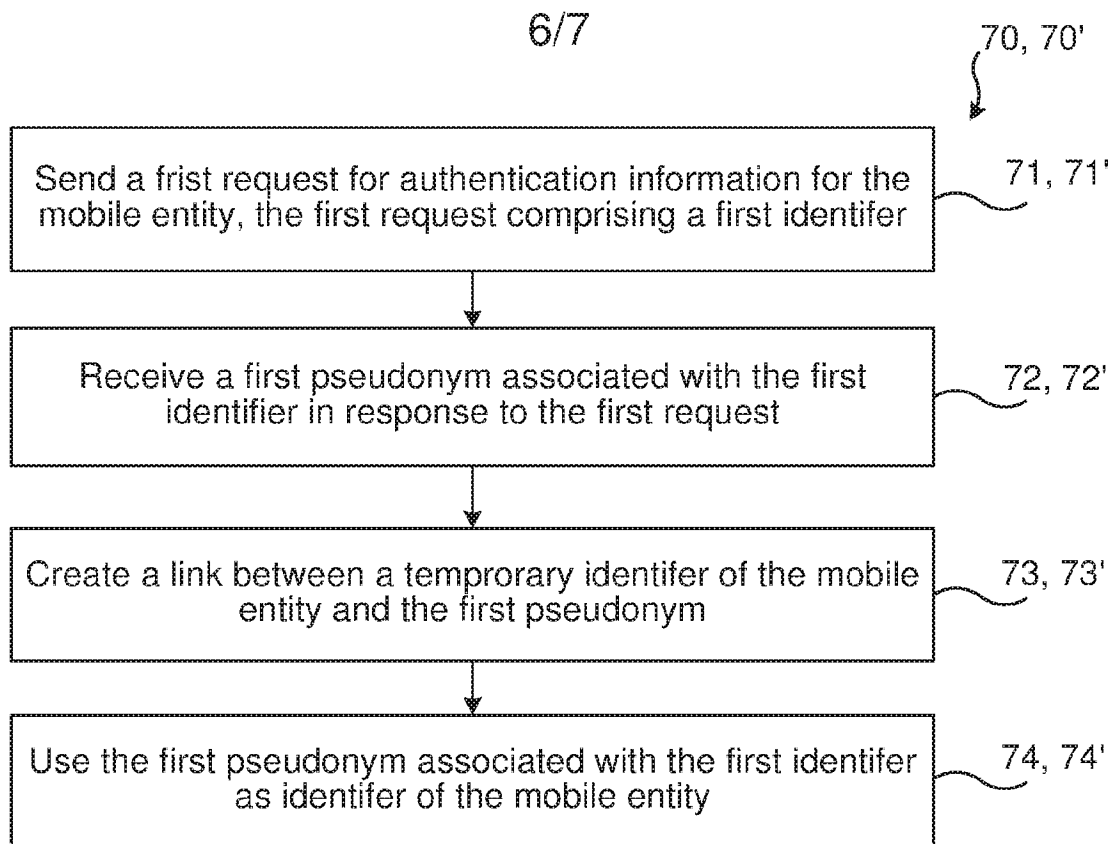


Fig. 9

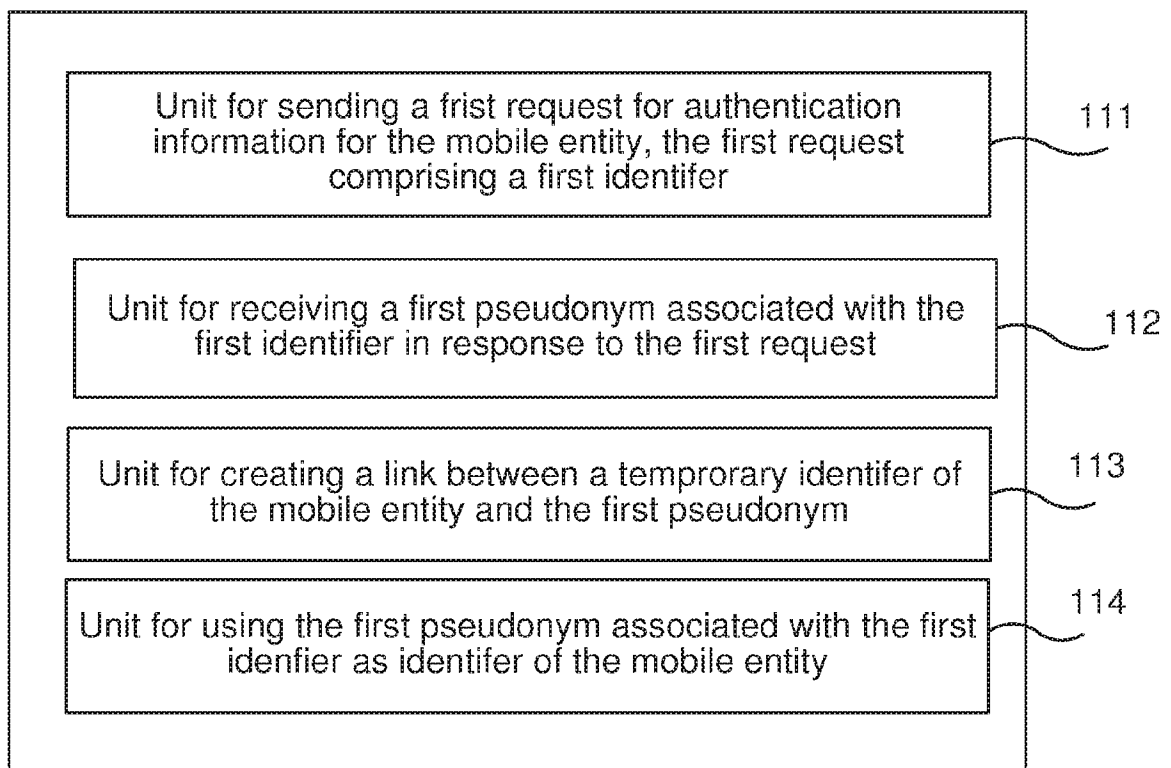


Fig. 10

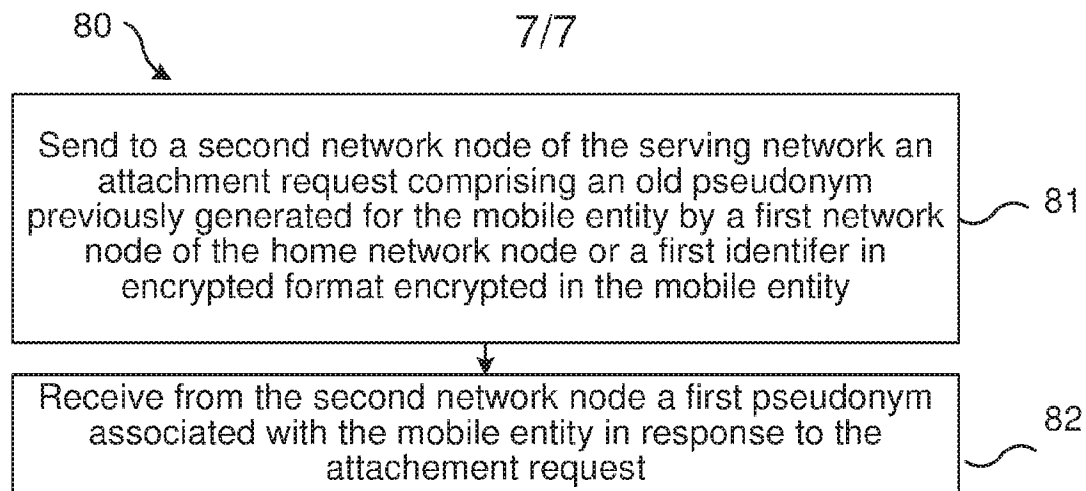


Fig. 11

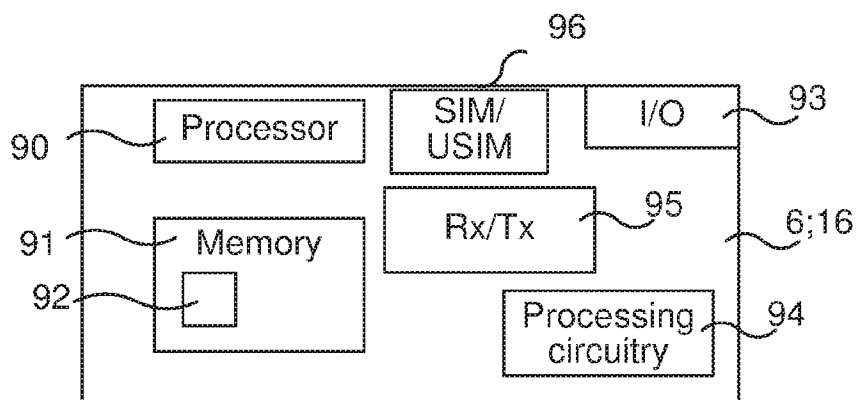


Fig. 12

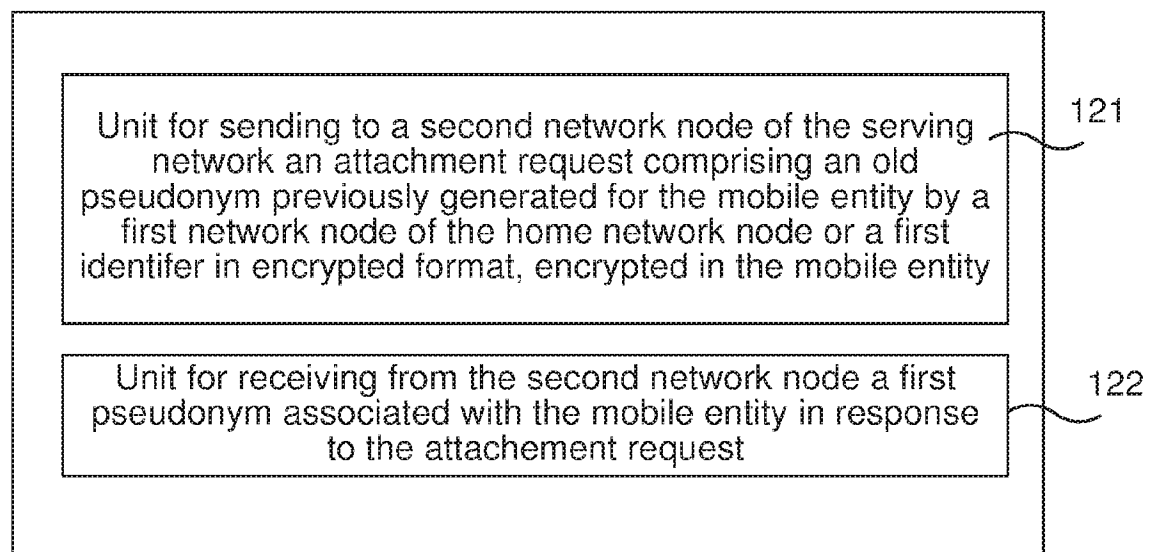


Fig. 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2015/050728

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L, H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE, DK, FI, NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, PAJ, WPI data, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2010012318 A1 (ERICSSON TELEFON AB L M ET AL), 4 February 2010 (2010-02-04); abstract; pages 1-4, 21-24; figure 5 --	1-34
A	3GPP TS 33.220, V12.3.0, (2014-06), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (Release 12).; figures 4.1a; Section 4.1 --	1-34
A	EP 2161963 A1 (HUAWEI TECH CO LTD), 10 March 2010 (2010-03-10); abstract; paragraphs [0084]-[0089] -- -----	1-34



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

08-02-2016

Date of mailing of the international search report

08-02-2016

Name and mailing address of the ISA/SE

Patent- och registreringsverket

Box 5055

S-102 42 STOCKHOLM

Facsimile No. + 46 8 666 02 86

Authorized officer

Ralf Boström

Telephone No. + 46 8 782 28 00

Continuation of: second sheet

International Patent Classification (IPC)

H04W 12/02 (2009.01)

H04L 9/32 (2006.01)

H04W 8/26 (2009.01)

H04W 12/06 (2009.01)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/SE2015/050728

WO	2010012318 A1	04/02/2010	EP	2308254 A1	13/04/2011
			US	20110126017 A1	26/05/2011
			US	8750506 B2	10/06/2014
EP	2161963 A1	10/03/2010	CN	101355793 A	28/01/2009
			EP	2621204 A1	31/07/2013
			EP	2528366 B1	08/01/2014
			EP	2442599 B1	03/04/2013
			ES	2397964 T3	12/03/2013
			ES	2414648 T3	22/07/2013
			ES	2455669 T3	16/04/2014
			JP	2014090450 A	15/05/2014
			JP	2014241651 A	25/12/2014
			JP	5628995 B2	19/11/2014
			JP	5835757 B2	24/12/2015
			JP	5432314 B2	05/03/2014
			JP	2012142991 A	26/07/2012
			JP	2010534961 A	11/11/2010
			JP	5010029 B2	29/08/2012
			US	8903389 B2	02/12/2014
			US	8200220 B2	12/06/2012
			US	8428590 B2	23/04/2013
			US	8238909 B2	07/08/2012
			US	20140038603 A1	06/02/2014
			US	20140038602 A1	06/02/2014
			US	20130217388 A1	22/08/2013
			US	20120270589 A1	25/10/2012
			US	20120028640 A1	02/02/2012
			US	20100120399 A1	13/05/2010
			WO	2009015595 A1	05/02/2009

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

To:

Ericsson
Patent Development
Torshamnsgatan 21-23
164 80 Stockholm
SUEDE

NOTIFICATION OF TRANSMITTAL OF
THE INTERNATIONAL SEARCH REPORT AND
THE WRITTEN OPINION OF THE INTERNATIONAL
SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Date of mailing (day/month/year) 7 November 2018 (07-11-2018)	
Applicant's or agent's file reference P72588 WO1	FOR FURTHER ACTION See paragraphs 1 and 4 below
International application No. PCT/EP2018/069432	International filing date (day/month/year) 17 July 2018 (17-07-2018)
Applicant TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)	

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

Filing of amendments and statement under Article 19:

The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

How? Directly to the International Bureau of WIPO, 34 chemin des Colombettes
1211 Geneva 20, Switzerland, Facsimile No.: (41-22) 338.82.70

For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 - 9.011.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

☐ the protest together with the decision thereon has been transmitted to the International Bureau together with any applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. Reminders

The applicant may **submit comments on an informal basis on the written opinion of the International Searching Authority** to the International Bureau. These comments will be made available to the public after international publication. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established.

Shortly after the expiration of **18 months from the priority date, the international application will be published** by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for **entry into the national phase** before those designated Offices. In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months. For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

Within **22 months from the priority date, the applicant may request that a supplementary international search be carried out** by a different International Searching Authority that offers this service (Rule 45*bis*.1). The procedure for requesting supplementary international search is described in the *PCT Applicant's Guide*, International Phase, paragraphs 8.006-8.032.

Name and mailing address of the International Searching Authority



European Patent Office, P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk
Tel. (+31-70) 340-2040
Fax: (+31-70) 340-3016

Authorized officer

SARDJOE, Irene
Tel: +31 (0)70 340-3273

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference P72588 WO1	FOR FURTHER ACTION see Form PCT/ISA/220 as well as, where applicable, item 5 below.	
International application No. PCT/EP2018/069432	International filing date (<i>day/month/year</i>) 17 July 2018 (17-07-2018)	(Earliest) Priority Date (<i>day/month/year</i>) 25 July 2017 (25-07-2017)
Applicant TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 5 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

a. With regard to the **language**, the international search was carried out on the basis of:

- ☒ the international application in the language in which it was filed
☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6**bis**(a)).

c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. ☐ **Certain claims were found unsearchable** (See Box No. II)

3. ☐ **Unity of invention is lacking** (see Box No. III)

4. With regard to the **title**,

- ☒ the text is approved as submitted by the applicant
☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

- ☒ the text is approved as submitted by the applicant
☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings**,

- a. the figure of the **drawings** to be published with the abstract is Figure No. 6
☒ as suggested by the applicant
☐ as selected by this Authority, because the applicant failed to suggest a figure
☐ as selected by this Authority, because this figure better characterizes the invention
b. ☐ none of the figures is to be published with the abstract

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2018/069432

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L29/06 H04W12/02 H04W12/06 H04W12/04
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EP0-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2016/209126 A1 (ERICSSON TELEFON AB L M [SE]) 29 December 2016 (2016-12-29)	16-35, 39-47
Y	abstract page 12, line 12 - page 13, line 6 figure 3	1-15, 36-38, 48,49
X	US 2013/003971 A1 (FORSBERG DAN [FI] ET AL) 3 January 2013 (2013-01-03)	16-35, 39-47
Y	abstract paragraph [0043] - paragraph [0046] paragraph [0049] - paragraph [0051] paragraph [0054] - paragraph [0055] paragraph [0057] - paragraph [0061] figures 2, 3, 4, 6	1-15, 36-38, 48,49
	----- -/--	

☒ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

24 October 2018

Date of mailing of the international search report

07/11/2018

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Poppe, Fabrice

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2018/069432

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	3RD GENERATION PARTNERSHIP PROJECT: "Study on the security aspects of the next generation system (Release 14)", TR 33.899 V1.2.0 , 21 June 2017 (2017-06-21), XP051310297, Retrieved from the Internet: URL: http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_87_Ljubljana/Docs/[retrieved on 2017-06-21] 5.7.3.2 Key issue #7.2: Concealing permanent or long-term subscription identifier 5.7.4.3 Solution #7.3: Concealing permanent or long-term subscriber identifier by using pseudonyms and public key encryption 5.7.4.15 Solution #7.15: Encrypting IMSI based on Elliptic Curve Integrated Encryption Scheme (ECIES) -----	1-49
A	3RD GENERATION PARTNERSHIP PROJECT: "Security Architecture and Procedures for 5G System (Release 15)", 3RD GENERATION PARTNERSHIP PROJECT, 15 June 2017 (2017-06-15), XP051298603, 3GPP TS 33.501 V0.2.0 [retrieved on 2017-06-15] cited in the application 6.8 Subscriber identifier privacy -----	1-49
X,P	NOKIA: "UDM and SIDF discovery", 3GPP DRAFT; S3-180767 UDM - SIDF DISCUSSION IMPLEMENTED IN PCR -V1, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRA , vol. SA WG3, no. San Diego (US); 20180226 - 20180302 19 February 2018 (2018-02-19), XP051409179, Retrieved from the Internet: URL: http://www.3gpp.org/ftp/tsg%5Fsa/WG3%5FSecurity/TSGS3%5F90Bis%5FSanDiego/Docs/[retrieved on 2018-02-19] the whole document ----- -/--	1-49

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2018/069432

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	ERICSSON: "Clause 6.12.5 (NF discovery with SUCI)", 3GPP DRAFT; S3-180824, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. SA WG3, no. San Diego (US); 20180226 - 20180302 19 February 2018 (2018-02-19), XP051409235, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/tsg%5Fsa/WG3%5FSecurity/TSGS3%5F90Bis%5FSanDiego/Docs/ [retrieved on 2018-02-19] the whole document -----	1-49

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2018/069432

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2016209126 A1	29-12-2016	NONE	

US 2013003971 A1	03-01-2013	EP 1873998 A1	02-01-2008
		US 2008002829 A1	03-01-2008
		US 2013003971 A1	03-01-2013

Information on Search Strategy - Pilot phase (see OJ 2015, A86)

The type of information contained in this sheet may change during the pilot for improving the usefulness of this new service.

Application Number

PCT/EP2018/069432

TITLE: SUBSCRIPTION CONCEALED IDENTIFIER

APPLICANT: TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)

IPC CLASSIFICATION: H04L29/06, H04W12/02, H04W12/06, H04W12/04

EXAMINER: Poppe, Fabrice

CONSULTED DATABASES: NPL, EPODOC, XP3GPP

CLASSIFICATION SYMBOLS DEFINING EXTENT OF THE SEARCH:

IPC:

CPC: H04L63/0414, H04W12/02, H04L2209/42, H04W12/06

FI/F-TERMS:

KEYWORDS OR OTHER ELEMENTS FEATURING THE INVENTION:

public-key encrypted SUPI, Subscription Identifier Deconcealing Function, SIDF, SUCI, encrypted part, clear-text part, home network identifier, encryption scheme identifier, SIDF selection

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

PCT

To:

see form PCT/ISA/220

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY (PCT Rule 43bis.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.
PCT/EP2018/069432

International filing date (day/month/year)
17.07.2018

Priority date (day/month/year)
25.07.2017

International Patent Classification (IPC) or both national classification and IPC
INV. H04L29/06 H04W12/02 H04W12/06 H04W12/04

Applicant
TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☒ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☒ Box No. VI Certain documents cited
- ☒ Box No. VII Certain defects in the international application
- ☒ Box No. VIII Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA:



European Patent Office
P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk - Pays Bas
Tel. +31 70 340 - 2040
Fax: +31 70 340 - 3016

Date of completion of
this opinion

see form
PCT/ISA/210

Authorized Officer

Poppe, Fabrice

Telephone No. +31 70 340-0



Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:
 - ☒ the international application in the language in which it was filed.
 - ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).
2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))
3. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing:
 - a. ☐ forming part of the international application as filed:
 - ☐ in the form of an Annex C/ST.25 text file.
 - ☐ on paper or in the form of an image file.
 - b. ☐ furnished together with the international application under PCT Rule 13ter.1(a) for the purposes of international search only in the form of an Annex C/ST.25 text file.
 - c. ☐ furnished subsequent to the international filing date for the purposes of international search only:
 - ☐ in the form of an Annex C/ST.25 text file (Rule 13ter.1(a)).
 - ☐ on paper or in the form of an image file (Rule 13ter.1(b) and Administrative Instructions, Section 713).
4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that forming part of the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5. Additional comments:

Box No. II Priority

1. ☒ The validity of the priority claim has not been considered because the International Searching Authority does not have in its possession a copy of the earlier application whose priority has been claimed or, where required, a translation of that earlier application. This opinion has nevertheless been established on the assumption that the relevant date (Rules 43bis.1 and 64.1) is the claimed priority date.
2. ☐ This opinion has been established as if no priority had been claimed due to the fact that the priority claim has been found invalid (Rules 43bis.1 and 64.1). Thus for the purposes of this opinion, the international filing date indicated above is considered to be the relevant date.
3. Additional observations, if necessary:

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	<u>1-49</u>
	No: Claims	
Inventive step (IS)	Yes: Claims	
	No: Claims	<u>1-49</u>
Industrial applicability (IA)	Yes: Claims	<u>1-49</u>
	No: Claims	

2. Citations and explanations

see separate sheet

Box No. VI Certain documents cited

1. Certain published documents (Rules 43bis.1 and 70.10)

and / or

2. Non-written disclosures (Rules 43bis.1 and 70.9)

see form 210

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

Re Item V

**Reasoned statement with regard to novelty, inventive step or industrial
applicability; citations and explanations supporting such statement**

- 1 Reference is made to the following documents:
 - D1 WO 2016/209126 A1 (ERICSSON TELEFON AB L M [SE]) 29 December 2016 (2016-12-29)
 - D2 US 2013/003971 A1 (FORSBERG DAN [FI] ET AL) 3 January 2013 (2013-01-03)
 - D3 3RD GENERATION PARTNERSHIP PROJECT: "Study on the security aspects of the next generation system (Release 14)", TR 33.899 V1.2.0, 21 June 2017 (2017-06-21)
- 2 The present application does not meet the criteria of Article 33(3) PCT, because the subject-matter of independent method claims 1, 16 and 24, in as far as said claims are clear (see Re Item VIII below) does not involve an inventive step.
- 2.1 Claim 1 relates to a method performed by an authentication server in a home network of a user equipment. Document D1 is regarded as being the prior art closest to the subject-matter of this claim, and discloses (the references in parentheses applying to this document):
 - a method performed by an authentication server (HSS 15) in a home network of a user equipment, UE (UE 16), for obtaining a subscription permanent identifier, SUPI (IMSI), the method comprising (page 12, lines 13-15: encryption of the IMSI by a public key of the home network 13 may in such cases be used to prevent the IMSI from being eavesdropped during transit of the IMSI from the UE 16 to the HSS 15): receiving a subscription concealed identifier, SUCI, which comprises an encrypted part in which at least a part of the SUPI is encrypted, and a clear-text part which comprises a home network identifier (page 12, lines 15-18: UE 16 may for instance encrypt part of the IMSI, e.g. encrypt the MSIN part of the IMSI using the public key of the home network 13 whereas MCC and MNC parts of the IMSI may be kept un-encrypted);

obtaining the SUPI from the SUCI (page 12, lines 28-29: decryption of IMSI by HSS 15).

