



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
62/502,266	05/05/2017		260	820662-US-PSP		

CONFIRMATION NO. 6444

FILING RECEIPT



0000000091387609

46304
RYAN, MASON & LEWIS, LLP
48 South Service Road
Suite 100
Melville, NY 11747

Date Mailed: 05/16/2017

Receipt is acknowledged of this provisional patent application. It will not be examined for patentability and will become abandoned not later than twelve months after its filing date. 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)

Suresh P. Nair, Whippany, NJ;
Anja Jerichow, Grafing, GERMANY;
Annett Seefeldt, Regensburg, GERMANY;

Applicant(s)

Suresh P. Nair, Whippany, NJ;
Anja Jerichow, Grafing, GERMANY;
Annett Seefeldt, Regensburg, GERMANY;

Power of Attorney:

William Lewis--39274

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: 05/15/2017

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 62/502,266**

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No

Title

PRIVACY INDICATORS FOR CONTROLLING AUTHENTICATION REQUESTS

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.

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	820662-US-PSP
		Application Number	
Title of Invention	PRIVACY INDICATORS FOR CONTROLLING AUTHENTICATION REQUESTS		
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	
	Suresh	P.	Nair		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					
City	Whippany	State/Province	NJ	Country of Residenceⁱ	US
Mailing Address of Inventor:					
Address 1	Alcatel-Lucent USA Inc.				
Address 2	600-700 Mountain Avenue				
City	Murray Hill	State/Province	NJ		
Postal Code	07974	Countryⁱ	US		
Inventor 2					Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Anja		Jerichow		
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service					
City	Grafing	Country of Residenceⁱ	DE		
Mailing Address of Inventor:					
Address 1	Nokia Solutions and Networks GmbH & Co. KG				
Address 2	Werinherstraße 91				
City	München	State/Province			
Postal Code	81541	Countryⁱ	DE		
Inventor 3					Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Annett		Seefeldt		

Lenovo Ex. 1008

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	820662-US-PSP
		Application Number	
Title of Invention	PRIVACY INDICATORS FOR CONTROLLING AUTHENTICATION REQUESTS		

Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service			
City	Regensburg	Country of Residence ⁱ	DE
Mailing Address of Inventor:			
Address 1	Nokia Solutions and Networks GmbH & Co. KG		
Address 2	Werinherstraße 91		
City	München	State/Province	
Postal Code	81541	Country ⁱ	DE
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	46304		
Email Address	nyoffice@rml-law.com	Add Email	Remove Email

Application Information:

Title of the Invention	PRIVACY INDICATORS FOR CONTROLLING AUTHENTICATION REQUESTS		
Attorney Docket Number	820662-US-PSP	Small Entity Status Claimed ☐	
Application Type	Provisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	7	Suggested Figure for Publication (if any)	

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

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	820662-US-PSP
		Application Number	
Title of Invention	PRIVACY INDICATORS FOR CONTROLLING AUTHENTICATION REQUESTS		

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	46304		

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			Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
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 Data Sheet 37 CFR 1.76		Attorney Docket Number	820662-US-PSP
		Application Number	
Title of Invention	PRIVACY INDICATORS FOR CONTROLLING AUTHENTICATION REQUESTS		

Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	 Access Code ^j (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	820662-US-PSP
		Application Number	
Title of Invention	PRIVACY INDICATORS FOR CONTROLLING AUTHENTICATION REQUESTS		

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	820662-US-PSP
		Application Number	
Title of Invention	PRIVACY INDICATORS FOR CONTROLLING AUTHENTICATION REQUESTS		

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. ☐				
Prefix	Given Name	Middle Name	Family Name	Suffix
Mailing Address Information For Applicant:				
Address 1				
Address 2				
City		State/Province		
Country		Postal Code		
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	820662-US-PSP
		Application Number	
Title of Invention	PRIVACY INDICATORS FOR CONTROLLING AUTHENTICATION REQUESTS		

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 Alcatel-Lucent USA Inc.

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1		600 Mountain Avenue	
Address 2			
City	Murray Hill	State/Province	NJ
Country ⁱ	US	Postal Code	07974
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

Assignee 2

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 Nokia Technologies Oy

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	820662-US-PSP
		Application Number	
Title of Invention	PRIVACY INDICATORS FOR CONTROLLING AUTHENTICATION REQUESTS		

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1		Karaportti 3	
Address 2			
City	Espoo	State/Province	
Country ⁱ	FI	Postal Code	02610
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	/William E. Lewis/		Date (YYYY-MM-DD)	2017-05-05	
First Name	William E.	Last Name	Lewis	Registration Number	39274

Additional Signature may be generated within this form by selecting the Add button.

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.**

Provisional Application for Patent Cover Sheet

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c)

Inventor(s)

Inventor 1

Remove

Given Name

Middle Name

Family Name

City

State

Country j

Suresh

P.