The subject-matter of claim 1 therefore differs from this known method in that:

- (i) the clear-text part of the SUCI comprises an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI,

and in that obtaining the SUPI from the SUCI comprises:

- (ii) determining a de-concealing server to use to decrypt the encrypted part of the SUCI,
- (iii) sending the SUCI to the de-concealing server, and
- (iv) receiving the SUPI in response.

The subject-matter of claim 1 is therefore new.

The objective technical problem corresponding to distinguishing feature (i) may be regarded as how to support a plurality of encryption schemes.

Corresponding feature (i) is considered to comprise a matter of normal design. The skilled person indeed knows that in connection with concealing subscription identifiers a plurality of encryption schemes may be standardized from D3 (section 5.7.4.3 Solution #7.3),

It is in the scope of the security area #17 'Cryptographic algorithms' to decide if and which public key encryption schemes to standardize.

It appears to be a matter of normal design to include an encryption scheme identifier in the SUCI to allow the determination of the encryption scheme to be used by the de-concealing server.

In D1, the authentication server itself decrypts the encrypted part of the SUCI to obtain the SUPI from the SUCI. The distinguishing features (ii)-(iv) may therefore be regarded to define an alternative solution to the objective technical problem of how to obtain the SUPI from the SUCI. In the same technical field, document D2 discloses features (ii)-(iv), see paragraphs [0044]-[0046], [0049]-[0051], [0054]-[0055] and Figs. 2 and 4:

second network entity (MME 43 of the home network 42) maintains information that is needed in the decryption,

determination of the second network entity based on information the (first, requesting) entity can gather from the identifier that was received from the user equipment (visited mobile management entity may analyse the mobile country code (MCC) and/or mobile network code (MNC) of the IMSI),

second or home entity may then decrypt the message based on information stored in a data storage thereof and return the identifier in decrypted format to the requesting entity (the home mobile management entity decrypts the MSIN part and send the IMSI in a clear text format back to the visited mobile management entity).

The skilled person would, starting from the teaching of D1, apply these features disclosed in D2, with corresponding technical effect, and thereby arrive at the subject-matter of claim 1 without performing any inventive activity. One may even argue that the visited MME 33 of D2, Fig. 4, which relies on the home MME 43 as a de-concealing server, in fact also is an authentication server, since it performs an authentication procedure for registering a user equipment, see paragraph [0043] of D2.

- 2.2 Claim 16 relates to a corresponding method performed by a de-concealing server. Document D2 is regarded as being the prior art closest to the subject-matter of this claim, and discloses (the references in parentheses applying to this document):

a method, performed by a de-concealing server (Fig. 4: home mobile management entity), for providing a subscription permanent identifier, SUPI, the method comprising:

receiving a subscription concealed identifier, SUCI, which comprises an encrypted part in which at least a part of the SUPI is encrypted, and a clear-text part which comprises a home network identifier (paragraph [0051] the visited mobile management entity asks the home mobile management entity to decrypt the IMSI on its behalf; paragraph [0049] at least the mobile subscriber identification number (MSIN) part of the IMSI may be transmitted as encrypted over the air interface);

decrypting the encrypted part of the SUCI, using the encryption scheme indicated by the encryption scheme identifier to obtain the SUPI (paragraph [0051] decrypt the encrypted portions of the IMSI identifier);
and

sending the SUPI (paragraph [0054] the home mobile management entity can then decrypt the MSIN part and send the IMSI in a clear text format back to the visited mobile management entity).

The subject-matter of claim 16 therefore differs from this known method in that:

(i) the clear-text part of the SUCI comprises an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI and which is supported by the de-concealing server,

and in that

(ii) the subscription concealed identifier, SUCI, is received from an authentication server, and

(iii) the obtained subscription permanent identifier, SUPI is sent to the authentication server.

The subject-matter of claim 1 is therefore new.

The objective technical problem corresponding to distinguishing feature (i) may be again be regarded as how to support a plurality of encryption schemes. Corresponding feature (i) is again considered to comprise a matter of normal design (see point 2.1 above).

Features (ii) and (iii) merely specify that the de-concealing server serves an authentication server. No structural adaptation of the de-concealing server known from D2 is required to this end, and no objective technical problem corresponding to these features can be identified. One may even argue that the visited MME 33 of D2, Fig. 4, which relies on the home MME 43 as a de-concealing server, in fact also is an authentication server, since it performs an authentication procedure for registering a user equipment, see paragraph [0043] of D2.

2.3 Claim 24 relates to a corresponding method performed by a user equipment. Document D1 is regarded as being the prior art closest to the subject-matter of this claim, and discloses (the references in parentheses applying to this document):

a method performed by a user equipment, UE, the method comprising:
generating a subscription concealed identifier, SUCI, which comprises an encrypted part in which at least a part of a subscription permanent identifier, SUPI, is encrypted (page 12, lines 15-18: UE 16 may for

instance encrypt part of the IMSI, e.g. encrypt the MSIN part of the IMSI using the public key of the home network 13 whereas MCC and MNC parts of the IMSI may be kept un-encrypted);

transmitting the SUCI to an authentication server (page 12, lines 13-15: encryption of the IMSI by a public key of the home network 13 may in such cases be used to prevent the IMSI from being eavesdropped during transit of the IMSI from the UE 16 to the HSS 15) for forwarding of the SUCI to a de-concealing server capable of decrypting the SUPI.

The subject-matter of claim 24 therefore differs from this known method in that:

- (i) the clear-text part of the SUCI comprises an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI,

The subject-matter of claim 24 is therefore new.

The objective technical problem corresponding to distinguishing feature (i) may be regarded as how to support a plurality of encryption schemes. Corresponding feature (i) is again considered to comprise a matter of normal design (see point 2.1 above).

It is noted that the subject-matter of claim 24 furthermore does not comprise an inventive step over D2, see the corresponding passages cited in the search report.

- 2.4 The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent claims 36-38, 39-41, 42-44, 48 and 49, which therefore are also considered not inventive.
- 3 Dependent claims 2-15, 17-23, 25-35 and 45-47 do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty and/or inventive step.

Re Item VII

Certain defects in the international application

- 1 The independent claims are not in the two-part form in accordance with Rule 6.3(b) PCT, which in the present case would be appropriate, with those features known in combination from the prior art being placed in the preamble (Rule 6.3(b)(i) PCT) and the remaining features being included in the characterising part (Rule 6.3(b)(ii) PCT).
- 2 Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in D1 and D2 is not mentioned in the description, nor are these documents identified therein.

Re Item VIII

Certain observations on the international application

- 1 Although claims 36, 37 and 38, all directed to an authentication server for a home network, have been drafted as separate independent claims, they appear to relate effectively to the same subject-matter and to differ from each other only with regard to the definition of the subject-matter for which protection is sought and/or in respect of the terminology used for the features of that subject-matter. The aforementioned claims therefore lack conciseness and as such do not meet the requirements of Article 6 PCT.

Also claims 39-41 directed to deconcealing servers, and claims 42-44 directed to user equipments, lack conciseness and as such do not meet the requirements of Article 6 PCT.
- 2 Claims 24 and 42-44 furthermore lack clarity. It is not clear how the forwarding by the authentication server of the SUCI to a de-concealing server capable of decrypting the SUPI can comprise a limitation of the claimed user equipments and the corresponding method performed by the user equipments.

POWER OF ATTORNEY

The undersigned, being duly authorized representatives of **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)** (hereinafter referred to as "Ericsson") having its registered office at SE-164 83 Stockholm, Sweden, does hereby authorize **Rothwell, Figg, Ernst & Manbeck, P.C.** practitioners associated with United States Patent and Trademark Office Customer Number 06449 to represent Ericsson before the United States Patent and Trademark Office in any and all matters regarding patents or patent applications filed by Ericsson or wherein Ericsson is the assignee of the entire interest thereto.

This Power of Attorney shall include the right for **Rothwell, Figg, Ernst & Manbeck, P.C.** practitioners associated with United States Patent and Trademark Office Customer Number 06449 to sign and submit in Ericsson's name and on Ericsson's behalf any document, notification, filing, petition or request in connection with any patent applications or patents owned by or assigned to Ericsson.

This Power of Attorney does not include the right to appoint substitutes but only the persons associated with the above United States Patent and Trademark Office Customer Number.

We hereby revoke all previous authorization, if any made, in respect of same matter or proceeding. This Power of Attorney shall be valid for five (5) years from the date hereof unless earlier revoked. This Power of Attorney may be revoked at any time by Ericsson.

Stockholm, Sweden on [Date] 2016-04-05

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)

Signature(s)

Gabriele Mohsler
Vice President Patent Development

Nabil Ayoub
Director Patent Unit RAN2

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)Applicant/Patent Owner: Telefonaktiebolaget LM Ericsson (publ)Application No./Patent No.: 16/200037Filed/Issue Date: November 26, 2018Titled: SUBSCRIPTION CONCEALED IDENTIFIERTelefonaktiebolaget LM Ericsson (publ), a corporation

(Name of Assignee)

(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☒ The assignee of the entire right, title, and interest.
2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):
- ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.
- ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (e.g., bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

- A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.
- B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:
1. From: _____ To: _____
- The document was recorded in the United States Patent and Trademark Office at
- Reel _____, Frame _____, or for which a copy thereof is attached.
2. From: _____ To: _____
- The document was recorded in the United States Patent and Trademark Office at
- Reel _____, Frame _____, or for which a copy thereof is attached.

[Page 1 of 2]

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
 Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☒ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Brian S. Rosenbloom/

December 6, 2018

Signature

Date

Brian S. Rosenbloom

41276

Printed or Typed Name

Title or Registration Number

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ASSIGNMENT

This Assignment is made by:

BEN HENDA, Noamen

**Tumultgränd 228
SE-162 47 Stockholm
Sweden**

CASTELLANOS ZAMORA, David

**C/ Embajadores 256, 1ºB
28045 MADRID
Spain**

NAKARMI, Prajwol Kumar

**Stupvägen 17
SE-19142 SOLLENTUNA
Sweden**

SAARINEN, Pasi

**Ripvägen 19A
17564 Järfälla
Sweden**

WIFVESSON, Monica

**Kruthornsgränden 3
226 52 LUND
Sweden**

(hereinafter referred to as "Assignor(s)") in favor, and for the benefit and behoof of, Telefonaktiebolaget LM Ericsson (publ), a corporation duly organized under and pursuant to the laws of Sweden and having its principal place of business at SE-164 83 Stockholm, Sweden (hereinafter referred to as "Assignee").

For good, sufficient and adequate consideration, the receipt of which is hereby acknowledged, the Assignor(s) have, as of the Effective Date, sold, assigned, transferred, and set over, and by these presents, and to the extent any transferable or assignable rights still remain with the inventor, do hereby sell, assign, transfer, and set over, unto the Assignee, its successors, legal representatives, and assigns the entire right, title, and interest in and to the following inventions, application(s) for Letters Patent, and any and all Letters Patent or Patents in all countries and pursuant to all multilateral treaty organizations, including Sweden, the United States of America, the Patent Cooperation Treaty and European Patent Convention, that may be granted therefor and thereon, and in and to any and all divisions, continuations, continuations-in-part, conversions and utility models of said application(s), and reissues and extensions of said Letters Patent or Patents, the same to be held and enjoyed by the Assignee, for its use and behoof and the use and the behoof of its successors, legal representatives, and assigns, to the full end of the term or terms for which Letters Patent, Patents and Utility Models may be granted as fully and entirely as the same would have been held and enjoyed by the Assignor(s) had this sale and assignment not been made:

ASSIGNMENT

SUBSCRIPTION CONCEALED IDENTIFIER

including, but not limited to, the application(s) for Letters Patent and Utility Model filed in:

Country Code	Priority Application(s)	Filing Date(s)
WO	PCT/EP2018/069432	2018-07-17
US	16/200037	2018-11-26

The Effective date is the earliest date of the above listed Filing Date(s).

Assignor(s) hereby authorize and request Assignee's Attorneys to insert the serial number and filing date of said application(s) for Letter Patent or Utility Model, when known. The assignment of the above mentioned rights includes a transfer of the whole right to use a priority (including priority according to any convention, multilateral agreement, bilateral agreement and national law) of the above mentioned application(s) for Letter Patent and Utility Model in all countries and multilateral treaty organizations wherein no residual rights shall remain with the Assignor(s). Assignor(s) hereby request that said Letters Patent, Patent or Utility Model be issued to Assignee as the Assignee of said inventions, the Letters Patent, Patent or Utility Model to be issued for the sole use and behoof of the Assignee, its successors, legal representatives, and assigns. Assignee alone hereinafter has the entire disposal of the invention and possesses entire ownership to any domestic and foreign patents or utility models granted thereafter. The rights granted hereunder shall include all rights to institute legal actions, obtain remedies and recover and retain damages in respect to said Letters Patent, Patent or Utility Model.

The Assignor(s) and Assignee hereby understand and agree that with the execution of this Assignment, to the extent necessary or appropriate, national and/or regional applications may be filed by the Assignee as the applicant and on behalf of the assignor.

To the extent Assignee is entitled to receive the rights hereunder pursuant to this Assignment, each of the Assignor(s) hereby covenants and agrees to and with the Assignee, its successors, legal representatives, and assigns, that, at the time of the Effective Date, the Assignor(s) were the sole and lawful owners of the entire right, title, and interest in and to the inventions and application(s) for Letters Patent or Utility Models above-mentioned, and that the same are unencumbered, and that the Assignor(s) have good and full right and lawful authority to sell and convey the same in the manner herein set forth.

Further, and for the same consideration, the Assignor(s) hereby covenant(s) and agree(s) to and with the Assignee, its successors, legal representatives, and assigns that the Assignor(s) will, whenever counsel of the Assignee, or the counsel of its successors, legal representatives, and assigns, shall advise that any proceeding in connection with said inventions or said application(s) for Letters Patent or Utility Model, or any proceeding in connection with Letters Patent or Utility Model for said inventions, in any country and any multilateral treaty organization, including interference proceedings, is lawful and desirable, or that any division, continuation, continuation-in-part, conversion or Utility Model of any application(s) for Letters Patent or Utility Model, or any reissue or extension of any Letters Patent to be obtained thereon, is lawful and desirable, sign all papers and documents, take all lawful oaths, and do all acts necessary or required to be done for the

ASSIGNMENT

procurement, maintenance, enforcement, and defense of Letters Patent, or Utility Model for said inventions, without charge to Assignee, its successors, legal representatives, and assigns, but at the cost and expense of the Assignee, its successors, legal representatives, and assigns. If any of the Assignor(s) is prevented by any obstacles from signing said documents in person, this Assignment shall be valid as a Power of Attorney for the Assignee to sign these documents on behalf of any such Assignor(s) or, in the event of the death of the latter, the estate thereof.

This Assignment shall be governed by and construed under, and any dispute, controversy or claim related hereto shall be decided in accordance with, the laws of:
Sweden

without regard to the conflicts of laws provisions thereof. Any dispute, controversy or claim arising under, out of or relating to this Assignment and any subsequent amendments of this Assignment, including, without limitation, its formation, validity, binding effect, interpretation, performance, breach or termination, as well as non-contractual claims, shall be referred to and finally determined by arbitration in accordance with the WIPO Arbitration Rules. The arbitral tribunal shall consist of a sole arbitrator. The place of arbitration shall be in the country of the inventor's residence. The language to be used in the arbitral proceedings shall be English.

No modifications shall be made to this Assignment unless in writing and signed by each of the Assignor(s) and Assignee. If any of the provisions of this Assignment shall be deemed invalid or unenforceable, then the entire Assignment shall be construed as if not containing the particular invalid or unenforceable provision or provisions, and the rights and obligations of Assignee and Assignor(s) shall be construed and enforced accordingly. Assignee's failure to exercise any option made available as a result hereof, shall not be construed as a waiver of such provisions, rights, or options, or affect the validity of this Assignment. Assignor covenants and agrees that it will not take any actions in violation of this Assignment.

Subsequent assignment from any of the assignors to the assignee purporting to convey the subject matter specified herein for a particular country, patent office, or jurisdiction shall not invalidate any provision of this assignment and any such subsequent assignment shall act as a further confirmation of the assignment herein.

Date 5 October 2018 Signature on behalf of Fredrik Egrelius
Assignee

Patent Unit Director

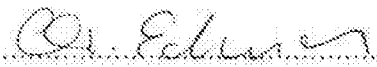
ASSIGNMENT

Title: SUBSCRIPTION CONCEALED IDENTIFIER

Date 2018-10-01 Signature of Assignor
BEN HENDA, NoamenDate 2018-10-01 Witnessed by

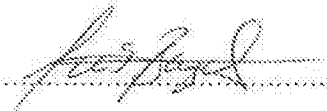
Name:

Address:


Christine Edman
Färtickevägen 43
18434 Åkersberg
SWEDENDate 2018-10-01 Witnessed by

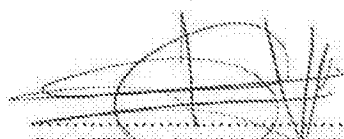
Name:

Address:


LUIS BARRIGA
Sjösavägen 15
12455 Bandhagen
Sweden

ASSIGNMENT

Title: SUBSCRIPTION CONCEALED IDENTIFIER

Date 19/07/2018 Signature of Assignor

 CASTELLANOS ZAMORA, David
Date 19/07/2018 Witnessed by

Name:


 JOSÉ MIGUEL DOPICO SANJUÁN

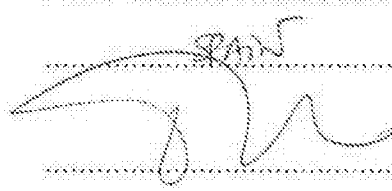
Address:

VIA DE LOS POBLADOS 13

MADRID 28033

Date 19/07/2018 Witnessed by

Name:


 TRINIDAD CASTAÑO CASERO

Address:

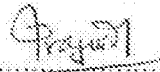
VIA DE LOS POBLADOS 13

MADRID 28033

SPAIN

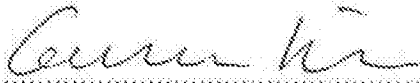
ASSIGNMENT

Title: SUBSCRIPTION CONCEALED IDENTIFIER

Date 23rd July 2018 Signature of Assignor

 NAKARMI, Prajwol Kumar
Date 23rd July 2018 Witnessed by

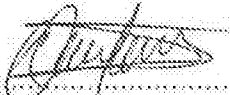
Name:

Address:


 Gunnar Mildh
 Koltrastvägen 28
 19255 SOLLENTUNA
 SWEDEN
Date 23rd July 2018 Witnessed by

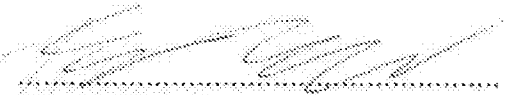
Name:

Address:


 Omer Teyeb
 Hundskogatan 30
 17144 SOLNA
 SWEDEN

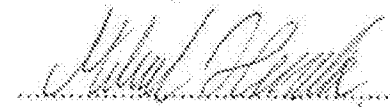
ASSIGNMENT

Title: SUBSCRIPTION CONCEALED IDENTIFIER

Date 2018-07-23 Signature of Assignor
SAARINEN, PasiDate 2018-07-23 Witnessed by

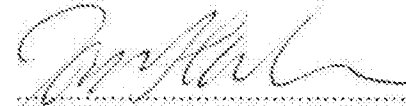
Name:

Address:


Mikael Herrala
Gårdsvägen 18
169 70 Solna
SWEDENDate 2018-07-23 Witnessed by

Name:

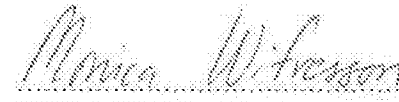
Address:


Jonas Hålen
Långdansvägen 1
196 37 Kungsängen
SWEDEN

ASSIGNMENT

Title: SUBSCRIPTION CONCEALED IDENTIFIER

Date: 2016-08-06 Signature of Assignor


 WIFVESSON, Monica

Date: 2018-08-06 Witnessed by

Name:

Address:


 PER LINDELL
 SÖMERVÄG 1241
 247 36 SÖDRA SANDBY
 SWEDEN

Date: 2018-08-06 Witnessed by

Name:

Address:


 CALLE HAGENFELDT
 FRODESÅTAN 2
 252 69 RÅK
 SWEDEN

ASSIGNMENT AGREEMENT

This Assignment is made by:

TORVINEN, Vesa

**Sauvontie 42
FI-21570 SAUVO
Finland**

(hereinafter referred to as "Assignor(s)") in favor, and for the benefit and behoof of, Oy L M Ericsson Ab, a corporation duly organized under and pursuant to the laws of Finland and having its principal place of business at Hirsalantie 11, 02420 Jorvas, Finland (hereinafter referred to as "Assignee").

The Assignor(s) have, as of the Effective Date, sold, assigned, transferred, and set over, and by these presents, and to the extent any transferable or assignable rights still remain with the inventor, do hereby sell, assign, transfer, and set over, unto the Assignee, its successors, legal representatives, and assigns the entire right, title, and interest in and to the following inventions, application(s) for any and all Letters Patent, Patents and Utility Model(s) in all countries and pursuant to all multilateral treaty organizations, including Finland, the United States of America, the Patent Cooperation Treaty and European Patent Convention, that may be granted therefor and thereon, and in and to any and all divisions, continuations, continuations-in-part, conversions and utility models of said application(s), and reissues and extensions of said Letters Patent, Patents or Utility Model(s), the same to be held and enjoyed by the Assignee, for its use and behoof and the use and the behoof of its successors, legal representatives, and assigns, to the full end of the term or terms for which Letters Patent, Patents and Utility Models may be granted as fully and entirely as the same would have been held and enjoyed by the Assignor(s) had this sale and assignment not been made:

SUBSCRIPTION CONCEALED IDENTIFIER

including, but not limited to, the application(s) for Letters Patent and Utility Model filed in:

Country Code	Priority Application(s)	Filing Date(s)
WO	PCT/EP2018/069432	2018-07-17
US	16/200037	2018-11-26
		- -

The Effective date is the earliest date of the above listed Filing Date(s).

This Assignment shall be subject to the laws of Finland and Ericsson Inventor Awards System valid at the time of the Assignors submitted the Applicable Notification Form to the Assignee. The Assignor(s) acknowledge that they are aware of the content and provisions of the Ericsson Inventor Awards System.

Assignor(s) hereby authorize and request Assignee's Attorneys to insert the serial number and filing date of said application(s) for Letter Patents, Patent or Utility Model, when known. The assignment of the above mentioned rights includes a transfer of the whole right to use a priority (including priority according to any convention, multilateral agreement, bilateral agreement and national law) of the above mentioned application(s) for Letter Patent, Patents and Utility Model in all countries and multilateral treaty organizations wherein no residual rights shall remain with the Assignor(s). Assignor(s)

ASSIGNMENT AGREEMENT

hereby request that said Letters Patent, Patents or Utility Model be issued to Assignee as the Assignee of said inventions, the Letters Patent, Patent or Utility Model to be issued for the sole use and behoof of the Assignee, its successors, legal representatives, and assigns. Assignee alone hereinafter has the entire disposal of the invention and possesses entire ownership to any domestic and foreign patents or utility models granted thereafter. The rights granted hereunder shall include all rights to institute legal actions, obtain remedies and recover and retain damages in respect to said Letters Patent, Patents or Utility Model.

The Assignor(s) and Assignee hereby understand and agree that with the execution of this Assignment, to the extent necessary or appropriate, national and/or regional applications may be filed by the Assignee as the applicant and on behalf of the Assignor(s).

The Assignor(s) hereby confirm that the remuneration to be paid to the Assignor(s) in accordance with the Ericsson Inventor Awards System, in addition to the salary of the Assignor(s) as such, constitute fair and reasonable compensation as defined in the Finnish Employee Inventions Act for the assignment an employee invention to the Assignee and that the Assignor(s) shall not have any other claims towards the Assignee. In connection with this the Assignor(s) and the Assignee have particularly taken into account the following factors: degree of readiness, scope of the invention and utilization of the invention. It has been taken into account that the invention may be used in or transferred to other Ericsson's group companies and there are also licensing possibilities.

To the extent Assignee is entitled to receive the rights hereunder pursuant to this Assignment, each of the Assignor(s) hereby covenants and agrees to and with the Assignee, its successors, legal representatives, and assigns, that, at the time of the Effective Date, the Assignor(s) were the sole and lawful owners of the entire right, title, and interest in and to the inventions and application(s) for Letters Patent, Patents or Utility Models above-mentioned, and that the same are unencumbered, and that the Assignor(s) have good and full right and lawful authority to sell and convey the same in the manner herein set forth.

Further, the Assignor(s) hereby covenant(s) and agree(s) to and with the Assignee, its successors, legal representatives, and assigns that the Assignor(s) will, whenever counsel of the Assignee, or the counsel of its successors, legal representatives, and assigns, shall advise that any proceeding in connection with said inventions or said application(s) for Letters Patent, Patents or Utility Models or any proceeding in connection with Letters Patent, Patents or Utility Model for said inventions, in any country and any multilateral treaty organization, including interference proceedings, is lawful and desirable, or that any division, continuation, continuation-in-part, conversion of any application(s) for Letters Patent, Patents or Utility Model, or any reissue or extension of any Letters Patent, Patents or Utility Model to be obtained thereon, is lawful and desirable, sign all papers and documents, take all lawful oaths, and do all acts necessary or required to be done for the procurement, maintenance, enforcement, and defense of Letters Patent, Patents or Utility Model for said inventions, without charge to Assignee, its successors, legal representatives, and assigns, but at the cost and expense of the Assignee, its successors, legal representatives, and assigns. If any of the Assignor(s) is prevented by any obstacles from signing said documents in person, this Assignment shall be valid as a Power of

ASSIGNMENT AGREEMENT

Attorney for the Assignee to sign these documents on behalf of any such Assignor(s) or, in the event of the death of the latter, the estate thereof.

This Assignment shall be governed by and construed under, and any dispute, controversy or claim related hereto shall be decided in accordance with, the laws of:

Sweden

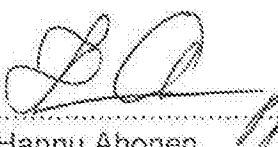
without regard to the conflicts of laws provisions thereof. Any dispute, controversy or claim arising under, out of or relating to this Assignment and any subsequent amendments of this Assignment, including, without limitation, its formation, validity, binding effect, interpretation, performance, breach or termination, as well as non-contractual claims, shall be referred to and finally determined by arbitration in accordance with the WIPO Arbitration Rules. The arbitral tribunal shall consist of a sole arbitrator. The place of arbitration shall be in the country of the inventor's residence. The language to be used in the arbitral proceedings shall be English.

No modifications shall be made to this Assignment unless in writing and signed by each of the Assignor(s) and Assignee. If any of the provisions of this Assignment shall be deemed invalid or unenforceable, then the entire Assignment shall be construed as if not containing the particular invalid or unenforceable provision or provisions, and the rights and obligations of Assignee and Assignor(s) shall be construed and enforced accordingly. Assignee's failure to exercise any option made available as a result hereof, shall not be construed as a waiver of such provisions, rights, or options, or affect the validity of this Assignment. Assignor covenants and agrees that it will not take any actions in violation of this Assignment.

Subsequent assignment from any of the Assignors to the Assignee purporting to convey the subject matter specified herein for a particular country, patent office, or jurisdiction shall not invalidate any provision of this assignment and any such subsequent assignment shall act as a further confirmation of the assignment herein.

Date: 38.2018

Signature on behalf of
Assignee

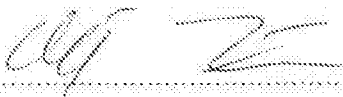

Hannu Ahonen
Senior Group Legal Counsel

ASSIGNMENT AGREEMENT

Title: SUBSCRIPTION CONCEALED IDENTIFIER

Date 24.7.2018 Signature of Assignor
Vesa TorvinenDate 24.7.2018 Witnessed by

Name:


MARJUT VAINOLA

Address:

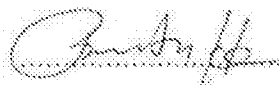
ETONIEMENTIE 1 CH5

02230 ESPOO

FINLAND

Date 24.7.2018 Witnessed by

Name:


PENITA HEINONEN

Address:

LUMIKIRKKA 8

02400 KIRKKONMÄKI

FINLAND

LMF to LME Assignment

This Assignment is made by **Oy L M Ericsson Ab**, a corporation duly organized under and pursuant to the laws of Finland and having its principal place of business at Hirsalantie 11, 02420 Jorvas, Finland (hereinafter referred to as "Assignor") in favor, and for the benefit and behoof of, **Telefonaktiebolaget LM Ericsson (publ)**, a corporation duly organized under and pursuant to the laws of Sweden and having its principal place of business at S-164 83 Stockholm, Sweden (hereinafter referred to as "Assignee").

For good, sufficient and adequate consideration, the receipt of which is hereby acknowledged, the Assignor has as of the Effective Date, sold, assigned, transferred, and set over, and by these presents, and to the extent any transferable or assignable rights still remain with the assignor do hereby sell, assign, transfer, and set over, unto the Assignee, its successors, legal representatives, and assigns the entire right, title, and interest in and to the following inventions, application(s) for Letters Patent, and any and all Letters Patent or Patents in all countries and pursuant to all multilateral treaty organizations, including Sweden, Finland, the United States of America, the Patent Cooperation Treaty and European Convention, that may be granted therefor and thereon, and in and to any and all divisions, continuations, continuations-in-part, conversions and utility models of said application(s), and reissues and extensions of said Letters Patent or Patents, the same to be held and enjoyed by the Assignee, for its use and behoof and the use and the behoof of its successors, legal representatives, and assigns, to the full end of the term or terms for which Letters Patent, Patents and Utility Models may be granted as fully and entirely as the same would have been held and enjoyed by the Assignor had this sale and assignment not been made:

SUBSCRIPTION CONCEALED IDENTIFIER

including, but not limited to, the application(s) for Letters Patent and Utility Model filed in:

Country Code	Application Number(s)	Filing Date(s)
WO	PCT/EP2018/069432	2018-07-17
US	16/200037	2018-11-26

The Effective date is the earliest date of the above listed Filing Date(s).

Assignor hereby authorizes and requests Assignee's Attorneys to insert the serial number and filing date of said application(s) for Letters Patent or Utility Model, when known. The assignment of the above mentioned rights includes a transfer of the whole right to use a priority (including priority according to any convention, multilateral agreement, bilateral agreement and national law) of the above mentioned application(s) for Letter Patent and Utility Model in all countries and multilateral treaty organizations wherein no residual rights shall remain with the Assignor. Assignor hereby request that said Letters Patent, Patent or Utility Model be issued to Assignee as the Assignee of said inventions, the Letters Patent, Patent or Utility Model to to be issued for the sole use and behoof of the Assignee, its successors, legal representatives, and assigns. Assignee alone hereinafter has the entire disposal of the invention and possesses entire ownership to any domestic and foreign patents or utility models granted thereafter. The rights granted hereunder shall include all rights to institute legal actions, obtain remedies and recover and retain damages in respect to said Letters Patent, Patent or Utility Model.

LMF to LME Assignment

The Assignor and Assignee hereby understand and agree that with the execution of this Assignment, to the extent necessary or appropriate, national and/or regional applications may be filed by the Assignee as the applicant and on behalf of the assignor.

To the extent Assignee is entitled to receive the rights hereunder pursuant to this Assignment, Assignor hereby covenants and agrees to and with the Assignee, its successors, legal representatives, and assigns, that, at the time of the Effective Date, the Assignor was the sole and lawful owner of the entire right, title, and interest in and to the inventions and application(s) for Letters Patent or Utility Models above-mentioned, and that the same are unencumbered, and that the Assignor has good and full right and lawful authority to sell and convey the same in the manner herein set forth.

Further, and for the same consideration, the Assignor hereby covenants and agrees to and with the Assignee, its successors, legal representatives, and assigns that the Assignor will, whenever counsel of the Assignee, or the counsel of its successors, legal representatives, and assigns, shall advise that any proceeding in connection with said inventions, or said application(s) for Letters Patent or Utility Model, or any proceeding in connection with Letters Patent or Utility Model for said inventions, in any country and any multilateral treaty organization, including interference proceedings, is lawful and desirable, or that any division, continuation, continuation-in-part, conversion or Utility Model of any application(s) for Letters Patent or Utility Model, or any reissue or extension of any Letters Patent or Utility Model to be obtained thereon, is lawful and desirable, sign all papers and documents, take all lawful oaths, and do all acts necessary or required to be done for the procurement, maintenance, enforcement, and defense of Letters Patent or Utility Model for said inventions, without charge to Assignee, its successors, legal representatives, and assigns, but at the cost and expense of the Assignee, its successors, legal representatives, and assigns. If the Assignor is prevented by any obstacles from signing said documents in person, this Assignment shall be valid as a Power of Attorney for the Assignee to sign these documents on behalf of any such Assignor.

This Assignment shall be governed by and construed under, and any dispute, controversy or claim related hereto shall be decided in accordance with the laws of Sweden, without regard to the conflicts of laws provisions thereof. Any dispute, controversy or claim arising under, out of or relating to this Assignment and any subsequent amendments of this Assignment, including, without limitation, its formation, validity, binding effect, interpretation, performance, breach or termination, as well as non-contractual claims, shall be referred to and finally determined by arbitration in accordance with the WIPO Arbitration Rules. The arbitral tribunal shall consist of a sole arbitrator. The place of arbitration shall be Sweden. The language to be used in the arbitral proceedings shall be English.

No modifications shall be made to this Assignment unless in writing and signed by each of the Assignor and Assignee. If any of the provisions of this Assignment shall be deemed invalid or unenforceable, then the entire Assignment shall be construed as if not containing the particular invalid or unenforceable provision or provisions, and the rights and obligations of Assignee and Assignor shall be construed and enforced accordingly. Assignee's failure to exercise any option made available as a result hereof, shall not be

LMF to LME Assignment

construed as a waiver of such provisions, rights, or options, or affect the validity of this Assignment. Assignor covenants and agrees that it will not take any actions in violation of this Assignment.

Subsequent assignment from any of the assignors to the assignee purporting to convey the subject matter specified herein for a particular country, patent office, or jurisdiction shall not invalidate any provision of this assignment and any such subsequent assignment shall act as a further confirmation of the assignment herein.

LMF to LME Assignment

SUBSCRIPTION CONCEALED IDENTIFIER

Signature of Assignee

Telefonaktiebolaget LM
Ericsson (publ)

Date.....

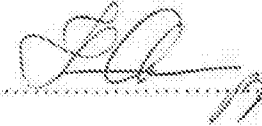
Name: Lena Lundholm
Carlsson
Title: Director, IPR
Processes & Tools

Signature of Assignor

Oy L M Ericsson Ab

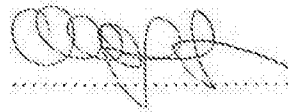
Date.....

28.8.2018

Name: Hannu Ahonen
Title: Senior Group Legal
Counsel

Date.....

28.8.2018

Name: Olli Sirkka
Title: President

LMF to LME Assignment

SUBSCRIPTION CONCEALED IDENTIFIER

Signature of Assignee

Telefonaktiebolaget LM
Ericsson (publ)

Date 21/9-2018

Lena Lundholm Carlsson

Name: Lena Lundholm
Carlsson
Title: Director, IPR
Processes & Tools

Signature of Assignor

Oy L M Ericsson Ab

Date

Name: Hannu Ahonen
Title: Senior Group Legal
Counsel

Date

Name: Olli Sirkka
Title: President

Electronic Acknowledgement Receipt

EFS ID:	34511100
Application Number:	16200037
International Application Number:	
Confirmation Number:	8611
Title of Invention:	SUBSCRIPTION CONCEALED IDENTIFIER
First Named Inventor/Applicant Name:	Vesa TORVINEN
Customer Number:	6449
Filer:	Brian S. Rosenbloom/Xania Steele
Filer Authorized By:	Brian S. Rosenbloom
Attorney Docket Number:	3602-1734US2
Receipt Date:	06-DEC-2018
Filing Date:	
Time Stamp:	21:02:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	3602-1734US2_SB08.pdf	67413	no	5
			1352c14897a5b521d23efa9fe66e223c3f6b1d0b		

Warnings:

Lenovo Ex. 1009

Page 226

Information:					
This is not an USPTO supplied IDS fillable form					
2	Foreign Reference	3602-1734US2_WO2016209126.pdf	6312697	no	54
			e787bd8e812ebf28d18b9152041f4f206f340934		
Warnings:					
Information:					
3	Other Reference-Patent/App/Search documents	3602-1734US2_ISR-WrittenOpinion.pdf	1765217	no	16
			4b8306a3475aa8d9f39d6c16ad93ad0b1096dc4e		
Warnings:					
Information:					
4	Non Patent Literature	3602-1734US2_S3-180824.pdf	290196	no	2
			95ef6932424dd926f61b122641e1c0060bb0a807		
Warnings:					
Information:					
5	Non Patent Literature	3602-1734US2_S3-180767.pdf	237018	no	2
			b7781eeecd78ad4d6c2d93f861f2e9b8d60f593f		
Warnings:					
Information:					
6	Non Patent Literature	3602-1734US2_TS-33501.pdf	2792247	no	25
			169af83850b684f1c797a0b3933a0cbb2f9c4ed8		
Warnings:					
Information:					
7	Non Patent Literature	3602-1734US2_lvd_5GEnsure.pdf	18432982	no	294
			54eaf1c23409dddde8b1ba5fb198d1dda5c5eba1a		
Warnings:					
Information:					
8	Non Patent Literature	3602-1734US2_lvd_TS-23003.pdf	852683	no	108
			6a6e30d6e184ece48670374b702b186be4af0655		
Warnings:					
Information:					

9	Non Patent Literature	3602-1734US2_IvD_TS-23501.pdf	1330419	no	146
			c1e8c86dd91cd4868ef9af72f5313b9203e40626		
Warnings:					
Information:					
10	Non Patent Literature	3602-1734US2_IvD_TS-33220.pdf	722273	no	93
			27dfce6efcb59ec83b6ecddeedb3bf8273cf372e7		
Warnings:					
Information:					
11	Non Patent Literature	3602-1734US2_IvD_ABOBA.pdf	44149	no	16
			2723d2fa209df1d0393041888696a2089e76504f		
Warnings:					
Information:					
12	Non Patent Literature	3602-1734US2_IvD_SIMON.pdf	73450	no	34
			2baf9c0d732ffe34b2da55b42239d6199488cc2		
Warnings:					
Information:					
13	Power of Attorney	3602-1734US2_POA.pdf	163587	no	1
			9475e176701bef5bc099c5ff9bcf8d6df1cc0933		
Warnings:					
Information:					
14	Assignee showing of ownership per 37 CFR 3.73	3602-1734US2_Statement373c.pdf	70728	no	3
			d18082d5745bb47d6641a62f75ae0d0a53c6bc613		
Warnings:					
Information:					
15	Assignee showing of ownership per 37 CFR 3.73	3602-1734US2_Assignment.pdf	5599033	no	17
			b4de3f2edfabbbf0eb977751c3253388aa3bb0e10		
Warnings:					
Information:					

16	Non Patent Literature	3602-1734US2_TR-33899-part1.pdf	14303131	no	300
			9b1ba87969de291a60fb8680c0ecdd8662f7af0d		

Warnings:

Information:

17	Non Patent Literature	3602-1734US2_TR-33899-part2.pdf	13663193	no	286
			32d542554721c870209bcc8e7f12c90269e816be		

Warnings:

Information:

Total Files Size (in bytes):			66720416		
-------------------------------------	--	--	----------	--	--

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

**CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION
UNDER 37 CFR 1.102(e) (Page 1 of 1)**

First Named Inventor:	Vesa TORVINEN	Nonprovisional Application Number (if known):	
Title of Invention:	SUBSCRIPTION CONCEALED IDENTIFIER		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i)(1) and the prioritized examination fee set forth in 37 CFR 1.17(c) have been filed with the request. The publication fee requirement is met because that fee, set forth in 37 CFR 1.18(d), is currently \$0. The basic filing fee, search fee, and examination fee are filed with the request or have been already been paid. I understand that any required excess claims fees or application size fee must be paid for the application.
2. I understand that the application may not contain, or be amended to contain, more than four independent claims, more than thirty total claims, or any multiple dependent claims, and that any request for an extension of time will cause an outstanding Track I request to be dismissed.
3. The applicable box is checked below:

I. ☒ Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)

- i. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.
---OR---
(b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.
- ii. An executed inventor's oath or declaration under 37 CFR 1.63 or 37 CFR 1.64 for each inventor, or the application data sheet meeting the conditions specified in 37 CFR 1.53(f)(3)(i) is filed with the application.

II. ☐ Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)

- i. A request for continued examination has been filed with, or prior to, this form.
- ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
- iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
- iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
- v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature /Brian S. Rosenbloom/	Date 2018-11-26
Name (Print/Typed) Brian S. Rosenbloom	Practitioner Registration Number 41276

Note: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required.*

☐ *Total of _____ forms are submitted.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

SUBSCRIPTION CONCEALED IDENTIFIER

CROSS-REFERENCE TO RELATED APPLICATIONS

[001] This application is a continuation of International patent application no. PCT/EP2018/069432, filed on July 17, 2018, which claims priority to U.S. provisional patent application no. 62/536,632, filed on July 25, 2017. The above identified applications are incorporated by this reference.

TECHNICAL FIELD

[002] The invention relates to methods performed by an authentication server, a de-concealing server and a User Equipment (UE), respectively. Furthermore, UEs, de-concealing servers, authentication servers, a computer program and a memory circuitry are also disclosed.

BACKGROUND

[003] It is important to maintain the confidentiality of a user equipment's (UE's) long-term subscription identifier (e.g., an IMSI (International Mobile Subscriber Identity)). Early generation 3GPP systems (e.g., 4G/LTE, 3G/UMTS, 2G/GSM) included a partial mechanism for long-term subscription identifier confidentiality using one or more short-term subscription identifiers. GUTI (Globally Unique Temporary ID) and C-RNTI (Cell-Radio Network Temporary Identifier) are examples of short-term subscription identifiers in 4G/LTE systems. However, the legacy partial mechanism may expose the long-term subscription identifier in clear text over the air interface. For example, so-called "IMSI catchers" could simply ask the long-term identifier from the UE, e.g., using identifier request/response messages.