Nair

Whippany

NJ

US

Inventor 2

Remove

Given Name

Middle Name

Family Name

City

State

Country j

Anja

Jerichow

Graefing

DE

Inventor 3

Remove

Given Name

Middle Name

Family Name

City

State

Country j

Annett

Seefeldt

Regensburg

DE

All Inventors Must Be Listed – Additional Inventor Information blocks may be generated within this form by selecting the **Add** button.**Add****Title of Invention**

PRIVACY INDICATORS FOR CONTROLLING AUTHENTICATION REQUESTS

Attorney Docket Number (if applicable)

820662-US-PSP

Correspondence Address

Direct all correspondence to (select one):

☒ The address corresponding to Customer Number☐ Firm or Individual Name

Customer Number

46304

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Entity Status

Applicant claims small entity status under 37 CFR 1.27

- ☐ Yes, applicant qualifies for small entity status under 37 CFR 1.27
- ☒ No

Warning

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

Signature

Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/William E. Lewis/			Date (YYYY-MM-DD)	2017-05-05
First Name	William E.	Last Name	Lewis	Registration Number (If appropriate)	39274

This collection of information is required by 37 CFR 1.51. 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 8 hours 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. **This form can only be used when in conjunction with EFS-Web. If this form is mailed to the USPTO, it may cause delays in handling the provisional application.**