[004] The 3rd Generation Partnership Project (3GPP) currently discusses how security, such as privacy, can be improved in communications networks. With respect to 5G, the 3GPP TS 33.501 V0.2.0 mentions a Subscription Permanent Identifier (SUPI) and it is there noted that the SUPI may be concealed, e.g. in the form of a pseudonym or a public-key encrypted SUPI.

SUMMARY

[005] An object of the invention is to facilitate security in communication between a UE and a communications network.

[006] A first aspect of the invention relates to a method performed by an authentication server in a home network of a UE for obtaining a SUPI. The method comprises: receiving a subscription concealed identifier (SUCI) which comprises an encrypted part in which at least a part of the SUPI is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI; determining a de-concealing server to use to decrypt the encrypted part of the SUCI; sending the SUCI to the de-concealing server; and receiving the SUPI in response.

[007] The clear-text part of the SUCI may comprise a public key identifier for a public key of the home network.

[008] The de-concealing server may be one of a plurality of de-concealing servers, and the determining of the de-concealing server may be based on information received from the UE. In such a case, the information may be a public key identifier for a public key of the home network. The public key identifier may be comprised in the clear-text part of the SUCI.

[009] The information may be the encryption scheme identifier, and the determined de-concealing server is then supporting decryption according to the encryption scheme.

[0010] The method may in an embodiment further comprise receiving the SUCI from the UE as part of a registration procedure for registering the UE with a wireless communication network.

[0011] The method may in an embodiment further comprise receiving the SUCI from the UE via an authentication request from a Security Anchor Function.

[0012] The authentication server may be one of the plurality of de-concealing servers.

[0013] The method may further comprise sending the SUCI and a request for an authentication vector for authenticating the UE to the determined de-concealing server in the same message.

[0014] The method may further comprise receiving the authentication vector and the SUPI from the determined de-concealing server in the same response.

[0015] The SUPI may comprise a Mobile Subscription Identification Number, MSIN, a Mobile Country Code, MCC, and a Mobile Network Code, MNC. The MSIN may in such an

embodiment be is encrypted in the encrypted part of the SUCI, and the MCC and the MNC are the home network identifier in the clear-text part of the SUCI. The SUPI may in an alternative embodiment be a Network Access Identifier.

[0016] A second aspect of the invention relates to a method, performed by a de-concealing server, for providing a SUPI to an authentication server. The method comprises: receiving, from the authentication server, a SUCI which comprises an encrypted part in which at least a part of the SUPI is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by a UE to encrypt the SUPI in the SUCI and which is supported by the de-concealing server; decrypting the encrypted part of the SUCI using the encryption scheme indicated by the encryption scheme identifier to obtain the SUPI; and sending the SUPI to the authentication server.

[0017] The clear-text part of the SUCI may also comprise a key identifier used for identifying a decryption key used for decrypting the SUPI. The key identifier may also be used for identifying the de-concealing server.

[0018] A key corresponding to the key identifier may be a public key of a home network of the UE.

[0019] In an embodiment of the second aspect, the receiving of the SUCI comprises receiving the SUCI and a request for an authentication vector for authenticating the UE in the same message.

[0020] Sending the authentication vector and the SUPI to the authentication server may be done in the same message.

[0021] A third aspect relates to a method performed by a UE. The method comprises: generating a SUCI, which comprises an encrypted part in which at least a part of a SUPI is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI; and transmitting the SUCI to an authentication server for forwarding of the SUCI to a de-concealing server capable of decrypting the SUPI.

[0022] The SUCI may be transmitted in a request to register with a wireless communication network.

[0023] Generating the SUCI may be done using a tamper resistant secure hardware component of the UE to generate the SUCI. In such a case, generating the SUCI may comprise generating the SUCI based on a privacy key selected from a plurality of privacy keys stored in the tamper resistant secure hardware component.

[0024] In an embodiment, the generation of the SUCI comprises sending a time to the tamper resistant secure hardware component for use in the generation of the SUCI.

[0025] Generating the SUCI comprises in an embodiment generating the SUCI from a privacy key comprising the SUPI.

[0026] Transmitting the SUCI to the authentication server comprises in an embodiment transmitting the SUCI to the authentication server in response to an identifier request message received from an Authentication and Mobility management Function, AMF, as part of a procedure for registering the UE with a wireless communication network. In such an embodiment, the method may further comprise transmitting a registration request to the AMF, wherein the registration request comprises a 5G Globally Unique Temporary Identifier, and receiving the identifier request message in response.

[0027] The method according to the third aspect may further comprise successfully authenticating with the authentication server after transmitting the SUCI, and receiving a registration acceptance message in response.

[0028] In an embodiment of the first, second and third aspects, the encryption scheme may be a null-encryption scheme.

[0029] In an embodiment of the first, second and third aspects, the encryption scheme may, alternatively to the null-scheme or any other encryption scheme, be an Elliptic Curve Integrated Encryption Scheme, ECIES, and the clear-text part of the SUCI may in such an embodiment comprise an ephemeral public key of the UE for use in the ECIES.

[0030] A fourth aspect relates to an authentication server for a home network of a UE for obtaining a SUPI. The authentication server comprises a processing circuitry and a memory circuitry. The memory circuitry contains instructions executable by the processing circuitry whereby the authentication server is operative to: receive a subscription concealed identifier (SUCI) which comprises an encrypted part in which at least a part of the SUPI is encrypted, and

a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI; determine a de-concealing server to use to decrypt the encrypted part of the SUCI; send the SUCI to the de-concealing server, and receive the SUPI in response.

[0031] A fifth aspect relates to an authentication server for a home network of a UE for obtaining a SUPI. The authentication server is configured to: receive a SUCI, which comprises an encrypted part in which at least a part of the SUPI is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI; determine a de-concealing server to use to decrypt the encrypted part of the SUCI; send the SUCI to the de-concealing server, and receive the SUPI in response.

[0032] A sixth aspect relates to an authentication server for a home network of a UE for obtaining a SUPI. The authentication server comprises: an interface module configured to receive a SUCI, which comprises an encrypted part in which at least a part of the SUPI is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI; a determining module configured to determine a de-concealing server to use to decrypt the encrypted part of the SUCI; and wherein the interface module is further configured to send the SUCI to the de-concealing server, and receive the SUPI in response.

[0033] The invention also relates to an authentication server of any one of the fourth to sixth aspects, configured to perform any one of the embodiments of the method according to the first aspect.

[0034] A seventh aspect relates to a de-concealing server for providing a SUPI to an authentication server. The de-concealing server comprises a processing circuitry and a memory circuitry. The memory circuitry contains instructions executable by the processing circuitry, whereby the de-concealing server is operative to: receive, from the authentication server, a SUCI, which comprises an encrypted part in which at least a part of the SUPI is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by a UE to encrypt the SUPI in the SUCI and which is supported by the de-concealing server; decrypt the encrypted part of the SUCI, using the

encryption scheme indicated by the encryption scheme identifier to obtain the SUPI; and send the SUPI to the authentication server.

[0035] An eighth aspect relates to a de-concealing server for providing a SUPI to an authentication server. The de-concealing server is configured to: receive, from the authentication server, a SUCI, which comprises an encrypted part in which at least a part of the SUPI is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by a UE to encrypt the SUPI in the SUCI and which is supported by the de-concealing server; decrypt at least part of the SUCI, using the encryption scheme indicated by the encryption scheme identifier to obtain the SUPI; and send the SUPI to the authentication server.

[0036] A ninth aspect relates to a de-concealing server for providing a SUPI to an authentication server. The de-concealing server comprises: a receiving module configured to receive, from the authentication server, a SUCI, which comprises an encrypted part in which at least a part of the SUPI is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by a UE to encrypt the SUPI in the SUCI and which is supported by the de-concealing server; a decrypting module configured to decrypt at least part of the SUCI, using the encryption scheme indicated by the encryption scheme identifier to obtain the SUPI; and a sending module configured to send the SUPI to the authentication server.

[0037] The invention also relates to a de-concealing server of any one of the sixth, eighth and ninth aspects configured to perform any one of the embodiments of the second aspect.

[0038] A tenth aspect relates to a UE which comprises a processing circuitry and a memory circuitry. The memory circuitry contains instructions executable by the processing circuitry whereby the UE is operative to: generate a SUCI, which comprises an encrypted part in which at least a part of a SUPI is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI; and transmit the SUCI to an authentication server for forwarding of the SUCI to a de-concealing server capable of decrypting the SUPI.

[0039] An eleventh aspect relates to a UE configured to: generate a SUCI, which comprises an encrypted part in which at least a part of a SUPI is encrypted, and a clear-text part

which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI; and transmit the SUCI to an authentication server for forwarding of the SUCI to a de-concealing server capable of decrypting the SUPI.

[0040] A twelfth aspect relates to a UE which comprises: a generating module configured to generate a SUCI, which comprises an encrypted part in which at least a part of a SUPI is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI, and a transmitting module configured to transmit the SUCI to an authentication server for forwarding of the SUCI to a de-concealing server capable of decrypting the SUPI.

[0041] The clear-text part of the SUCI may according to an embodiment of the first, third and twelfth aspects comprise a public key identifier for a public key of the home network.

[0042] The SUPI may comprise a Mobile Subscription Identification Number.

[0043] The SUPI may be a Network Access Identifier.

[0044] The invention also relates to a user equipment of any one of the tenth, eleventh and twelfth aspects, configured to perform any one of the embodiments of the third aspect.

[0045] A 13th aspect relates to a computer program, comprising instructions which, when executed on at least one processing circuitry of a server device, cause the at least one processing circuitry to carry out the method according to any one of the embodiments of the first to third aspects.

[0046] A 14th aspect relates to a memory circuitry containing the computer program.

BRIEF DESCRIPTION OF THE DRAWINGS

[0047] FIG. 1 illustrates an exemplary wireless communication network.

[0048] FIG. 2 illustrates an example in which a UE encrypts its long-term subscription identifier as part of an attachment procedure.

[0049] FIG. 3 illustrates an example of a Subscription Concealed Identifier (SUCI).

[0050] FIG. 4 illustrates an example of a privacy key.

- [0051]** FIG. 5 illustrates a 3GPP public key privacy scheme.
- [0052]** FIG. 6 illustrates an example of a registration procedure.
- [0053]** FIG. 7 illustrates an example in which a 5G-USIM/UICC of a UE generates the SUCI.
- [0054]** FIG. 8 illustrates an example in which the 5G-USIM/UICC does not have a privacy key.
- [0055]** FIG. 9 illustrates an example in which an ME generates the SUCI.
- [0056]** FIG. 10 illustrates an example in which the ME is notified about an updated privacy key.
- [0057]** FIG. 11 illustrates an example in which the ME detects that the 5G-USIM/UICC has been replaced.
- [0058]** FIG. 12 illustrates an example of Privacy Key Verification Data.
- [0059]** FIG. 13 illustrates an example UE Registration process in which the UE has no valid privacy key.
- [0060]** FIG. 14 illustrates an example UE Registration process in which the UE's privacy key needs to be updated.
- [0061]** FIG. 15 illustrates an example of how the privacy key and Privacy Key Verification Data are related to each other.
- [0062]** FIG. 16 illustrates a hardware embodiment for e.g. an authentication server.
- [0063]** FIG. 17 illustrates an embodiment of an authentication server.
- [0064]** FIG. 18 illustrates an embodiment of an authentication server.
- [0065]** FIG. 19 illustrates an embodiment for e.g. a de-concealing server.
- [0066]** FIG. 20 illustrates an embodiment of a de-concealing server.
- [0067]** FIG. 21 illustrates an embodiment of a UE.
- [0068]** FIG. 22 illustrates an embodiment of a UE.
- [0069]** DETAILED DESCRIPTION

[0070] FIG. 1 illustrates an example wireless communication network 30 that includes a UE 1, a serving network 2, and a home network 3. The UE and home network are both communicatively connected to, and exchange signals with each other via, the serving network. The UE is configured with a subscription identifier identifying a subscription supported by the home network, and accesses the home network using the serving network.

[0071] Typical examples of the UE 1 include a mobile equipment (ME), mobile terminal, smartphone, personal computer, a laptop computer, a desktop computer, a workstation, a tablet computer, a wearable computer, and/or a smart appliance. According to particular embodiments of the UE, the UE may comprise a general memory storage as part of an ME, and a tamper resistant secure hardware component providing secure storage, such as a 5G-USIM (Universal Subscriber Identity Module), a UICC (Universal Integrated Circuit Card), e.g. with a 5G-USIM installed thereon, and/or other secure storage device. According to such embodiments, any of the capabilities attributed to the UE, generally, may be performed using the tamper resistant secure hardware component of the UE.

[0072] The serving network 2 includes one or more physical devices and/or signaling mediums capable of exchanging communication signals with the UE 1 and the home network 3. In particular, the serving network may include hardware that provides one or more: access points (e.g., a base station, eNodeB, femtocell, and/or wireless access point), access networks, authentication servers, Access and Mobility management Functions (AMFs), Security Anchor Functions (SEAFs), Authentication Server Functions (AUSFs), and/or any combination thereof (not shown). In particular, an authentication server may provide one or more AMFs, SEAFs, AUSFs, and/or any combination thereof. Details of these network entities will be discussed in further detail below.

[0073] The home network 3 includes one or more physical devices and/or signaling mediums capable of exchanging communication signals with the UE 1 via the serving network 2. In particular, the home network may include one or more: de-concealing servers, authentication servers (e.g., as described above), key provisioning servers, Subscription Identifier De-concealing Functions (SIDFs), Privacy Key Provisioning Functions (PKPFs), Unified Data Management (UDM) and/or any combination thereof (not shown). In particular, a de-concealing

server may provide one or more SIDs, PKPFs, and/or any combination thereof. Particular of these network entities will also be discussed in further detail below.

[0074] Examples of the serving and/or home network include (but are not limited to) one or more: local area networks; wireless networks; cellular networks; Internet Protocol-based networks; Ethernet networks; optical networks; and/or circuit switched networks. Such networks may comprise any number of networking devices such as routers, gateways, switches, hubs, firewalls, and the like (not shown) supporting the exchange of such communication signals.

[0075] Although FIG. 1 illustrates separate serving and home networks, in some embodiments of the present disclosure, the home network 3 is the serving network 2, i.e. in the case when the UE is not roaming. Further, although examples of particular functions in either the home network or the serving network were specified above, those particular functions may be in the other of the home network or serving network according to particular embodiments. Further still, although only one UE 1 is illustrated in FIG. 1, the serving and home networks may support a plurality of UEs, according to particular embodiments.

[0076] One example way to maintain the confidentiality of a UE's long-term subscription identifier is to protect the long-term subscription identifier using a home network public key. The home network public key may be provisioned within the UE 1 without a certificate, such that a global public key infrastructure (PKI) or certificate authority (CA) is not required (i.e., because the technique is used asymmetrically between the UE and a function in the home network 3). In such an example, the UE may be expected to encrypt the long-term subscription identifier, which is then transmitted towards the home network, using the home network public key.

[0077] FIG. 2 illustrates one such particular example in which the UE encrypts its long-term subscription identifier as part of an attachment procedure. According to the example of FIG. 2, the UE 1 encrypts its IMSI, leaving its MCC (Mobile Country Code) and MNC (Mobile Network Code) parts in clear-text, and sends an Attach Request to the serving network 2 with the encrypted IMSI as its identifier (step 1). The serving network identifies the UE's home network 3 using clear-text MCC/MNC and requests authentication information from the UE's home network using the encrypted IMSI as the UE's identifier (step 2). The home network decrypts the IMSI from the encrypted IMSI and fetches the corresponding authentication information. In

response to the authentication information request, the home network sends the UE's authentication information along with the clear-text IMSI to the serving network (step 3). The serving network performs an authentication procedure with the UE to authenticate the UE (step 4). If the authentication procedure succeeds, the serving network sends an Attach Accept message to the UE (step 5).

[0078] In such an approach, the home network public key may be pre-provisioned in a USIM and/or may be provisioned using an OTA (Over-the-Air) provisioning procedure. Although the approach illustrated in FIG. 2 does protect the long-term subscription identifier in at least some embodiments, some such embodiments may include one or more deficiencies. For example, the approach illustrated in FIG. 2 may be frustrated by legacy USIMs that cannot be feasibly changed, certain home operators that may not support OTA provisioning, and/or USIMs that may not be updatable (e.g., due to technical limitations, lack of storage space, or other limitations).

[0079] Various embodiments of the present disclosure provide alternatives to at least some aspects of the particular embodiment illustrated in FIG. 2, which corresponds to Fig. 3-8: Interactions between components in the document “Deliverable D3.6 5G-PPP Security enablers open specifications (v2.0)”. Particular embodiments enable the public key of the home network 3 to be provisioned (e.g., newly or refreshed) and stored in the UE 1, such that the UE 1 is able to encrypt its subscription identifier with this public key. Moreover, in particular embodiments, the core network (such as a 5GC (5G core) network) triggers the provisioning of the home network public key over existing traffic procedures defined by 3GPP (e.g., registration/authentication signaling, e.g. Non Access Stratum messages between the UE and the an AMF/SEAF node in relation to a registration procedure) without the need to rely on additional infrastructure and out-of-band procedures such as performing an OTA update procedure.

[0080] Although various embodiments herein will describe certain features or actions performed by the UE 1, it should not be presumed that such features or actions are performed by any particular component of the UE unless otherwise specified. For example, such functions may or may not be performed by a UICC, USIM, embedded UICC, integrated UICC or other circuitry and/or software of the UE (e.g. baseband circuitry in the ME), depending on the particular embodiment.

[0081] Particular embodiments include a Subscription Permanent Identifier (SUPI). A SUPI is a clear-text, globally unique, 5G, permanent identifier allocated to each subscriber in a 5G system. The SUPI may be IMSI-based or non-IMSI based. Embodiments that include an IMSI-based SUPI may use the IMSI as described in 3GPP TS 23.003 V15.0.0, for example. Embodiments that include a non-IMSI based SUPI may be based on a Network Access Identifier (NAI) according to the NAI IETF RFC 4282 based user identification described in 3GPP TS 23.003 V15.0.0. In some embodiments, the SUPI contains the address of the home network (e.g. the MCC and MNC in the case of an IMSI based SUPI). Such embodiments may enable certain roaming scenarios, e.g., by providing the serving network 2 with information useful for identifying the UE's home network 3. In case the SUPI is a NAI, it may also contain the IMSI, but it may also be non-IMSI based.

[0082] Particular embodiments additionally or alternatively include a Subscription Concealed Identifier (SUCI), such as illustrated in the example of FIG. 3. A SUCI is a protected version of a SUPI. The SUCI includes a clear-text part and an encrypted part.

[0083] The clear-text part includes a home network identifier that identifies the home network of the UE 1. For example, the SUCI may include an MCC and MNC of the home network. The clear-text part may also include a public key identifier, an encryption scheme identifier, and/or scheme related parameters useful for decrypting the encrypted part of the SUCI according to an encryption scheme, such as an ephemeral public key of the UE or other parameters for use in Elliptic Curve Integrated Encryption Scheme (ECIES) or other encryption scheme. The term ephemeral key is known to the person skilled in the art and is defined as a key whose use is restricted to a short time period, such as a single telecommunication connection (or session), after which all traces of it is eliminated. As will be discussed below, the public key identifier is an identifier that may be used within the home network to identify the correct SIDF in a home network that includes a plurality of SIDFs. The ECIES, the public key identifier, and SIDFs will be described in greater detail below. The skilled person understands that 'clear-text part' within the context of the SUCI means that the information therein is non-concealed/not encrypted information.

[0084] When the encrypted part is included in the SUCI, the SUCI is a protected version of SUPI. The encrypted part includes an encrypted subscription identifier, such as an

MSIN (Mobile Subscription Identification Number) or username. The username may be the whole or a part of the characters that comes before the '@' in a NAI, e.g. username@mnc<MNC>.mcc<MCC>.3gppnetwork.org. In this example, all characters before the '@' are encrypted. In the case of a Decorated NAI, which has the form 'homerealm!username@otherrealm', only the username part of the text to the left of the '@' is encrypted, since the homerealm might be used as routing information. Thus, decrypting the encrypted part of the SUCI may be performed to learn the corresponding SUPI. ECIES is an example of a public key encryption scheme that may be used to generate a SUCI from a SUPI and/or a SUPI from a SUCI. As will be discussed further below, the encrypted part of the SUCI may use a null encryption scheme, e.g., if the UE 1 has not been provisioned with the public key of the home network.

[0085] A SIDF is a function located in the home network that is responsible for decrypting the SUCI. Particularly in 5G architecture, a SIDF may be co-located in UDM (Unified Data Management). The SIDF may alternatively be said to be a part of the UDM or provided by the UDM. Additionally or alternatively, a SIDF may be an entity separate from UDM and/or co-located with an AUSF (Authentication Server Function).

[0086] FIG. 4 illustrates an example of a privacy key. This particular example of the privacy key includes a public key of the home network. In some embodiments, the privacy key also includes one or more public key scheme related parameters, the long-term subscription identifier, a subject field indicating a network, domain, or context to which the privacy key pertains (e.g., the subject may be a home network identifier, such as an MCC/MNC), a public key scheme identifier, public key scheme related domain specific values (e.g. values for the elliptic curve domain in case of ECIES scheme), the public key identifier as will be discussed in greater detail below, validity times indicating specifying when the privacy key is valid (e.g., not valid before and/or not valid after times), a key usage field indicating one or more ways the key may be used (e.g., subscription identifier privacy, slice selection privacy, etc.), and/or a digital signature calculated over some or all of the privacy key.

[0087] In particular, the key usage field may be set to indicate that the key is useful for "subscription privacy," in accordance with embodiments of the present disclosure. Uses of the privacy that are beyond the scope of the present disclosure may additionally or alternatively

indicate other uses for the privacy key. For example, the private key may be used for "Network Slice Selection Assistance Information (NSSAI) privacy" purposes instead of, or in addition to, "subscription privacy" purposes. Indeed, such other purposes may include similar methods, devices, and systems in the UE 1 and/or in the home network for initial provisioning, refresh, and other features as described herein. Although one privacy key may, in some embodiments, indicate multiple usages, other embodiments may include respective privacy keys for respective usages, the key usage field of each privacy key indicating a single key usage (e.g., one of the privacy keys may indicate "subscription privacy" and the other may indicate "NSSAI privacy"). The key usage field may be formatted as an integer, one or more enumerated values, an alphanumeric string, a bit string, a delimited string, and/or an array of any of the above-mentioned formats, among other things.

[0088] A 3GPP public key privacy scheme (3GPK schemes) is a standardized public key scheme that a UE 1 may support for interoperability between the UE and, e.g., a mobile operator. In absence of a standardized scheme, UE vendors would likely need to coordinate with such operators to implement privacy mechanisms. According to particular embodiments, the UE should support whichever schemes are allowed and/or standardized so that the home network is able to freely choose a scheme without creating any interoperability difficulties. One such scheme in particular is, for example, ECIES. Particular schemes may be adopted by as standard, and given an identifier (also called a "register") for interoperability. For each such scheme, any specific algorithms that need to be supported may also be specified. For example, in the case of ECIES, key agreement (KA), key derivation (KD) function (KDF), symmetric integrity, and symmetric encryption may be specified. One or more parameters relating to such a scheme, as well as (in one or more cases) their potential static values may also be specified. For example, in ECIES, elliptic curve domain parameters (p, a, b, G, n, h) for a curve over a prime field and/or $(m, f(x), a, b, G, n, h)$ for a curve over a binary field may be specified.

[0089] FIG. 5 illustrates an example 3GPK scheme. Each scheme adopted as standard may be assigned a specific identifier. For example, the null-scheme may be assigned a 0, ECIES may be assigned a 1, and so on. The identifier may be e.g. a 4-bit identifier. Other embodiments may format the scheme identifier in other ways, including but not limited to one or more integers, numeric strings, alphanumeric strings, bit strings, and/or other data types.

[0090] According to embodiments herein, the UE registers with the wireless communication network 30 according to a registration procedure, such as the example registration procedure illustrated in FIG. 6. According to the example registration procedure illustrated in FIG. 6, the UE uses a public key of the home network to conceal a long-term subscription identifier. Although one or more particular interfaces illustrated in FIG. 6, such as those specified by an N followed by a numerical designation (e.g., N1, N12, N13), are in accordance with 3GPP TS 23.501, the signaling performed over such interfaces as described herein, as well as other of the interfaces themselves (e.g., Nxx), are not known or described in any known art.

[0091] According to the example of FIG. 6, the UE 1 includes a temporary identifier (e.g., a 5G-GUTI) in a registration request and sends the registration request to an AMF/SEAF 4 (step 1). The AMF/SEAF, failing to recognize the 5G-GUTI, transmits an identifier request message to the UE to request the UE's identifier (step 2). The UE responds to the identifier request message with an identifier response message comprising a SUCI (step 3). The AMF/SEAF requests authentication of the UE from the AUSF 5 in the home network 3, and includes the SUCI in the authentication request (step 4). The AUSF uses information encoded in the SUCI to determine which of a plurality of SIDFs to use to decrypt at least part of the SUCI (step 5). In particular, the AUSF may use the public key identifier carried in the SUCI (or otherwise present in the authentication request message) to identify the correct SIDF 6. In some embodiments, the AUSF may additionally or alternatively use the scheme identifier to identify the correct SIDF. In other words, different SIDFs may handle different encryption schemes (e.g., a first SIDF may handle ECIES and a second SIDF may handle RSA), and the AUSF may choose an appropriate SIDF based on which scheme is identified by the SUCI. In yet an alternative embodiment, the information used to identify the correct SIDF 6 may be a parameter or ID which indicates the SIDF 6 and which parameter/ID is stored or provisioned to the tamper resistant secure hardware component 8.

[0092] Embodiments of the present disclosure may include multiple SIDFs to avoid having a single point of failure for networks having a large number of subscribers, for example. Consequently, distributed SIDF deployments may be advantageous to improve the fault tolerance, load balancing, and/or overall capacity of the network. Additionally or alternatively, different SIDF instances may be deployed to handle different sets of home

network public keys. Accordingly, the public key identifier in the SUCI may be used to select the proper SIDF instance(s), according to one or more embodiments herein. Alternatively, in particular embodiments that only have one SIDF deployed, the public key identifier may be omitted from the SUCI.

[0093] The AUSF 5 sends the SUCI to the selected SIDF 6 (step 6). If the SIDF is co-located in UDM 7 (such that the Nxx message in step 6 of Fig. 6 is a N13 message, for example), then the same message may be used to request an authentication vector or authentication credentials from the UDM. The SIDF decrypts the SUCI to obtain a corresponding SUPI, and returns the SUPI to the AUSF (step 7). If the SIDF is co-located in UDM, then the same message may be used to return authentication vector/credentials to AUSF.

[0094] AUSF 5 and UE 1 exchange authentication messages using authentication vectors/credentials received from the UDM 7 (step 8). If the AUSF has not already received the required authentication vector/credentials from the UDM (e.g., in step 7 discussed above), the AUSF may request authentication vector/credentials from the UDM before initiating authentication with the UE (not shown). Alternatively, the AUSF may have delegated the authentication to SEAF. In such embodiments, the AUSF may simply forward the SUPI to the SEAF in this step, and rely on the SEAF to perform the authentication in the next step.

[0095] Continuing with the example in which the AUSF 5 successfully authenticates the UE 1, the AUSF returns the SUPI to the AMF/SEAF 4 (step 9). The AMF/SEAF accepts the registration of the UE and transmits a registration acceptance message to the UE (step 10).

[0096] As briefly discussed above, particular features of the UE 1 may be performed by a tamper resistant secure hardware component 8 of the UE. FIG. 7 illustrates a particular example in which a 5G-USIM/UICC 8a of a UE generates the SUCI. Although this particular example uses the term 5G-USIM/UICC, this term should not be considered as limiting with respect to any version or vendor of USIM or UICC technology, nor should this term be considered as limiting with respect to any generation of mobile network, e.g., 2G/3G/4G/5G.

[0097] According to the example of FIG. 7, an ME 9 requests a SUCI (step 1). In some such embodiments, this SUCI request may include the time. In other such embodiments, the request may simply be a read operation from the 5G-USIM/UICC 8a. According to such embodiments in which there are multiple home network public keys, the 5G-USIM/UICC

chooses the correct corresponding privacy key (e.g., based on the time), and generates the SUCI using the selected privacy key (step 2). Alternatively, if such embodiments in which there is only one privacy key, the 5G-USIM/UICC simply uses that privacy key. The 5G-USIM/UICC then returns the SUCI to the ME (step 3).

[0098] FIG. 8 illustrates an example in which the 5G-USIM/UICC does not have a privacy key, or does not support the feature.

[0099] According to the example of FIG. 8, the ME 9 requests a SUCI with a request (which may include the time, in some embodiments) in similar fashion as described above with respect to FIG. 7. In this example, however, the 5G-USIM/UICC 8a does not have privacy key or does not recognize the command because it does support the feature (step 2). Accordingly, the 5G-USIM/UICC returns an error message (or empty data) to the ME (step 3).

[00100] Alternatively to the example of FIG. 8, the ME 9 may know that 5G-USIM/UICC 8a does not have privacy key or does not support privacy key by other means, according to particular embodiments. For example, the ME may obtain the version and or vendor information of 5G-USIM/UICC and determine, based on this information, that a privacy key is not supported or present. As another example, the ME may determine that a privacy key is not supported or present in 5G-USIM/UICC based on some other response message from the 5G-USIM/UICC.

[00101] FIG. 9 illustrates an example in which the ME 9 generates the SUCI, but the privacy key itself is stored in the 5G-USIM/UICC 8a.

[00102] According to the example of FIG. 9, the ME 9 has no privacy key and requests one from the 5G-USIM/UICC 8a (step 1). In some embodiments, the request includes the time. In other embodiments, the request is a direct read operation from the 5G-USIM/UICC memory. The 5G-USIM/UICC then chooses the privacy key (e.g., based on time, if provided in the request) (step 2). The 5G-USIM/UICC returns the privacy key to the ME (step 3). At this point, the ME may, in some embodiments (but not necessarily all embodiments) store the privacy key and/or the SUPI to a non-volatile memory of the ME (step 4). The ME then generates the SUCI based on the SUPI and the privacy key (step 5).

[00103] FIG. 10 illustrates an example in which the ME 9 gets notified if the privacy key is updated in the 5G-USIM/UICC 8a. In this scenario, the ME subscribes to changes in the

privacy keys, and gets notifications when updates are available. This scenario assumes that the ME stores the privacy key or asks the 5G-USIM/UICC for the privacy key as needed to obtain the latest privacy key.

[00104] According to the example of FIG. 10, the ME 9 sends a request to the 5G-USIM/UICC 8a requesting to subscribe to privacy key updates (step 1). The request may, in some embodiments, include a SUPI. The 5G-USIM/UICC accepts the subscription and transmits an acknowledgement to the ME in response (step 2). When the home network updates the privacy key(s) or delivers one or more new ones to the 5G-USIM/UICC (step 3), the 5G-USIM/UICC notifies the ME that one or more new privacy keys are available (step 4). Although FIG. 10 depicts the notification message including the privacy key(s), according to other embodiments, the ME may alternatively read the key from the 5G-USIM/UICC based on the notification. The ME acknowledges the notification (step 5). The ME then stores the new privacy key(s) to the non-volatile memory of the ME (step 6). The ME may replace existing privacy key data if MCC/MNC/MSID in previously stored privacy key data are identical.

[00105] FIG. 11 illustrates an example in which the UE is powered on, and the ME 9 detects that the 5G-USIM/UICC 8a has been replaced (e.g., with a different 5G-USIM/UICC, or simply removed and reinserted, according to various embodiments). Although particular embodiments may treat replacement with a different 5G-USIM/UICC the same as a removal and reinsertion (e.g., for security reasons), other embodiments may respond differently based on which of these two scenarios is detected.

[00106] According to the example of FIG. 10, the UE 1 is powered on (step 1). The ME 9 sends a message to the 5G-USIM/UICC 8a (step 2) and the 5G-USIM/UICC responds in a manner that is inconsistent with when the UE was previously powered on (step 3). For example, the response message may include a different SUPI than any previously seen by the ME.

[00107] The ME 9 determines that the 5G-USIM/UICC 8a has been replaced (step 4). For example, the 5G-USIM/UICC may be different in some way from the previous time when the UE 1 was powered on, indicating that the 5G-USIM/UICC has been replaced with a different one. Alternatively, the ME may detect that the 5G-USIM/UICC has been replaced using non-volatile memory that is updated by a mechanical, electrical, or software mechanism, such as an optical sensor, switch, weight sensor, pressure sensor, and/or electrical circuitry that

is triggered when 5G-USIM/UICC is removed and/or inserted, e.g., regardless of whether the same 5G-USIM/UICC or a different one has been removed and reinserted.

[00108] The ME 9 removes the privacy key it had previously stored from the non-volatile memory (if there is one). Additionally or alternatively, if the ME stored the SUPI of the old 5G-USIM/UICC with the privacy key to its memory, the ME may decide to remove the privacy key from the non-volatile memory based on a comparison of the SUPI returned by the new 5G-USIM/UICC 8a with the SUPI stored with the old privacy key.

[00109] Particular embodiments described above describe ways in which the devices within a wireless communication system may securely exchange a subscription identifier, including the generation and use of particular data structures and corresponding encryption/decryption schemes. In particular, embodiments described above allow for this secure exchange to be performed as part of registering the UE 1 with the wireless communication network 30. Many such embodiments presume that the UE is provisioned with a valid privacy key.

[00110] To ensure that the UE 1 does, in fact, have a valid privacy key, further embodiments of the present disclosure describe ways in which to provision the UE. Particular embodiments relating to provisioning may include Privacy Key Verification Data (MAC-P). As shown in the example of FIG. 12, a MAC-P includes a message authentication code (MAC). The MAC is calculated based on the privacy key and a provisioning key (which will be explained in greater detail below). For example, the MAC may be calculated over the various fields of the privacy key, including but not limited to the home network public key and its related parameters as described above, in combination with the provisioning key.

[00111] The MAC-P may, according to some embodiments, also include a provisioning key identifier (e.g. a RAND) and/or an integrity protection algorithm identifier. According to some embodiments in which the MAC-P does not include the integrity protection algorithm identifier, the integrity protection algorithm to be used may be identified separately from the MAC-P, or a predefined Key Derivation Function (KDF) such as, e.g., HMAC-SHA-256 may be used. The MAC-P may additionally or alternatively include a counter field, which may be used to identify the MAC-P from a plurality of MAC-Ps (e.g., in cases where more than one MAC-P is calculated using the same provisioning key). The relationship between the privacy

key (e.g., as shown in FIG. 4) and the MAC-P (e.g., as shown in FIG. 12) is further explained below with respect to FIG. 15.

[00112] The provisioning key is a secret shared between the UE 1 and a PKPF 10 (see Fig 13), which is described in further detail below. The provisioning key is UE-specific, i.e. it is a key which in the home network 3 is associated with the UE and/or the 5G USIM, UICC 8a or any other hardware in the UE/ME in which a SIM/USIM is allowed to be stored. In some embodiments, the provisioning key may be derived from the home network master key, e.g. K_{AUSF} in a 5G or future network as created in e.g. 5G AKA, EAP-AKA' and EAP-TLS (Extensible Authentication Protocol - Transport Layer Security), that is created when the UE 1 authenticates with the network. In some such embodiments, the AUSF may have the home network master key. Further, a new home network master key may be created when the UE re-authenticates.

[00113] According to one example, the provisioning key may be created from a CK (Ciphering Key), IK (Integrity Key) (e.g., by applying a KDF such as HMAC-SHA-256 or other secure one-way hash function, such as SHA-256, or a concatenation of CK and IK). The provisioning key may, alternatively to a direct generation from the master key or CK/IK, be generated from CK' and IK' as generated from CK and IK in the EAP-AKA' method. In another alternative, the provisioning key may be generated from EMSK (Extended Master Session Key) in the case of EAP-TLS as specified in RFC5216. As the same home network master key may be used to derive numerous keys, embodiments of the present disclosure use at least one further standard parameter in combination with the home network master key as input for deriving the provisioning key. For example, when standard KDF is used, the FC (Function Code) may be used as an input (e.g., as specified in TS 33.220, such as TS33.220 V15.0.0) to produce a provisioning key that is distinguishable from other keys produced using the home network master key.

[00114] According to another example, the provisioning key may be a key which is same as, or derived from, an ephemeral shared key that is shared between the SIDF 6 and the UE 1, particularly when the encryption scheme used is a hybrid public key scheme such as ECIES. For example, ECIES uses a public key mechanism (e.g., Diffie-Hellman) for key agreement that results in a shared key, which is ephemeral, between the SIDF and the UE. That ephemeral

shared key, for security purposes, is generally processed further through a key derivation function (e.g., SHA-256) to derive yet other derived shared keys between the SIDF and the UE (e.g., encryption key and MAC key in ECIES). One of these other derived shared keys is generally used for encryption and is called the ephemeral encryption key. As applied to embodiments of the present disclosure, one of these other derived shared keys may be used, e.g., to generate a SUCI from a SUPI. Further, in some embodiments, another of the derived shared keys (e.g., MAC key in ECIES), a new one further derived from one of the derived shared keys, or yet another key derived from the ephemeral shared key, may be used as the provisioning key. In some embodiments in which the SIDF has, or is able to obtain/derive the provisioning key, the SIDF may also calculate the MAC or MAC-P.

[00115] The PKPF 10 is a function located in the home network 3 that is responsible for provisioning the privacy key. According to particular embodiments, the PKPF may be co-located with the AUSF 5, and particularly in at least some embodiments in which the provisioning key is derived from the home network master key that is created based on primary authentication between UE and the network. In other embodiments, the PKPF may be collocated with other 5GC entities, such as UDM 7. According to yet other embodiments, the PKPF is its own separate entity. In some embodiments, the SIDF 6 and PKPF are implemented together as a single function, and there is no need to transfer the provisioning key. In some other embodiments, the PKPF may obtain the provisioning key from the SIDF. The PKPF may also obtain the MAC/MAC-P from the SIDF.

[00116] FIG. 13 illustrates an example UE Registration process in which the UE 1 has no valid privacy key. For example, the end-user may have inserted a new USIM/UICC into the UE, and this new USIM/UICC does not contain a privacy key.

[00117] According to the example illustrated in FIG. 13, the UE 1 sends a Registration request to an AMF/SEAF 4, including a SUCI in the request (step 1). Because the UE initially has no privacy key in this scenario, the UE uses a null-scheme or null-encryption method to create the SUCI. The null-scheme is implemented such that it returns the same output as the input, and it applies to both the encryption in the UE and the decryption by the SIDF 6. Further, because the UE has no privacy key that would indicate the null-scheme or null-encryption method (which the home network may be free to choose, according to

embodiments), an explicit or implicit indicator that the actual privacy key is missing from the UE may be used, according to particular embodiments. For example, as discussed above, the SUCI may use a null encryption scheme for the encrypted part, which may implicitly signal that the privacy key is missing. Alternatively, a "missing privacy key" indicator may be, e.g., a standardized or well-known public key identifier value, a flag and/or a message type indicator (e.g., a registration request of type "privacy provisioning" or "pre initial registration").

[00118] The AMF/SEAF 4, having received the registration request, requests UE authentication from the AUSF 5/PKPF 10 (step 2). The AUSF sends the SUCI (and the "missing privacy key" indicator, if one was included in the authentication request) to a SIDF 6 (step 3). According to embodiments in which the SIDF is co-located in UDM 7 (e.g., the Nxx message is a N13 message), then the same message may be used to request an authentication vector/credentials from the UDM.

[00119] The SIDF 6 sees that the SUCI is in cleartext, and that the UE 1 is missing a privacy key. According to this example, the SIDF has a local policy that all SUCIs must be protected using ECIES. Accordingly, the SIDF returns a SUPI to the AUSF, together with a request to provision the ECIES privacy key to the UE (step 4). In some embodiments, the response includes multiple privacy keys to be provisioned to the UE. According to embodiments in which the SIDF is co-located in UDM 7, then the same message may be used to return the authentication vector/credentials to the AUSF 5.

[00120] According to embodiments in which the AUSF 5 has not received the authentication vector/credentials from UDM 7 already, the AUSF 5 may request said authentication vector/credentials from UDM before initiating the authentication with the UE (not shown). Alternatively, according to embodiments in which the AUSF has received the authentication vector/credentials from UDM already, the AUSF and UE exchange authentication messages using said authentication vectors/credentials (step 5). Alternatively, the AUSF may have delegated the authentication to the AMF/SEAF 4.

[00121] According to this example, the PKPF 10 is co-located with the AUSF 5. Consequently, upon successful authentication, the AUSF/PKPF creates a provisioning key that may be used to protect the privacy key provisioning message to the UE 1, i.e., without the need to exchange signaling to transfer the provisioning key. According to other embodiments in

which the AUSF and PKPF are not co-located, the AUSF may request that the provisioning key be generated by the PKPF and the PKPF may transfer the provisioning key to the AUSF in response (not shown).

[00122] The AUSF 5 / PKPF 10 protects the privacy key(s) (received from SDF 6 in step 4) with the provisioning key by calculating a MAC (e.g., as described above with respect to FIG. 12) and constructing MAC-P (step 6). In some embodiments, the privacy key may also be encrypted. In some embodiments, the AUSF/PKPF may receive the MAC and/or MAC-P from the SDF, as described above, particularly in at least some embodiments in which the provisioning key is based on the ephemeral shared key of, e.g., an EICES scheme. In particular, as discussed above, the SDF may have generated the MAC and/or MAC-P.

[00123] The AUSF 5 then returns the SUPI, the privacy key(s), and the MAC-P to AMF/SEAF 4 (step 7). In some embodiments, the SUPI, the privacy key(s), and/or the MAC-P are transmitted to the AMF/SEAF in the same registration related message flow for registering the UE 1 with the wireless communication network 30. In some embodiments, the SUPI, the privacy key(s), and/or the MAC-P are transmitted to the AMF/SEAF in a separate message flow (not shown).

[00124] According to embodiments in which the AUSF 5 delegated authentication of the UE 1 to the AMF/SEAF 4, the AMF/SEAF may authenticate the UE at this point (not shown). In such embodiments, the AMF/SEAF may have received the SUPI, the privacy key(s), and the MAC-P previously, e.g., directly from the SDF 6 in step 4.

[00125] The AMF/SEAF 4 accepts the registration of the UE 1, and forwards the privacy key(s) and the MAC-P to the UE, e.g., in a registration acceptance message (step 8). The UE then attempts to verify the MAC, and if successful, stores the privacy key(s). To verify the MAC, the UE creates the same provisioning key as the AUSF 5 /PKPF 10 previously did. In other words, when the UE generates an expected MAC and then compare it with the received MAC, the MAC is verified if the expected MAC is deemed as being the same as the received MAC.

[00126] In some embodiments, the UE 1 then detaches from the network (step 9), e.g., to start a new registration procedure using a provisioned privacy key to conceal its subscriber identity, according to one of the embodiments described above. For example, detaching and

reregistering in this way may prevent an attacker from linking the SUPI to a temporary identifier of the UE.

[00127] The UE 1 may, in some embodiments, need to be provisioned with a privacy key due to the expiration or invalidation of a privacy key that was previously provisioned to the UE. FIG. 14 illustrates an example UE Registration process in which the UE's privacy key needs to be updated, e.g., for some security or operational reason. Some reasons that the previously provisioned privacy key may need to be updated, according to various embodiments, may be that the previously provisioned privacy may have reached (or is reaching) its expiry date, security in the wireless communication network 30 has been compromised in some way, and/or the privacy key is subject to regular updates.

[00128] According to the example of FIG. 14, the UE 1 sends a registration request to an AMF/SEAF 4 (step 1). The registration request includes a SUCI. In this example, since the UE has a privacy key, the UE uses an encryption scheme or method (e.g., ECIES) to create the SUCI, e.g., according to one of the embodiments described above.

[00129] The AMF/SEAF 4 requests UE authentication from a AUSF 5 / PKPF 10 (step 2). The AUSF sends the SUCI to an SIDF 6 (step 3). As in the previous example, according to some embodiments in which the SIDF is co-located with UDM 7, then the same message may be used to request an authentication vector/credentials from the UDM.

[00130] The SIDF 6 sees that the SUCI is encrypted with a privacy key that needs to be updated. For example, the SIDF may detect that the privacy key is expired or is about to expire, or that the privacy key is invalid for any other reason as previously discussed. The SIDF returns a SUPI to the AUSF 5 together with a request to provision the updated ECIES privacy key to the UE (step 4). According to some embodiments, the response may include several privacy keys. Further, as previously discussed, according to some embodiments in which the SIDF is co-located in UDM, the same message may be used to return the authentication vector/credentials to the AUSF.