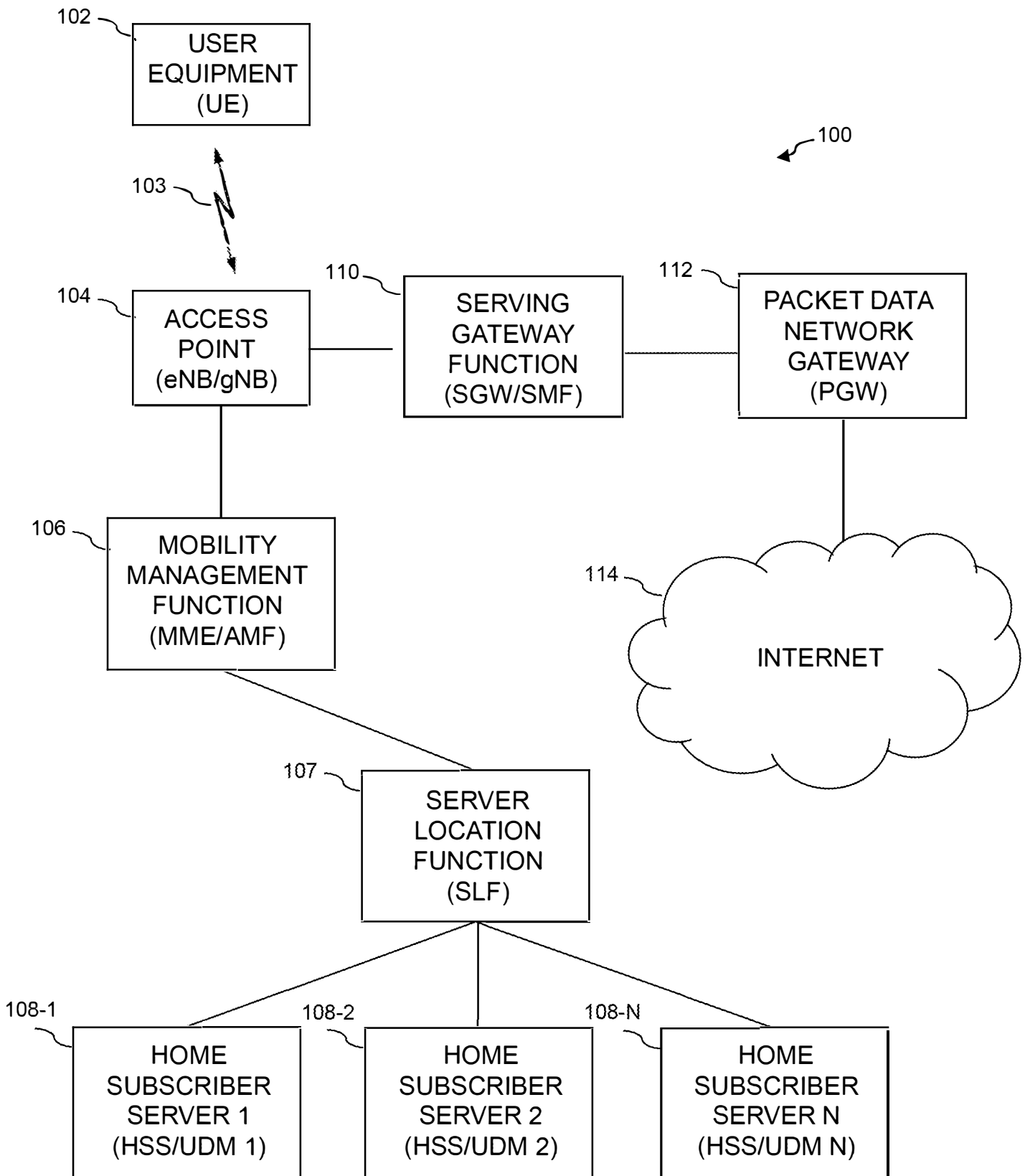


FIG. 1

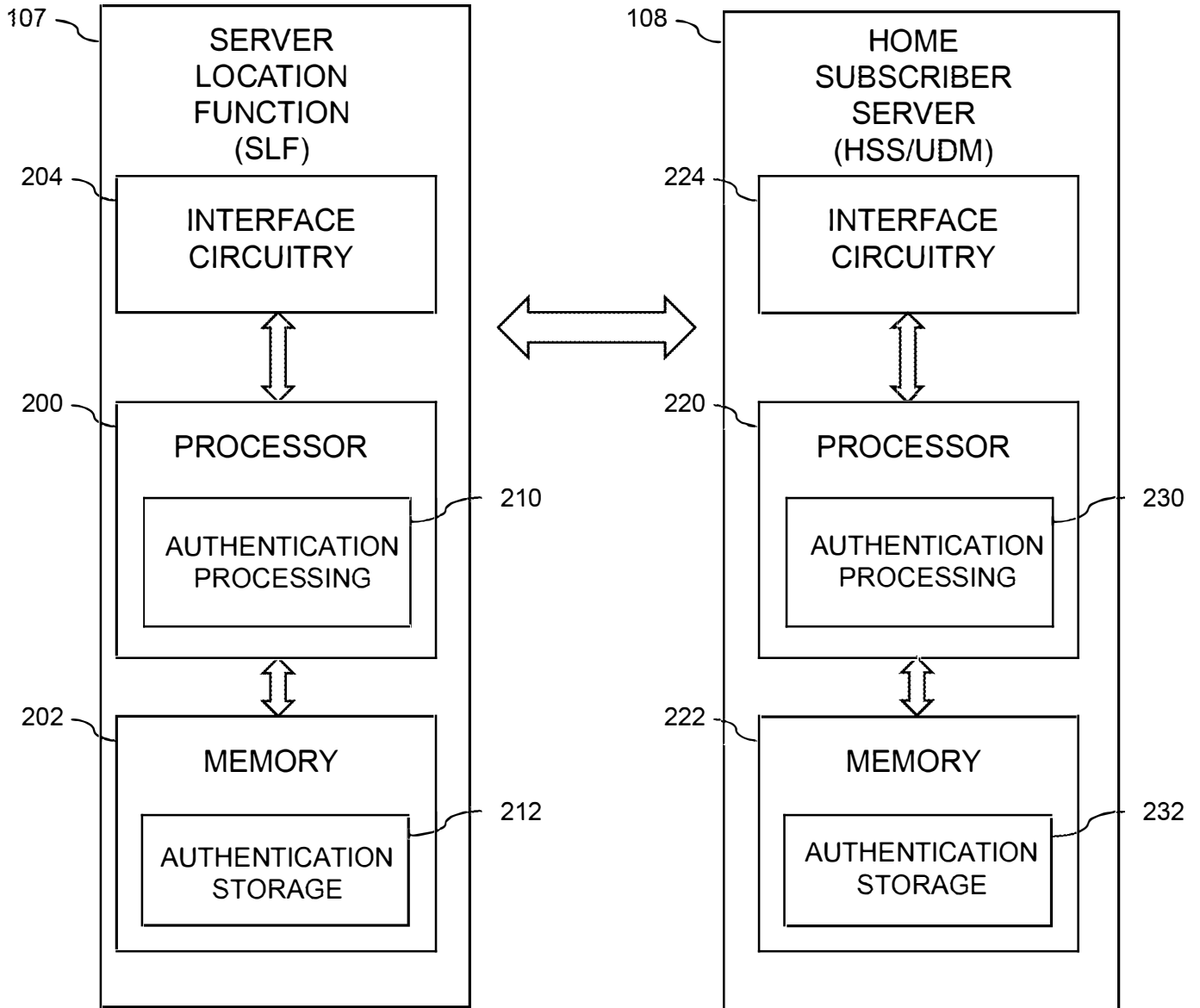