[00131] The AUSF 5 and UE 1 exchange authentication messages using authentication vectors/credentials received from UDM 7 (step 5). As discussed in previous examples, the AUSF may have received the required authentication vector/credentials from UDM already in step 4 (e.g., in some embodiments in which the SIDF 6 is co-located in UDM), or the AUSF may

request such authentication vector/credentials from UDM before initiating the authentication with the UE.

[00132] According to embodiments in which the PKPF 10 is co-located with the AUSF 5, the AUSF/PKPF may create a provisioning key used to protect the privacy key provisioning message to the UE 1 as a result of successful authentication. For example, the authentication procedure may include producing a home network master key that may be used to derive the provisioning key. Alternatively, in embodiments in which the PKPF and AUSF are not co-located, the AUSF and PKPF may exchange the provision key through appropriate messaging (not shown).

[00133] The AUSF 5 / PKPF 10 protects the privacy key(s) (received from SIDF 6 in step 4) with the provisioning key by calculating a MAC and constructing MAC-P, e.g., according to the example illustrated in FIG. 14 (step 6). As discussed above, in some embodiments, the AUSF/PKPF may receive the MAC and/or MAC-P from the SIDF, as described above, particularly in at least some embodiments in which the provisioning key is based on the ephemeral shared key of, e.g., an EICES scheme. In particular, as discussed above, the SIDF may have generated the MAC and/or MAC-P.

[00134] After successful authentication, the AUSF 5 sends the SUPI, the privacy key(s) and the MAC-P to the AMF/SEAF 4 (step 7), e.g., in the same registration-related message flow. Other embodiments may use separate message flows for one or more of the SUPI, privacy key(s) or MAC-P. Also, as previously discussed, the AUSF may have delegated authentication of the UE to the SEAF, in which case the SUPI, the privacy key(s), and the MAC-P may have been returned to SEAF already in step 4, and the AUSF performs the authentication as previously described.

[00135] The AMF/SEAF 4 accepts the registration of the UE 1, and forwards the privacy key(s) and the MAC-P to the UE, e.g., in a registration acceptance message (step 8). The UE creates the same provisioning key from the primary authentication as AUSF 5 / PKPF 10 did, and verifies the MAC in the message. If verification is successful, the UE stores the privacy key(s). The old privacy key may also be removed.

[00136] According to yet an example, the AUSF 5 generates the MAC and MAC-P and sends the privacy key(s) and the MAC-P to the UE 1 via the UDM 7 which forwards the privacy

key(s) and the MAC-P to the AMF, which then forwards the privacy key(s) and the MAC-P to the UE 1. In such an example the AUSF may be an Home Public Land Mobile Network AUSF and the AMF may in that case be a Visited Public Land Mobile Network (VPLMN) AMF. In such a case, the authentication may have been delegated by the AUSF to the VPLMN AMF.

[00137] As previously discussed, the MAC may be calculated based on a privacy key (e.g., as illustrated in FIG. 4) and a provisioning key to generate a MAC-P (e.g., as illustrated in FIG. 12). In some embodiments in which multiple privacy keys are being provisioned to the UE 1, the same MAC may be calculated over all of the privacy keys sent in the same message.

[00138] FIG. 15 illustrates an example of how the privacy key and MAC-P are related to each other, and what parameters are used as input to the MAC calculation (or expected MAC (XMAC), as appropriate). As shown in FIG. 15, the provisioning key and privacy key are both used to generate a MAC, which may be then used in combination with another privacy key to update the MAC, and so on until all privacy keys are processed. Once all privacy keys are processed, the privacy key(s) and MAC may be sent to the UE.

[00139] In view of all of the above, one or more of the devices or functions described above may be implemented using the example hardware illustrated in FIG. 16. The example hardware includes processing circuitry 11 and communication circuitry 12. The processing circuitry is communicatively coupled to the communication circuitry, e.g., via one or more buses. The processing circuitry may comprise one or more microprocessors, microcontrollers, hardware circuits, discrete logic circuits, hardware registers, digital signal processors (DSPs), field-programmable gate arrays (FPGAs), application-specific integrated circuits (ASICs), or a combination thereof. For example, the processing circuitry may be programmable hardware capable of executing software instructions stored, e.g., as a machine-readable computer program 133 in a memory circuitry 13. The memory circuitry of the various embodiments may comprise any non-transitory machine-readable media known in the art or that may be developed, whether volatile or non-volatile, including but not limited to solid state media (e.g., SRAM, DRAM, DDRAM, ROM, PROM, EPROM, flash memory, solid state drive, etc.), removable storage devices (e.g., Secure Digital (SD) card, miniSD card, microSD card, memory stick, thumb-drive, USB flash drive, ROM cartridge, Universal Media Disc), fixed drive (e.g., magnetic hard disk drive), or the like, wholly or in any combination. According to particular embodiments in which

the hardware is used to implement the UE 1, the memory circuitry may comprise a tamper resistant secure hardware component 8 providing secure storage, such as a 5G-USIM and/or UICC 8a.

[00140] The communication circuitry 12 may be a controller hub configured to control the input and output (I/O) data paths of the hardware. Such I/O data paths may include data paths for exchanging signals over a wireless communication network 30. For example, the communication circuitry may comprise a transceiver configured to send and receive communication signals within and/or between the UE 1, the serving network 2, and/or the home network 3, e.g., over an air, electrical, and/or optical medium.

[00141] The communication circuitry 12 may be implemented as a unitary physical component, or as a plurality of physical components that are contiguously or separately arranged, any of which may be communicatively coupled to any other, or may communicate with any other via the processing circuitry 11. For example, the communication circuitry may comprise transmitter circuitry configured to send communication signals, and receiver circuitry configured to receive communication signals (not shown).

[00142] According to particular embodiments, the hardware illustrated in FIG. 16 may be configured with a plurality of components. These components may include a plurality of communicatively coupled hardware units and/or software modules. One or more of the hardware units may be, e.g., part of the processing circuitry 11. One or more of the software units may be, e.g., stored in the memory circuitry 13 and executed by the processing circuitry.

[00143] For example, hardware such as illustrated in FIG. 16 may be used to implement an authentication server 14 (e.g., an AMF, SEAF 4, AUSF 5) in a home network 3 of a UE 1 and configured with the example components illustrated in FIG. 17 to obtain a subscription identifier, such as a SUPI, of a UE. The components of FIG. 17 include a determining unit or module 15 and an interfacing unit or module 16. The determining unit or module is configured to determine a de-concealing server 19 to use to decrypt the encrypted part of the SUCI, and based on information received from the UE, which of a plurality of de-concealing servers to use to decrypt at least part of a subscription concealed identifier (SUCI) in which the subscription identifier is encrypted. The interfacing unit or module is configured to send the SUCI to the determined de-concealing server and receiving the subscription identifier, e.g. SUPI, in response. In other

words, the interface module is configured to also receive the SUCI generated by the UE, where the SUCI comprises an encrypted part in which at least a part of the SUPI is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI.

[00144] Such an authentication server 14 may additionally or alternatively be configured with the example components illustrated in FIG. 18 to provision a UE 1. The components of FIG. 18 include an obtaining unit or module 17, and a transmitting unit or module 18. The obtaining unit or module is configured to obtaining a message authentication code (MAC) based on a provisioning key specific to the UE 1 and a privacy key of a home network 3 of the UE. The transmitting unit or module is configured to transmit the privacy key and MAC to the UE.

[00145] Such an authentication server 14 may further be configured to additionally or alternatively perform any of the methods described herein with respect to an authentication server, e.g., using any of the above described authentication server hardware or software components.

[00146] Other hardware consistent with the example illustrated in FIG. 16, may be used to implement a de-concealing server 19 (e.g., SDF 6) for providing a subscription identifier of a UE 1 to an authentication server 14, and may be configured with the example components illustrated in FIG. 19. The components of FIG. 19 include a receiving unit or module 20, a decrypting unit or module 21, and a sending unit or module 22. The receiving unit or module is configured to receive, from the authentication server, a SUCI which comprises an encrypted part in which at least a part of the SUPI is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by a UE to encrypt the SUPI in the SUC and which is supported by the de-concealing server. The decrypting unit or module is configured to decrypt at least part of the SUCI, using the encryption scheme indicated by the encryption scheme identifier to obtain the SUPI. The sending unit or module is configured to send the SUPI to the authentication server.

[00147] Such a de-concealing server 19 may additionally or alternatively be configured with the example components illustrated in FIG. 20 to provision a UE 1. The components of FIG. 20 include a generating unit or module 23, and a transmitting unit or module 24. The generating unit or module is configured to generate a Subscription Permanent Identifier (SUPI)

and privacy key for the UE responsive to receiving, from an authentication server 14, a Subscription Concealed Identifier (SUCI) of the UE that indicates that the UE lacks a valid privacy key. The transmitting unit or module is configured to transmit the SUPI and privacy key to the authentication server. Thus the term ‘de-concealing server’ may also be termed a SUCI de-concealing server.

[00148] Such a de-concealing server 19 may further be configured to additionally or alternatively perform any of the methods described herein with respect to a de-concealing server, e.g., using any of the above described de-concealing server hardware or software components.

[00149] Yet other hardware consistent with the example illustrated in FIG. 16, may be used to implement a UE 1 for securely notifying a wireless communication network 30 of a subscription identifier, and may be configured with the example components illustrated in FIG. 21. The components of FIG. 21 include a generating unit or module 25, and a transmitting unit or module 26. The generating unit or module is configured to generate a SUCI which comprises an encrypted part in which at least a part of a SUPI is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI. The transmitting unit or module is configured to transmit the SUCI to an authentication server 14 for forwarding of the SUCI to a de-concealing server 19 capable of decrypting the SUPI.

[00150] Such a UE 1 may additionally or alternatively be configured with the example components illustrated in FIG. 22 to obtain a privacy key. The components of FIG. 22 include a receiving unit or module 27, and a verifying unit or module 28. The receiving unit or module is configured to receiving the privacy key and a message authentication code (MAC) from an authentication server 14. The verifying unit or module is configured to verify the integrity of the privacy key by generating a provisioning key and using the provisioning key and privacy key to reproduce the MAC received from the authentication server, the provisioning key being a shared secret between the UE and the authentication server.

[00151] Such a UE 1 may further be configured to additionally or alternatively perform any of the methods described herein with respect to a UE, e.g., using any of the above-described UE hardware or software components.

[00152] The various methods and processes described herein may be implemented in ways that vary in certain details from the broad descriptions given above. For example, although steps of various processes or methods described herein may be shown and described as being in a sequence or temporal order, the steps of any such processes or methods are not limited to being carried out in any particular sequence or order, absent an indication otherwise. Indeed, the steps in such processes or methods generally may be carried out in various different sequences and orders while still falling within the scope of the present disclosure. The embodiments described herein are to be considered in all respects as illustrative and not restrictive. In particular, all changes coming within the meaning and equivalency range of the enumerated embodiments appended below are intended to be embraced therein.

CLAIMS

1. A method performed by an authentication server in a home network of a user equipment (UE) for obtaining a subscription permanent identifier (SUPI), the method comprising:

receiving a subscription concealed identifier (SUCI) which comprises an encrypted part in which at least a part of the SUPI is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI;

determining a de-concealing server to use to decrypt the encrypted part of the SUCI;
sending the SUCI to the de-concealing server; and
receiving the SUPI in response.

2. The method of claim 1, wherein the clear-text part of the SUCI comprises a public key identifier for a public key of the home network.

3. The method of claim 1, wherein the de-concealing server is one of a plurality of de-concealing servers, and the determining of the de-concealing server is based on information received from the UE.

4. The method of claim 1, wherein the encryption scheme is a null-encryption scheme.

5. The method of claim 1, further comprising receiving the SUCI from the UE as part of a registration procedure for registering the UE with a wireless communication network.

6. The method of claim 1, further comprising receiving the SUCI from the UE via an authentication request from a Security Anchor Function.

7. The method of claim 1, further comprising sending the SUCI and a request for an authentication vector for authenticating the UE to the determined de-concealing server in the same message.

8. The method of claim 1, wherein the SUPI comprises a Mobile Subscription Identification Number, MSIN, a Mobile Country Code, MCC, and a Mobile Network Code, MNC, and where the MSIN is encrypted in the encrypted part of the SUCI, and the MCC and the MNC are the home network identifier in the clear-text part of the SUCI.

9. The method of claim 1, wherein the SUPI is a Network Access Identifier.

10. The method of claim 1, wherein the encryption scheme is an Elliptic Curve Integrated Encryption Scheme (ECIES) and the clear-text part of the SUCI comprises an ephemeral public key of the UE for use in the ECIES.

11. A method, performed by a de-concealing server, for providing a subscription permanent identifier (SUPI) to an authentication server, the method comprising:

receiving, from the authentication server, a subscription concealed identifier (SUCI) which comprises an encrypted part in which at least a part of the SUPI is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by a UE to encrypt the SUPI in the SUCI and which is supported by the de-concealing server;

decrypting the encrypted part of the SUCI, using the encryption scheme indicated by the encryption scheme identifier to obtain the SUPI; and

sending the SUPI to the authentication server.

12. The method of claim 11, wherein the clear-text part of the SUCI also comprises a key identifier used for identifying a decryption key used for decrypting the SUPI.

13. A method performed by a user equipment (UE), the method comprising:

generating a subscription concealed identifier (SUCI) which comprises an encrypted part in which at least a part of a subscription permanent identifier (SUPI) is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI; and

transmitting the SUCI to an authentication server for forwarding of the SUCI to a de-concealing server capable of decrypting the SUPI.

14. The method of claim 13, wherein the SUCI is transmitted in a request to register with a wireless communication network (30).

15. The method of claim 13, wherein generating the SUCI comprises using a tamper resistant secure hardware component of the UE to generate the SUCI.

16. The method of claim 13, wherein transmitting the SUCI to the authentication server comprises transmitting the SUCI to the authentication server in response to an identifier request message received from an Authentication and Mobility management Function, AMF, as part of a procedure for registering the UE with a wireless communication network.

17. The method of claim 13, wherein the clear-text part comprises a public key identifier for the home network.

18. The method of claim 13, wherein the encryption scheme is a null-encryption scheme.

19. The method of claim 13, wherein the encryption scheme is an Elliptic Curve Integrated Encryption Scheme.

20. A user equipment (UE) comprising:
processing circuitry and memory circuitry, the memory circuitry containing instructions executable by the processing circuitry, wherein the UE is operative to:
generate a subscription concealed identifier (SUCI) which comprises an encrypted part in which at least a part of a Subscription Permanent Identifier (SUPI) is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI; and
transmit the SUCI to an authentication server for forwarding of the SUCI to a de-concealing server capable of decrypting the SUPI.

21. The UE of claim 20, wherein the clear-text part comprises a public key identifier for the home network.

22. The UE of claim 20, wherein the SUPI comprises a Mobile Subscription Identification Number.

23. The UE of claim 20, wherein the SUPI is a Network Access Identifier.

ABSTRACT

A method performed by an authentication server in a home network of a UE for obtaining a subscription permanent identifier, SUPI. The method comprises: receiving a SUCI which comprises an encrypted part in which at least a part of the SUPI is encrypted, and a clear-text part which comprises a home network identifier and an encryption scheme identifier that identifies an encryption scheme used by the UE to encrypt the SUPI in the SUCI; determining a de-concealing server to use to decrypt the encrypted part of the SUCI; sending the SUCI to the de-concealing server; and receiving the SUPI in response. Methods performed by a UE and a de-concealing server are also disclosed. Furthermore, UEs, de-concealing servers, authentication servers, computer program and a memory circuitry are also disclosed.

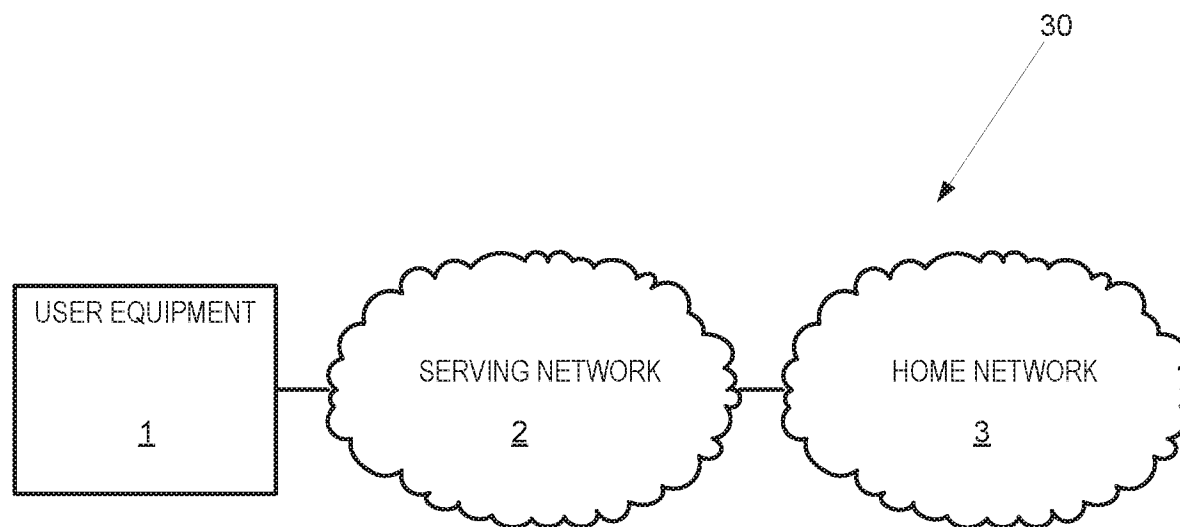


FIG. 1

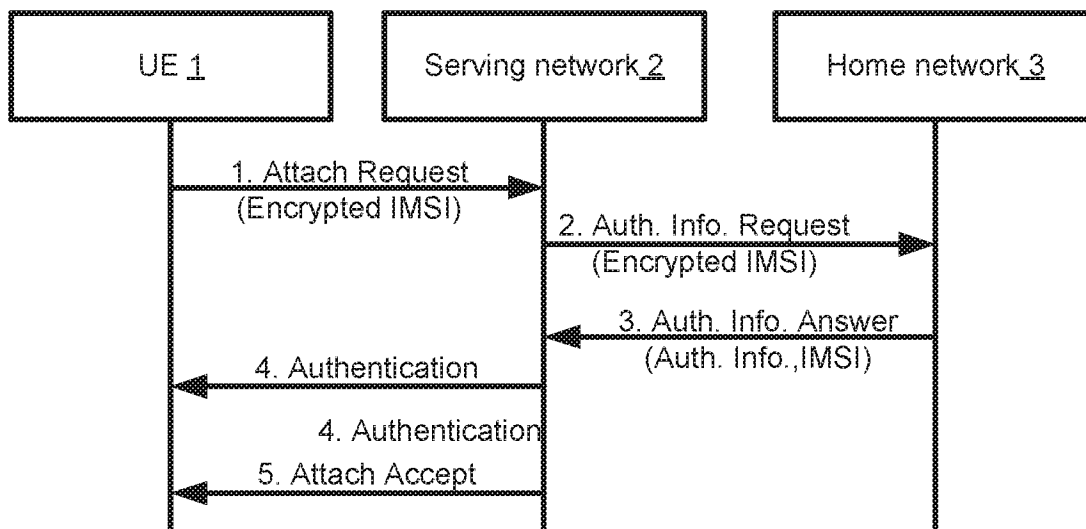


Fig. 2

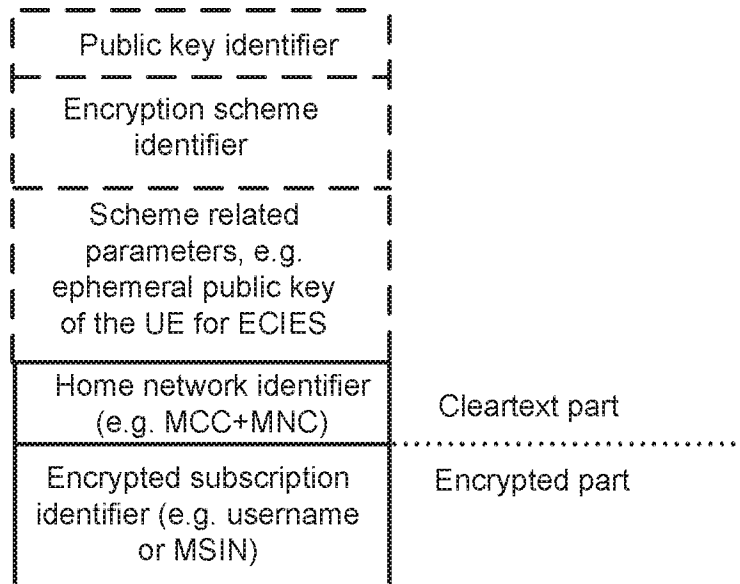


Fig. 3

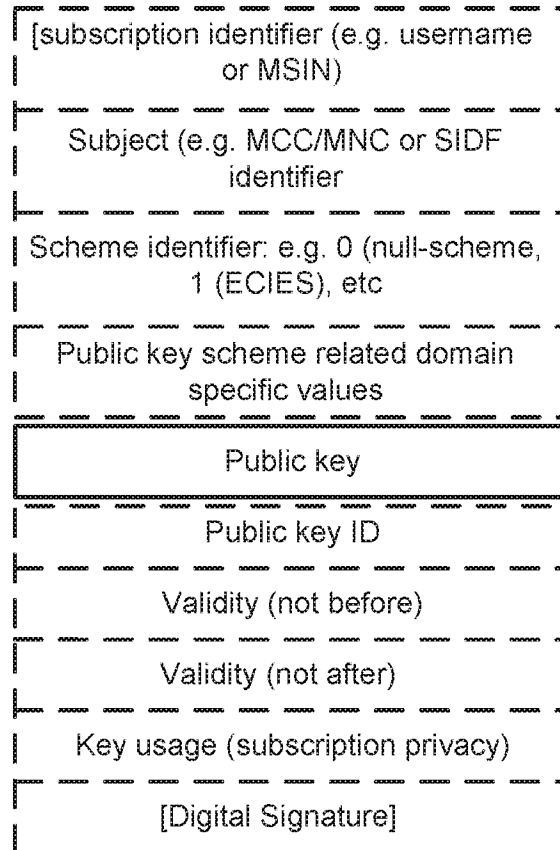


Fig. 4

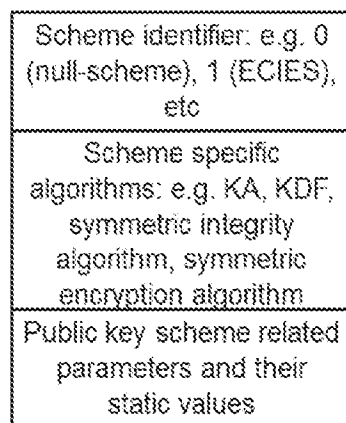


Fig. 5

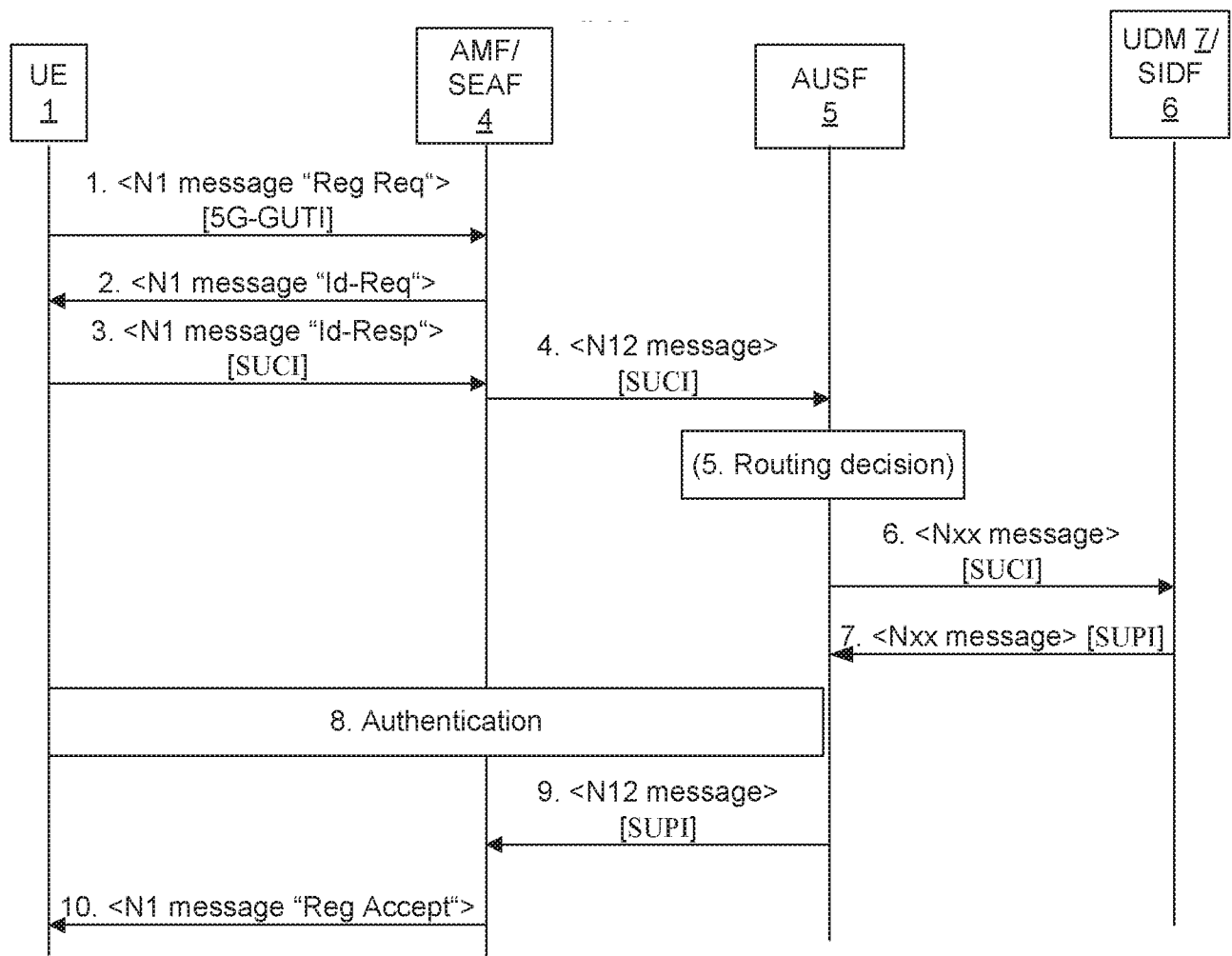


Fig. 6

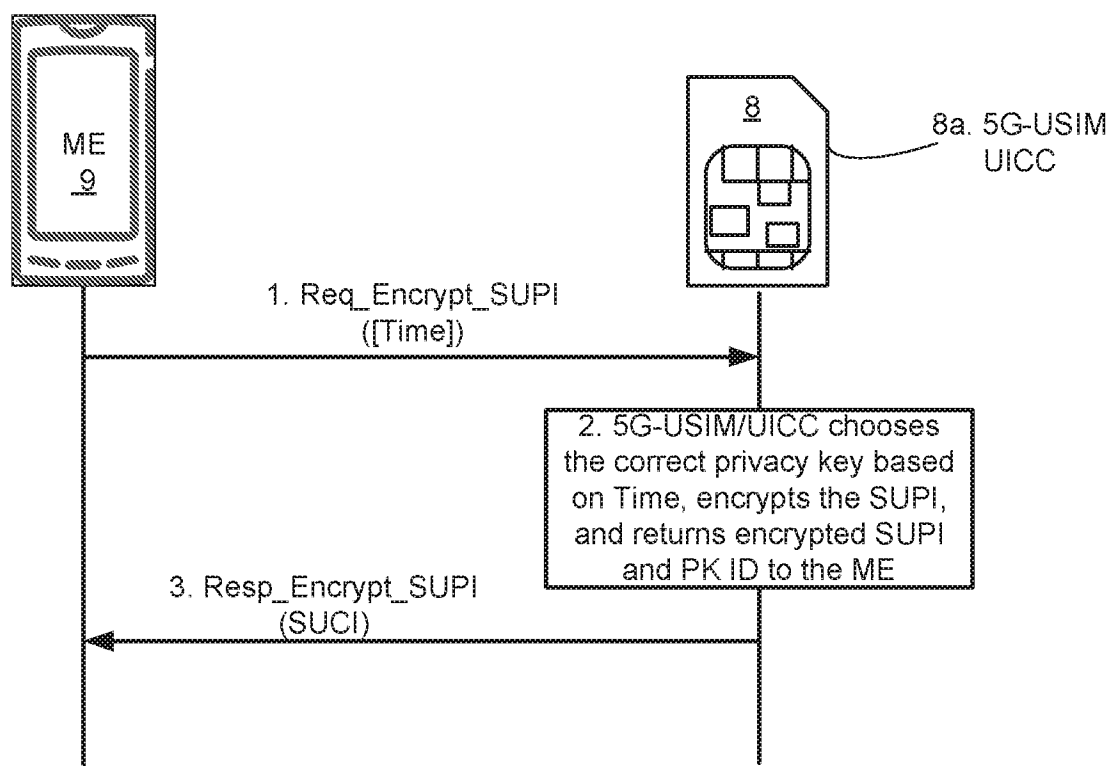


Fig. 7

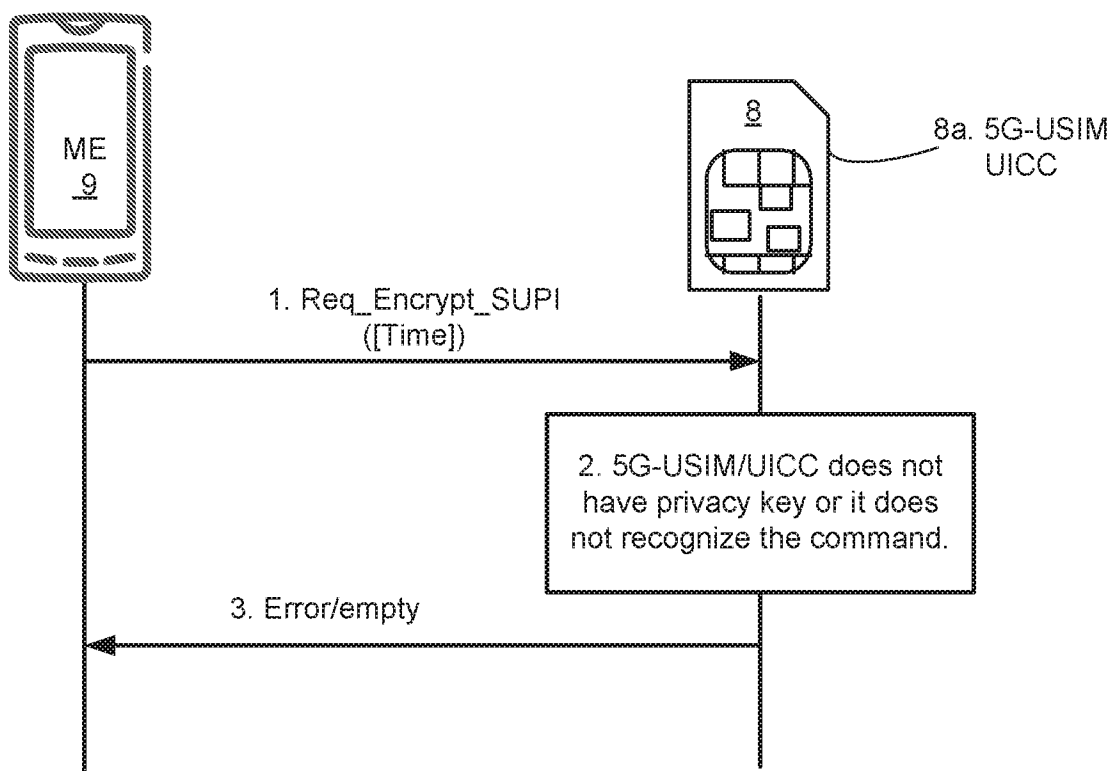


Fig. 8

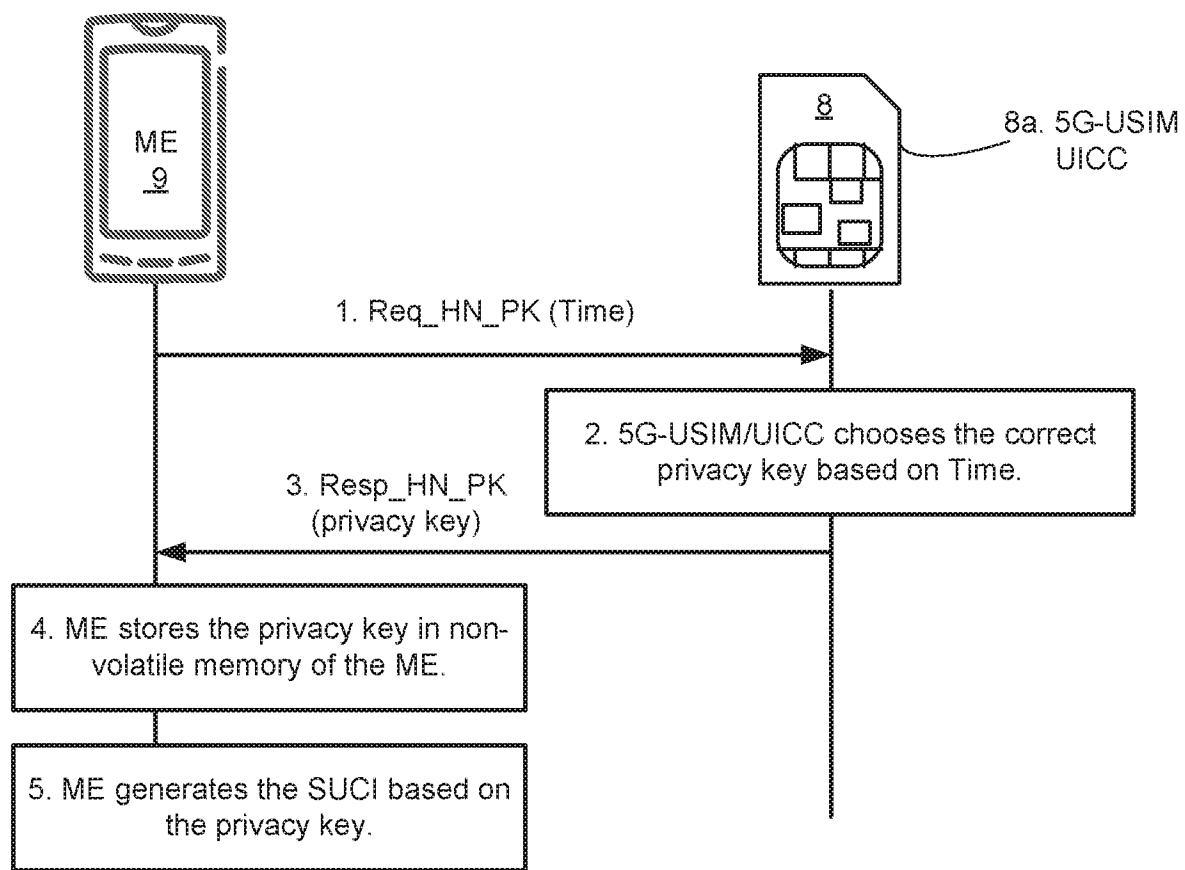


Fig. 9

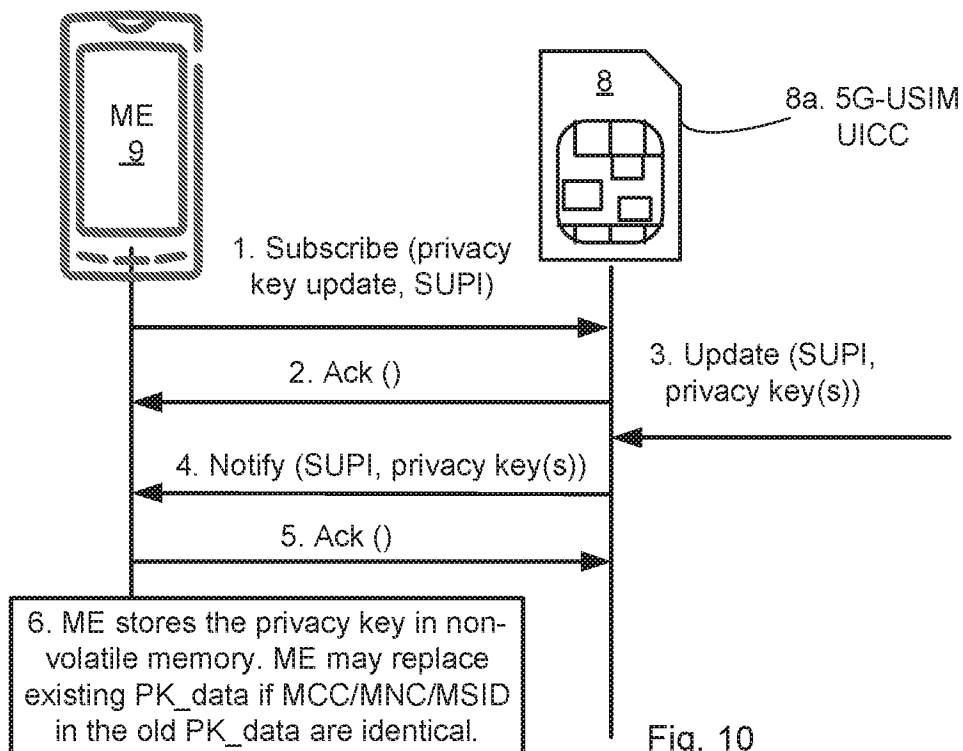


Fig. 10

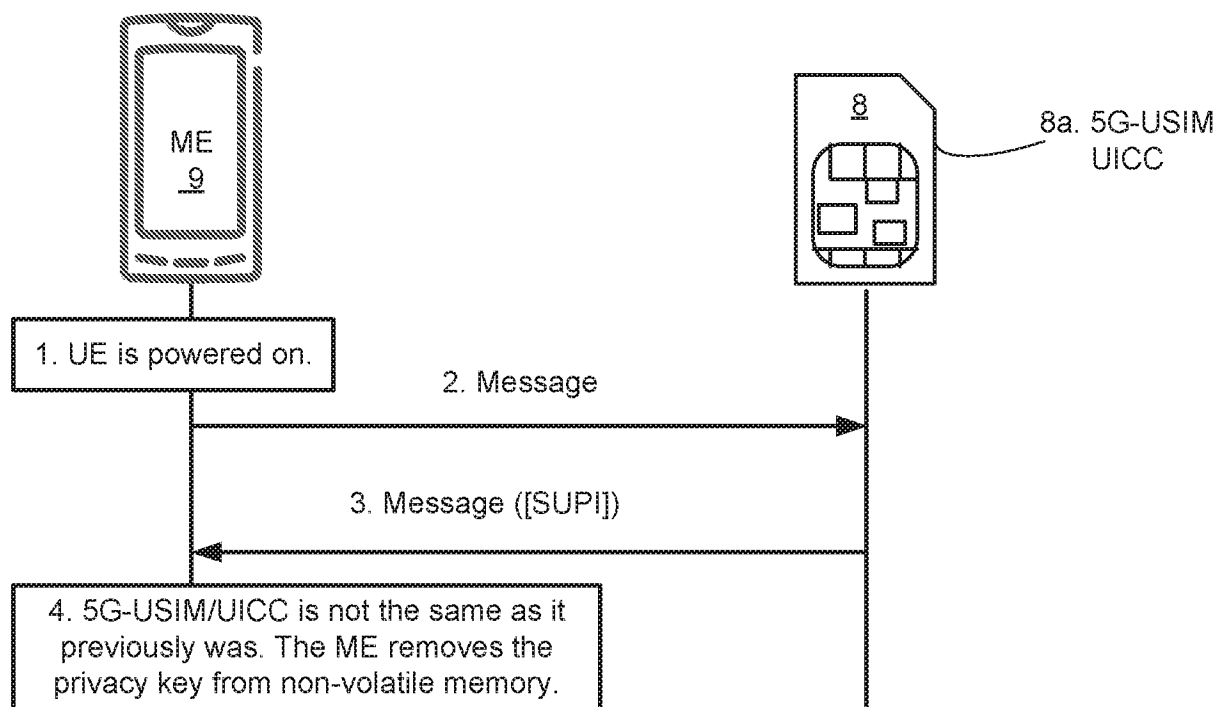


Fig. 11

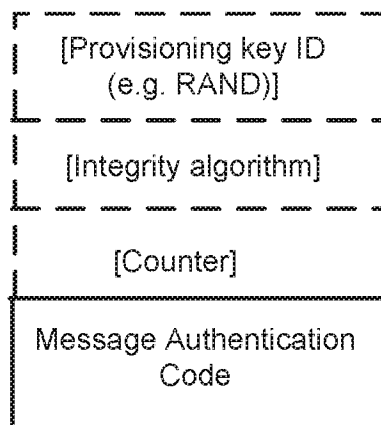
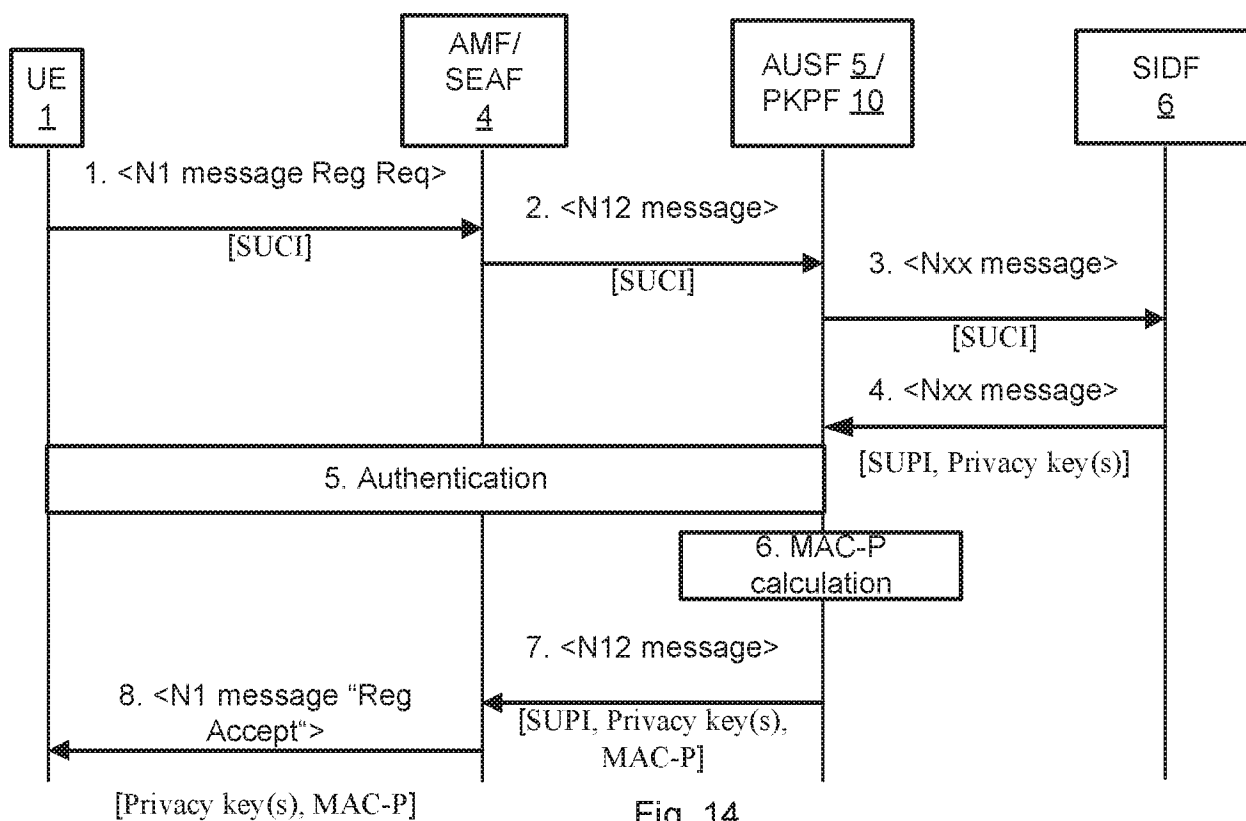
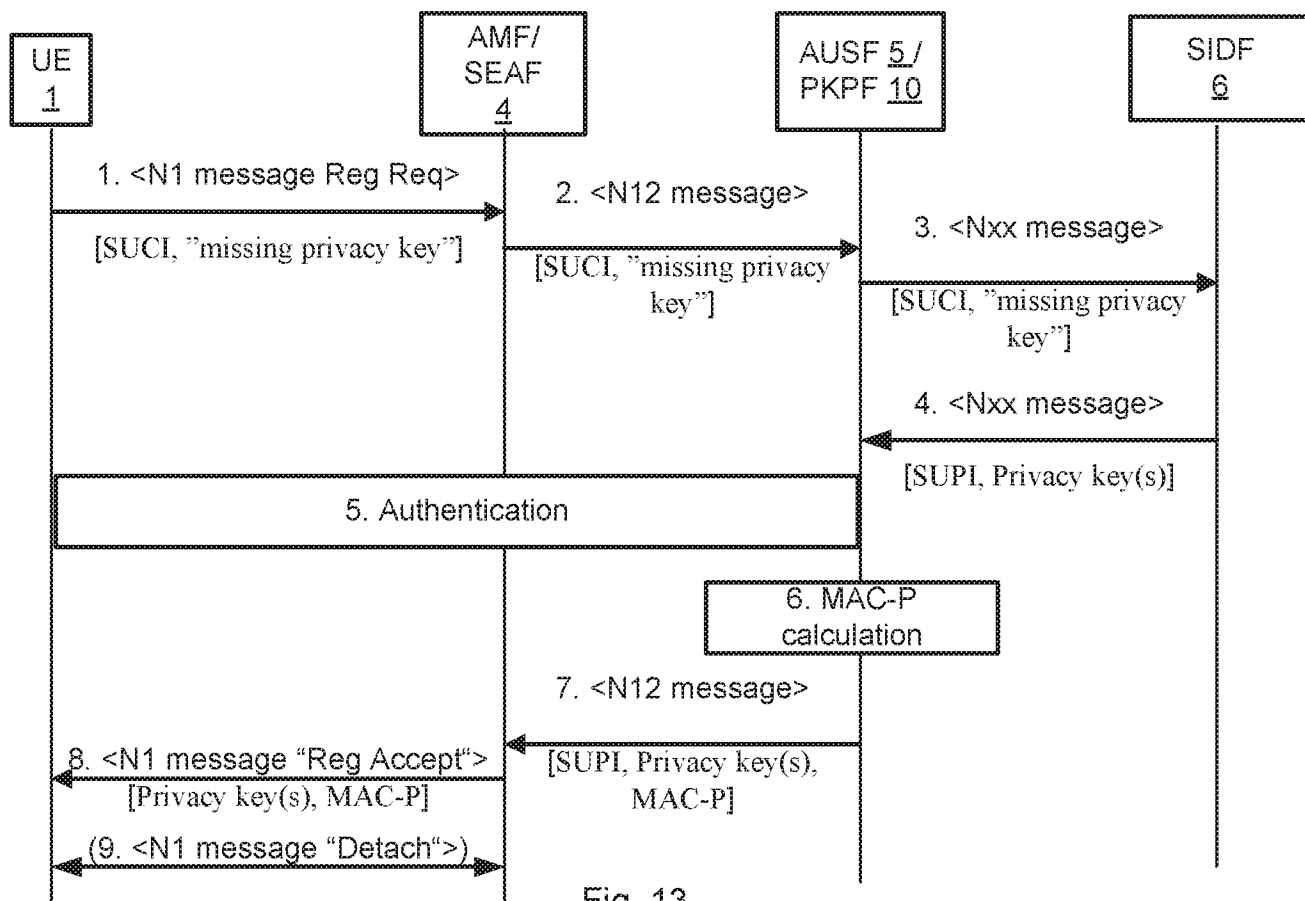