FIG. 2

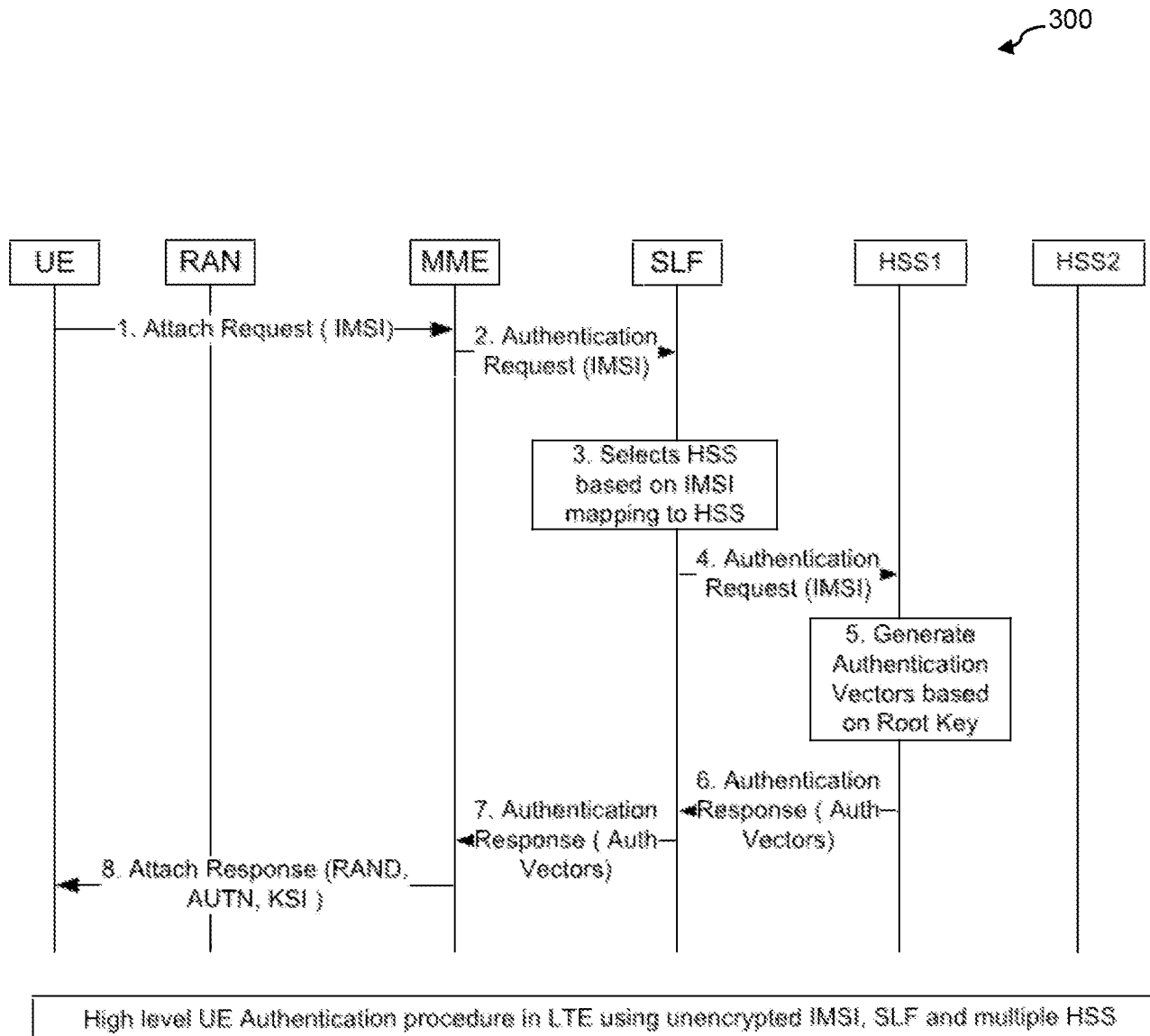
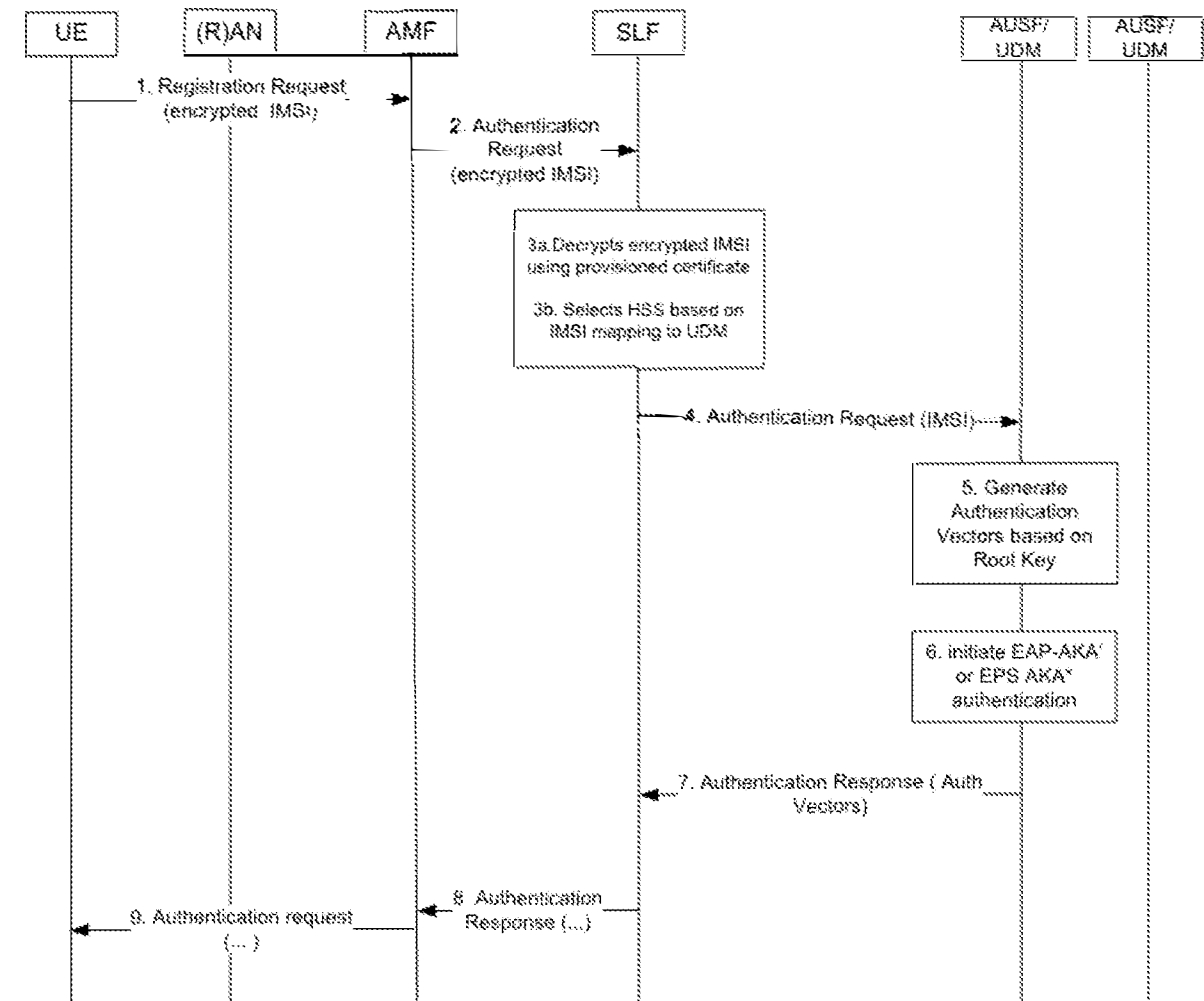


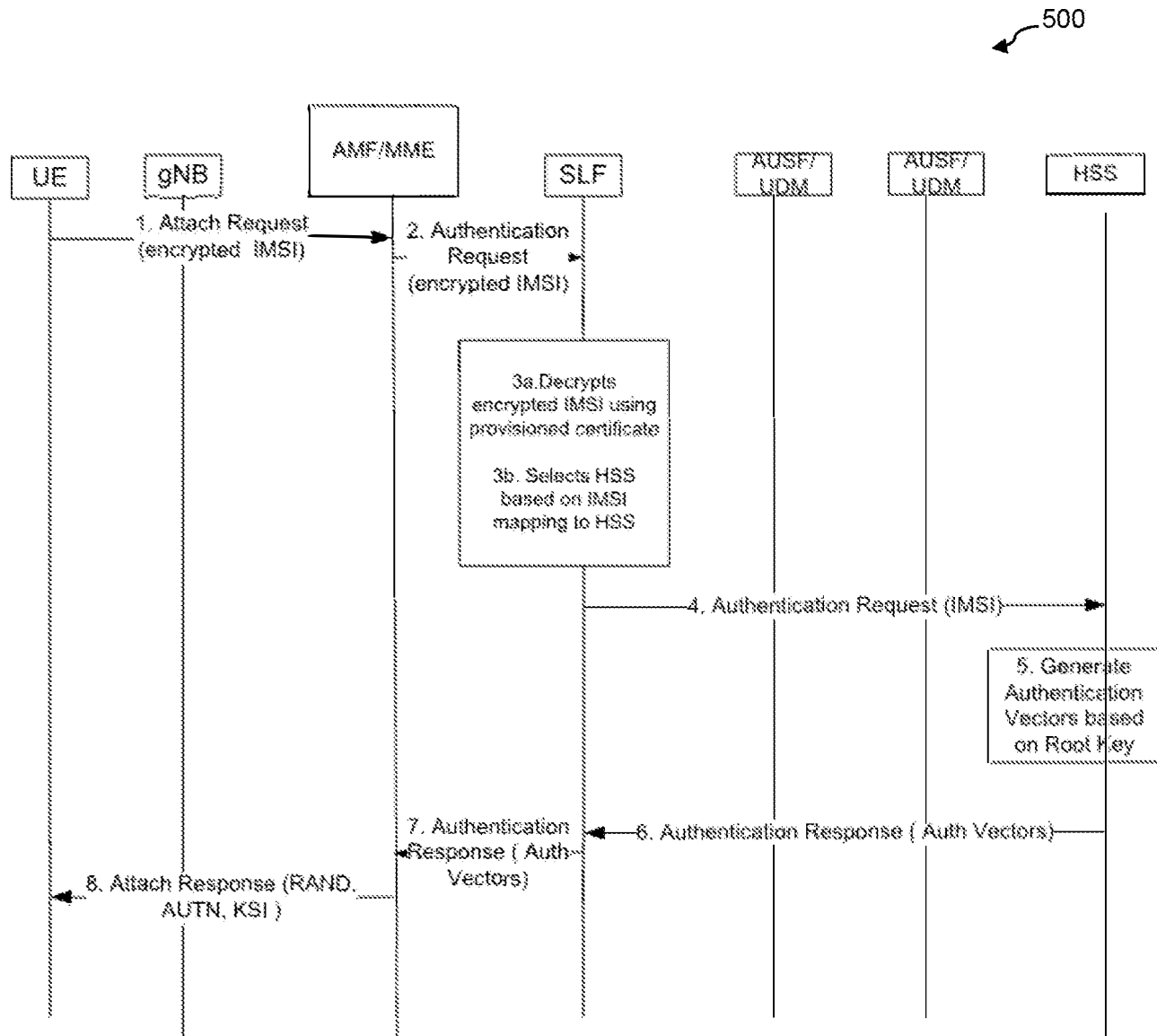
FIG. 3

400



High level UE Authentication procedure in 5G using encrypted IMSI, SLF and multiple UDM
Performing the IMSI decryption at the SLF instead of the UDM helps to maintain the core authentication functions unchanged.