Fig. 12



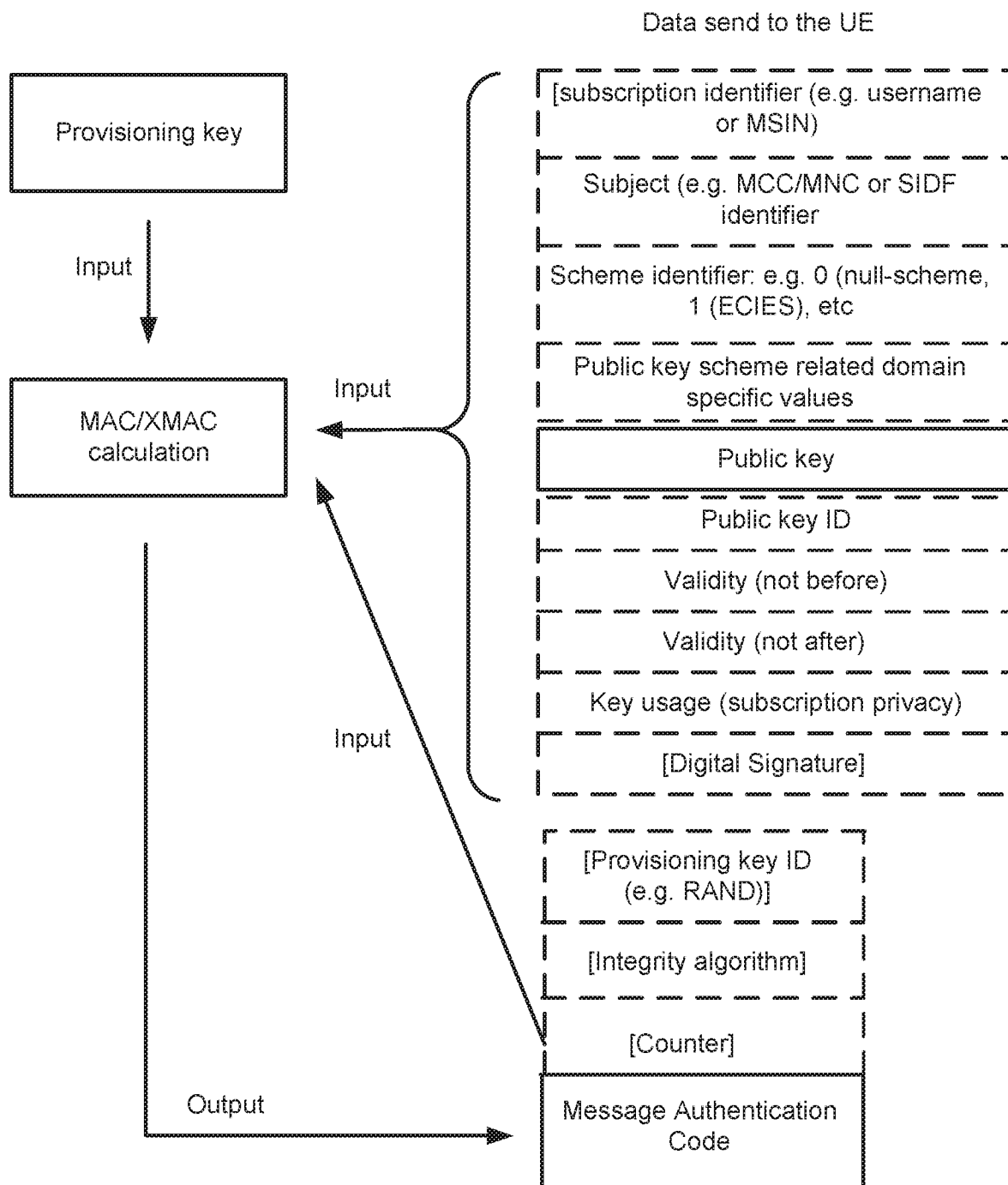


Fig. 15

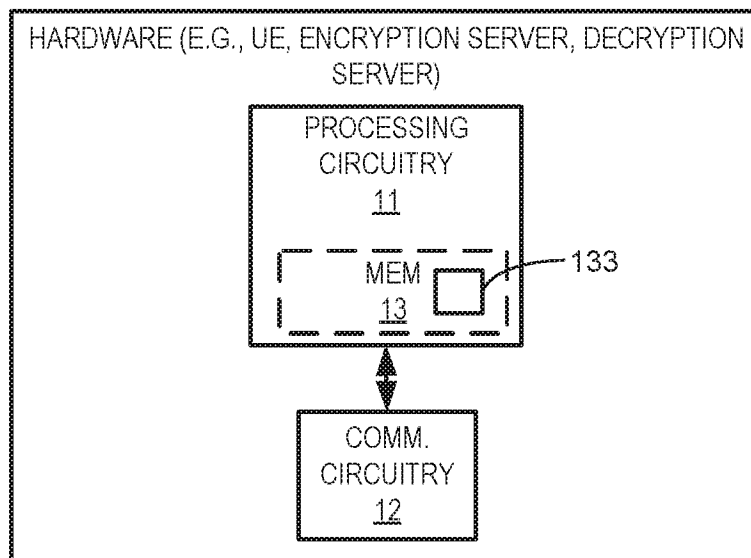


Fig. 16

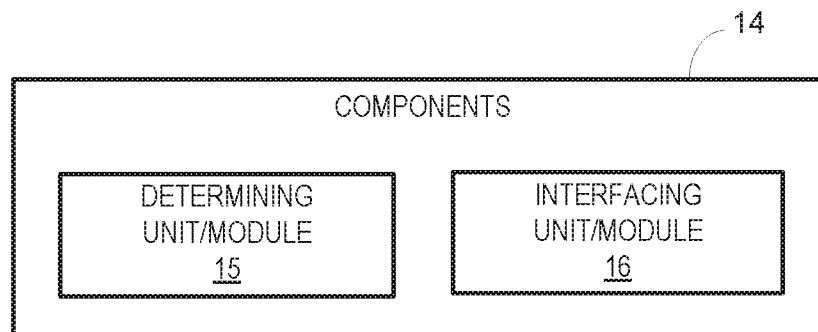


Fig. 17

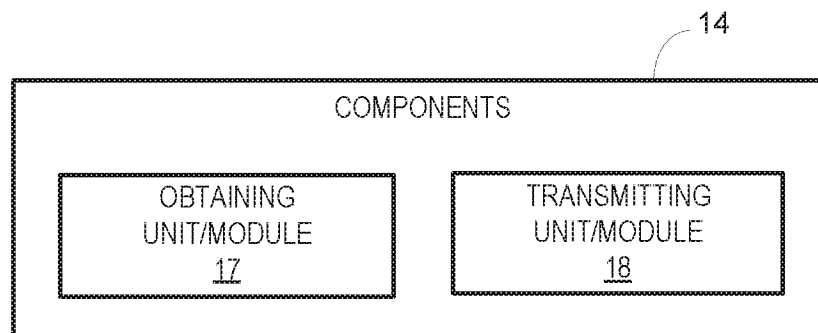


Fig. 18

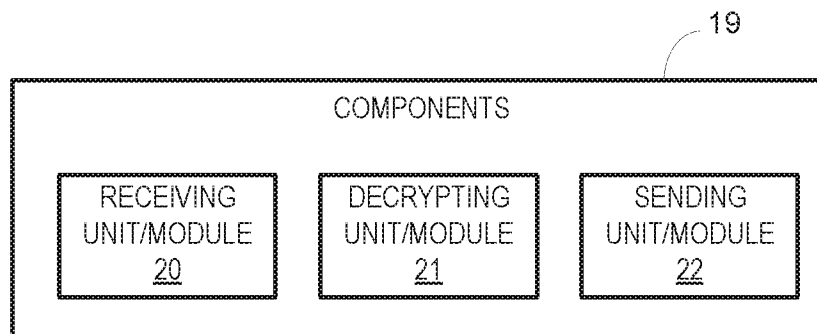


Fig. 19

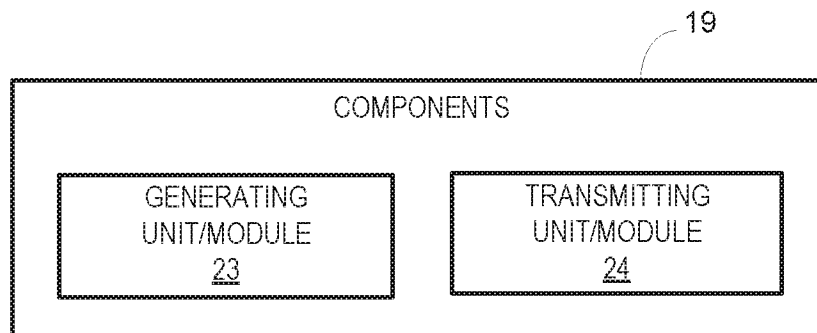


Fig. 20

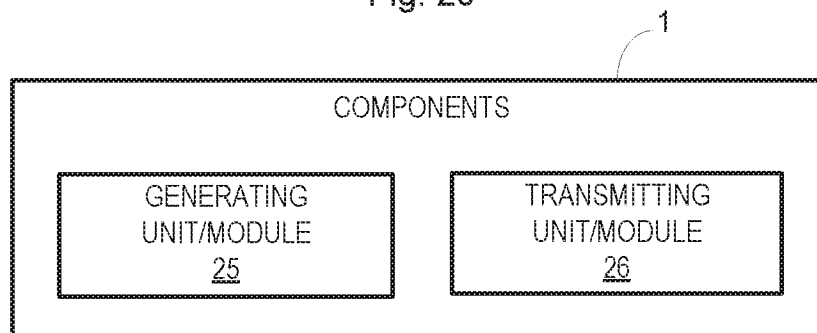


Fig. 21

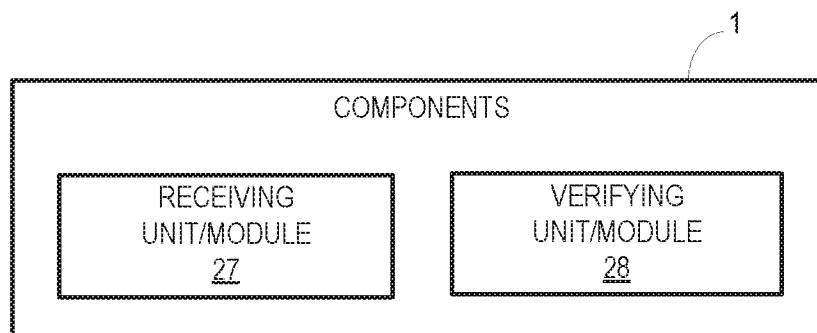


Fig. 22

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	3602-1734US2
		Application Number	
Title of Invention	SUBSCRIPTION CONCEALED IDENTIFIER		
The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76. This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.			

Secrecy Order 37 CFR 5.2:

☐	Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)
--------------------------	---

Inventor Information:

Inventor 1					Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Vesa		TORVINEN		
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service					
City	Sauvo	Country of Residence ⁱ	FI		
Mailing Address of Inventor:					
Address 1		Sauvontie 42			
Address 2					
City	Sauvo	State/Province			
Postal Code	FI-21570	Country ⁱ	FI		
Inventor 2					Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Noamen		BEN HENDA		
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service					
City	Stockholm	Country of Residence ⁱ	SE		
Mailing Address of Inventor:					
Address 1		Tumultgränd 228			
Address 2					
City	Stockholm	State/Province			
Postal Code	SE-162 47	Country ⁱ	SE		
Inventor 3					Remove
Legal Name					

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	3602-1734US2
		Application Number	
Title of Invention	SUBSCRIPTION CONCEALED IDENTIFIER		

Prefix	Given Name	Middle Name	Family Name	Suffix
	David		CASTELLANOS ZAMORA	
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service				
City	Madrid	Country of Residence ⁱ	ES	

Mailing Address of Inventor:				
Address 1	C/ Embajadores 256 1°B			
Address 2				
City	Madrid	State/Province		
Postal Code	28045	Country ⁱ	ES	
Inventor 4				Remove
Legal Name				

Prefix	Given Name	Middle Name	Family Name	Suffix
	Prajwol	Kumar	NAKARMI	
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service				
City	Sollentuna	Country of Residence ⁱ	SE	

Mailing Address of Inventor:				
Address 1	Stupvägen 17			
Address 2				
City	Sollentuna	State/Province		
Postal Code	SE-191 42	Country ⁱ	SE	
Inventor 5				Remove
Legal Name				

Prefix	Given Name	Middle Name	Family Name	Suffix
	Pasi		SAARINEN	
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service				
City	Järfälla	Country of Residence ⁱ	SE	

Mailing Address of Inventor:				
Address 1	Ripvägen 19A			
Address 2				
City	Järfälla	State/Province		
Postal Code	SE-175 64	Country ⁱ	SE	

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	3602-1734US2
		Application Number	
Title of Invention	SUBSCRIPTION CONCEALED IDENTIFIER		

Inventor 6					Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Monica		WIFVESSON		
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service					
City	Lund	Country of Residence ⁱ		SE	
Mailing Address of Inventor:					
Address 1		Kruthornsgränden 3			
Address 2					
City	Lund	State/Province			
Postal Code	SE-226 52	Country ⁱ	SE		
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button. Add					

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).			
☐ An Address is being provided for the correspondence Information of this application.			
Customer Number	06449		
Email Address	pto-pat-email@rfem.com	Add Email	Remove Email

Application Information:

Title of the Invention	SUBSCRIPTION CONCEALED IDENTIFIER		
Attorney Docket Number	3602-1734US2	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	11	Suggested Figure for Publication (if any)	

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	3602-1734US2
		Application Number	
Title of Invention	SUBSCRIPTION CONCEALED IDENTIFIER		

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)
Customer Number	06449		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending	Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Continuation of	PCT/EP2018/069432	2018-07-17

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	3602-1734US2
		Application Number	
Title of Invention	SUBSCRIPTION CONCEALED IDENTIFIER		
Prior Application Status	Expired	Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
PCT/EP2018/069432	Claims benefit of provisional	62/536632	2017-07-25
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.			

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)ⁱ the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Remove
			Access Code ⁱ (if applicable)
Additional Foreign Priority Data may be generated within this form by selecting the Add button.			

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.

☐ NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	3602-1734US2
	Application Number	
Title of Invention	SUBSCRIPTION CONCEALED IDENTIFIER	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	3602-1734US2
		Application Number	
Title of Invention	SUBSCRIPTION CONCEALED IDENTIFIER		

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.			
Applicant 1			
If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.			
Clear			
☒ Assignee	☐ Legal Representative under 35 U.S.C. 117	☐ Joint Inventor	
☐ Person to whom the inventor is obligated to assign.		☐ Person who shows sufficient proprietary interest	
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:			
Name of the Deceased or Legally Incapacitated Inventor:			
If the Applicant is an Organization check here. ☒			
Organization Name	Telefonaktiebolaget LM Ericsson (publ)		
Mailing Address Information For Applicant:			
Address 1			
Address 2			
City	Stockholm	State/Province	
Country	SE	Postal Code	SE-164 83
Phone Number		Fax Number	
Email Address			
Additional Applicant Data may be generated within this form by selecting the Add button.			

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	3602-1734US2
		Application Number	
Title of Invention	SUBSCRIPTION CONCEALED IDENTIFIER		

Assignee 1			
Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.			
If the Assignee or Non-Applicant Assignee is an Organization check here. ☒			
Organization Name	Telefonaktiebolaget LM Ericsson (publ)		
Mailing Address Information For Assignee including Non-Applicant Assignee:			
Address 1			
Address 2			
City	Stockholm	State/Province	
Country ⁱ	SE	Postal Code	SE-164 83
Phone Number		Fax Number	
Email Address			
Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.			

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). However, if this Application Data Sheet is submitted with the **INITIAL** filing of the application **and** either box A or B is **not** checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Brian Rosenbloom/		Date (YYYY-MM-DD)	2018-11-26	
First Name	Brian	Last Name	Rosenbloom	Registration Number	41276
Additional Signature may be generated within this form by selecting the Add button.					

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	3602-1734US2
		Application Number	
Title of Invention	SUBSCRIPTION CONCEALED IDENTIFIER		

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

- 1 The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
- 2 A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
- 3 A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
- 4 A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
- 5 A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
- 6 A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
- 7 A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
- 8 A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
- 9 A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:				
Filing Date:				
Title of Invention:	SUBSCRIPTION CONCEALED IDENTIFIER			
First Named Inventor/Applicant Name:	Vesa TORVINEN			
Filer:	Brian S. Rosenbloom/Xania Steele			
Attorney Docket Number:	3602-1734US2			
Filed as Large Entity				
Filing Fees for Track I Prioritized Examination - Nonprovisional Application under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
UTILITY APPLICATION FILING	1011	1	300	300
UTILITY SEARCH FEE	1111	1	660	660
UTILITY EXAMINATION FEE	1311	1	760	760
REQUEST FOR PRIORITIZED EXAMINATION	1817	1	4000	4000
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	1202	3	100	300
INDEPENDENT CLAIMS IN EXCESS OF 3	1201	1	460	460

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous-Filing:				
PUBL. FEE- EARLY, VOLUNTARY, OR NORMAL	1504	1	0	0
PROCESSING FEE, EXCEPT PROV. APPLS.	1830	1	140	140
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				6620

Electronic Acknowledgement Receipt

EFS ID:	34390524
Application Number:	16200037
International Application Number:	
Confirmation Number:	8611
Title of Invention:	SUBSCRIPTION CONCEALED IDENTIFIER
First Named Inventor/Applicant Name:	Vesa TORVINEN
Customer Number:	6449
Filer:	Brian S. Rosenbloom/Xania Steele
Filer Authorized By:	Brian S. Rosenbloom
Attorney Docket Number:	3602-1734US2
Receipt Date:	26-NOV-2018
Filing Date:	
Time Stamp:	16:46:16
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	\$6620
RAM confirmation Number	112718INTEFSW00004037022135
Deposit Account	022135
Authorized User	Xania Steele

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

Lenovo Ex. 1009

Page 290

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	TrackOne Request	3602-1734US2_Track-One-Request.pdf	117483	no	2
			aa9d09993bfeef16ed31d8931e560c4048fe f29c		

Warnings:**Information:**

2		3602-1734US2_Specification.pdf	168312	yes	35
			0e5000d5b39e5c6293118386fbf8a11401e e5055		

Multipart Description/PDF files in .zip description

	Document Description	Start	End
	Specification	1	30
	Claims	31	34
	Abstract	35	35

Warnings:**Information:**

3	Drawings-only black and white line drawings	3602-1734US2_Drawings.pdf	191889	no	11
			73ab704b92cdb47046ca948d8e88453872 dab7fd		

Warnings:**Information:**

4	Application Data Sheet	3602-1734US2_ADS.pdf	116936	no	10
			7519fe08d0185a52b4d2609503c627dc952 4295f		

Warnings:**Information:**

This is not an USPTO supplied ADS fillable form

5	Fee Worksheet (SB06)	fee-info.pdf	42924	no	2
			34084e0df05d8d949a2e764e41ad9687c25f1fd9		

Warnings:

Information:

Total Files Size (in bytes):	637544
-------------------------------------	--------

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.