FIG. 4



Mixed Core architecture of UDM and HSS to support 4G LTE and 5G Network.
IMSI decryption at SLF helps to manage both cores

FIG. 5

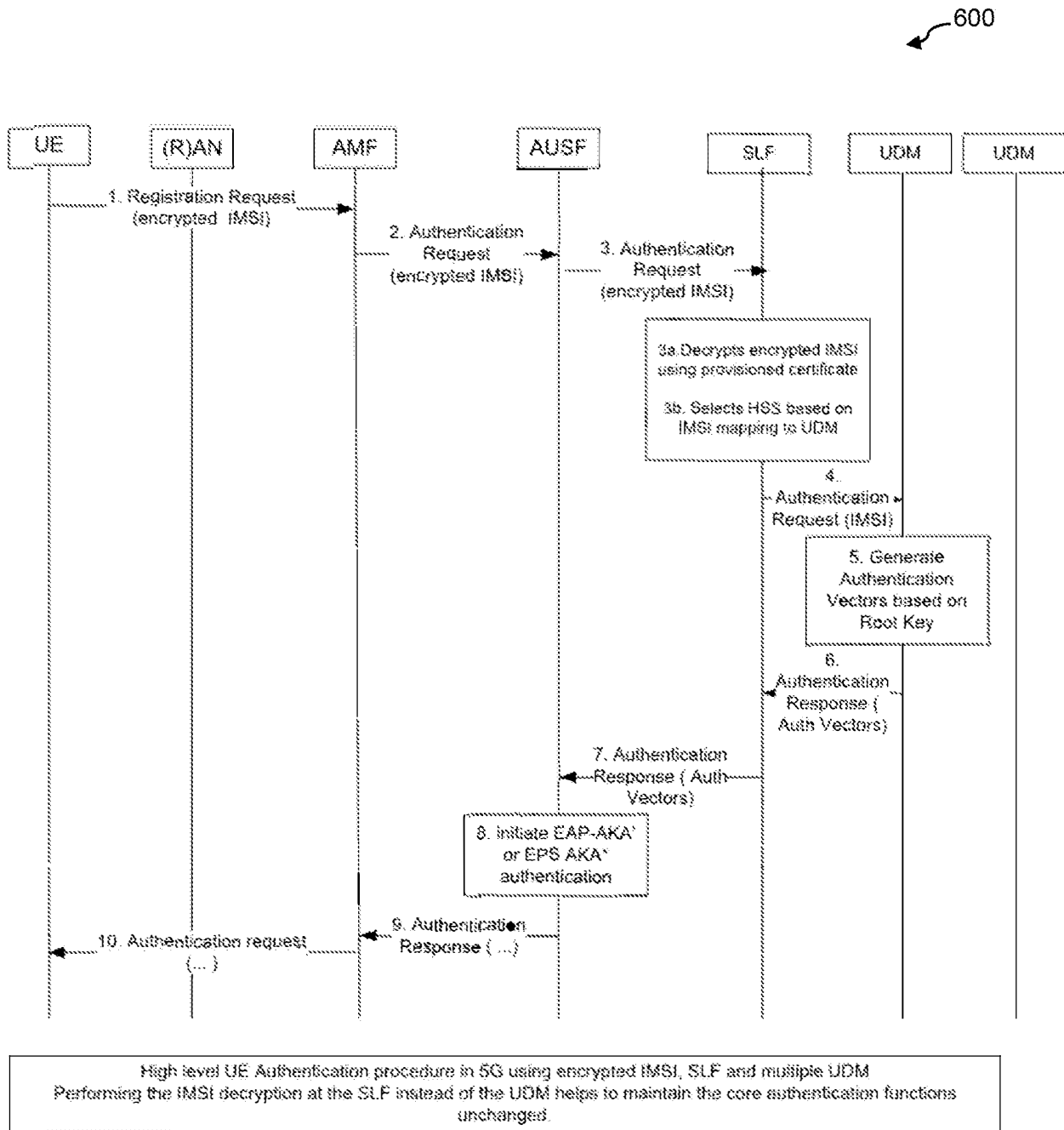
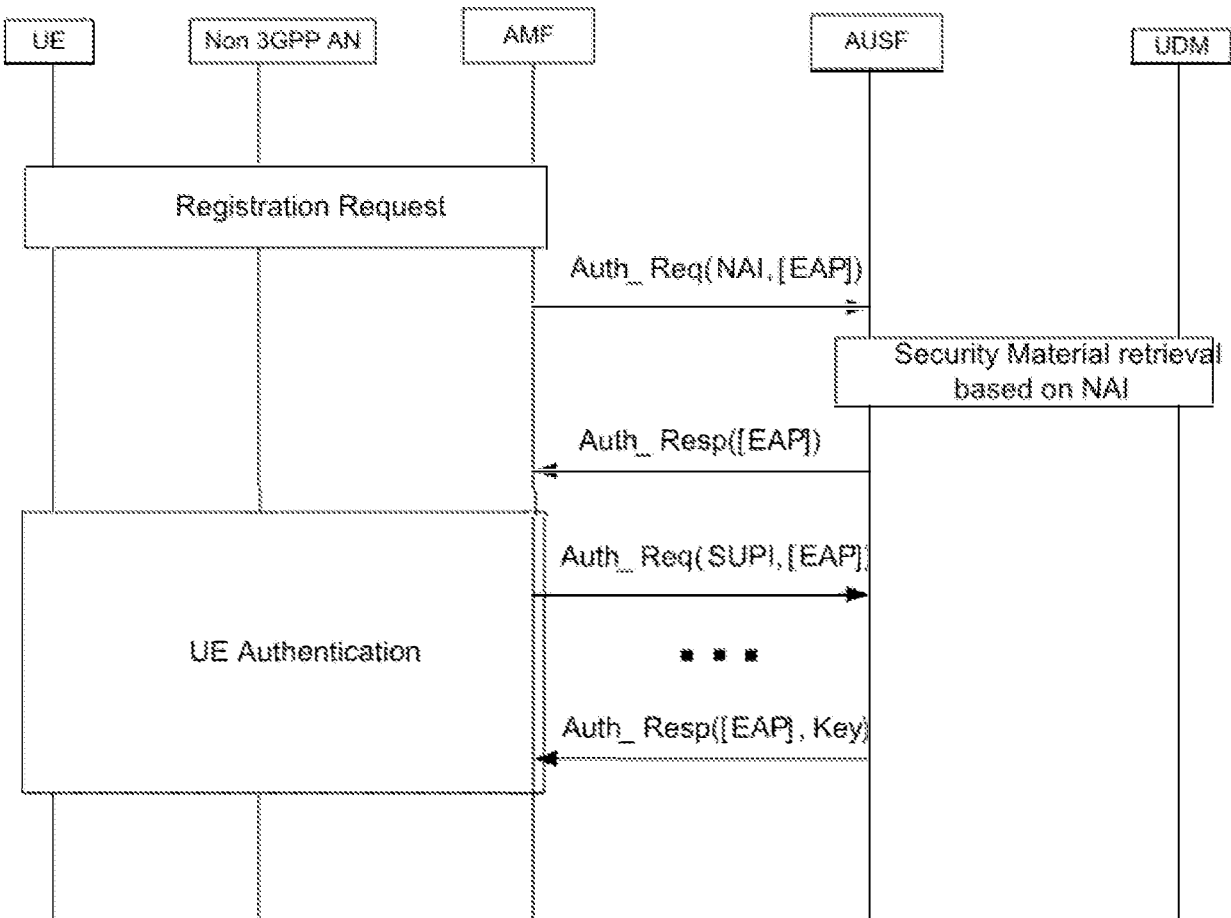


FIG. 6

700



- UE accessing the 5G network via non-3gpp access (WLAN) and authentication**
- During the registration procedure over the 3GPP or non-3GPP access networks the AUSF is contacted by the AMF to perform UE authentication.
 - AUSF decides for authentication type, in N3 case it has to act as an EAP server. In 3GPP access type case optionally EAP AKA* is possible.
 - Several EAP request/response messages may be required between the UE and AUSF (via the AMF) depending on the chosen EAP authentication method. Upon successful UE authentication, the AUSF provides the AMF with a security key that will be used by the AMF to generate NAS, CP and UP specific security keys.

FIG. 7

PRIVACY INDICATORS FOR CONTROLLING AUTHENTICATION REQUESTS**Field**

5 The field relates generally to communication systems, and more particularly, but not exclusively, to security within such systems.

Background

10 This section introduces aspects that may be helpful to facilitating a better understanding of the inventions. Accordingly, the statements of this section are to be read in this light and are not to be understood as admissions about what is in the prior art or what is not in the prior art.

15 Fourth generation (4G) wireless mobile telecommunications technology, also known as Long Term Evolution (LTE) technology, was designed to provide high capacity mobile multimedia with high data rates particularly for human interaction. Next generation or fifth generation (5G) technology is intended to be used not only for human interaction, but also for machine type communications in so-called Internet of Things (IoT) networks.

20 While 5G networks are intended to enable massive IoT services (e.g., very large numbers of limited capacity devices) and mission-critical IoT services (e.g., requiring high reliability), improvements over legacy mobile communication services are supported in the form of enhanced mobile broadband (eMBB) services intended to provide improved wireless Internet access for mobile devices.

25 In an example communication system, user equipment (5G UE in a 5G network or, more broadly, a UE) such as a mobile terminal (subscriber) communicates over an air interface with a base station or access point referred to as a gNB in a 5G network or an eNB (evolved Node B) in an LTE network. The access point (e.g., gNB/eNB) is illustratively part of an access network of the communication system. For example, in a 5G network, the access network is referred to as a 5G System and is described in 5G Technical Specification (TS) 23.501, V0.4.0, entitled “Technical Specification Group Services and System Aspects; System Architecture for the 5G System,” the disclosure of which is incorporated by reference herein
30 in its entirety. In an LTE network, the access network is an Evolved Universal Terrestrial

Radio Access Network (E-UTRAN). In general, the access point (e.g., gNB/eNB) provides access for the UE to a core network (CN), which then provides access for the UE to other UEs and/or a data network such as a packet data network (e.g., Internet).

Privacy is an important consideration in any communication system. Privacy is broadly addressed in 5G Technical Report (TR) 33.899, V1.1.0, entitled “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on the security aspects of the next generation system (Release 14),” the disclosure of which is incorporated by reference herein in its entirety. In particular, TR 33.899 identifies subscription (UE) privacy as one of the most important security areas to be addressed in 5G networks.

Summary

Illustrative embodiments provide one or more privacy indicators for controlling authentication requests in communication systems.

In one or more methods according to illustrative embodiments, such privacy indicators can be controlled (e.g., set) by using one or more bits in an information element or flag that is transmitted to elements of a communication system. Furthermore, illustrative embodiments provide methods that address how the home network of user equipment and other elements/functions in the core network (e.g., a server location function) can efficiently process the one or more privacy indicators. Advantageously, the one or more privacy indicators save wasted computing resources in the one or more network configurations in which they are implemented.

While these techniques can be applied to various communication networks, they are particularly suitable for 5G and next generation communication networks.

Further embodiments are provided in the form of non-transitory computer-readable storage medium having embodied therein executable program code that when executed by a processor causes the processor to perform the above steps. Still further embodiments comprise apparatus with a processor and a memory configured to perform the above steps.

These and other features and advantages of embodiments described herein will become more apparent from the accompanying drawings and the following detailed description.

Brief Description of the Drawings

FIG. 1 is a block diagram of a communication system in an illustrative embodiment.

FIG. 2 shows a more detailed view of a server location function and a home subscriber
5 server in an illustrative embodiment.

FIG. 3 shows a message flow for a user equipment authentication procedure for an LTE network in an illustrative embodiment.

FIG. 4 shows a message flow for a user equipment authentication procedure for an 5G network in an illustrative embodiment.

10 FIG. 5 shows a message flow for a user equipment authentication procedure for a mixed LTE/5G network in an illustrative embodiment.

FIG. 6 shows a message flow for a user equipment authentication procedure for an 5G network in another illustrative embodiment.

15 FIG. 7 shows a message flow for a user equipment accessing a 5G network via non-3GPP access and authentication in an illustrative embodiment.

Detailed Description

Embodiments will be illustrated herein in conjunction with example communication systems and associated techniques for managing authentication requests in a manner which
20 protects the privacy of the user's subscription identity. It should be understood, however, that the scope of the claims is not limited to particular types of communication systems and/or processes disclosed. Embodiments can be implemented in a wide variety of other types of communication systems, using alternative processes and operations. For example, although illustrated in the context of wireless cellular systems utilizing 3GPP system elements such as
25 an LTE Evolved Packet Core (EPC) and a 3GPP next generation system (5G), the disclosed embodiments can be adapted in a straightforward manner to a variety of other types of communication systems including, but not limited to, WiMAX systems and Wi-Fi systems.

As mentioned above, privacy of subscription identifiers when communicating over the air interface between the user equipment and the network access point has been a significant
30 issue for 2G/3G/4G networks. Efforts have been made in 5G networks to address this

significant issue. Even if it is unavoidable that down bidding attacks (e.g., an attacker impersonates the user equipment to negotiate an inferior security capability with the network access point) may force an 5G UE to attach to a lower generation network, it is realized that there is a need to address these privacy demands.

5 The above-referenced TR 33.899 describes several solutions to provide privacy over the air interface that can be generally grouped in three solution classes:

1) pseudonym solutions based on symmetric cryptographic systems, which demand a home subscriber server/function of the UE's home network to map a changing pseudonym to the permanent subscription identifier of the UE;

10 2) encryption of the permanent subscription identifier of the UE using the public key of the home network operator; and

3) encryption of the permanent subscription identifier of the UE using the public key of the serving network operator.

Note that, in one example, an International Mobile Subscriber Identity (IMSI) is a permanent subscription identifier (subscriber identity) of a UE. In one embodiment, the IMSI is a fixed 15-digit length and consists of a 3-digit Mobile Country Code (MCC), a 3-digit Mobile Network Code (MNC), and a 9-digit Mobile Station Identification Number (MSIN).

Note also that in an LTE network, the home subscriber server/function is called a Home Subscriber Server (HSS), and in a 5G network it is called User Data Management (UDM) which may also comprise an Authentication and Security Function (AUSF) and an Authentication Credential Repository and Processing Function (ARPF) as part of the UDM function.

While some illustrative embodiments are described herein from the perspective of the second solution class (i.e., the home network public key based solution), alternative embodiments may be implemented for the other two solution classes. See SA2 TS 23.502 and SA3 TR 33.899, the disclosures of which are incorporated by reference herein in their entireties.

In the home network public key based solution, the home operator provides its public key to all home network subscribers. They will use it to encrypt the subscriber identity, which is the MSIN part of IMSI. Only the MSIN part needs to be encrypted, because MNC+MCC is

needed by the serving network to route to the correct home network. Only the home HSS can decrypt the message because it possesses the private key. Once the IMSI is identified, HSS/AuC (where AuC is the Authentication Center part of the HSS) will create authentication vectors (AVs) based on the distinct shared root key K between a user (subscriber) and the HSS/AuC. Similarly, in the 5G network, the UDM/ARPF creates the AV's requested via AUSF. AUSF and UDM could be co-located for optimization reasons.

An operator in his network may have implementations of multiple HSSs which allows him to manage distinct sets of users in different HSSs/UDMs. Because of the multiple HSSs, a Server Location Function (SLF) is implemented in front of a set of HSSs. SLF analyses the authentication request for a user received from the MME/AMF and routes it to the correct HSS.

By way of example only, operation of the SLF is described in 3GPP TS 29.272 (Section 8: "User identity to HSS resolution") entitled "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol (Release 14)," the disclosure of which is incorporated by reference herein in its entirety. SLF provides user identity (IMSI) to HSS resolution using a locally maintained subscriber profile database and routes the Diameter messages containing the user authentication requests, as a Diameter proxy to the chosen HSS. Note that, in 5G, similar functionality would also be requested if 5G core network protocols are different from Diameter, e.g., using http-proxies. In the following descriptions, it is assumed that the SLF is covering both the DRA (Diameter Routing Agent) based solution as per 4G or any other proxy related solution dependent on protocol decisions for the 5G core network.

It is realized herein that if the home operator uses an SLF to split its set of subscribers, the SLF would need to evaluate the received identifier first. Thus, in a 5G network with permanent subscriber identity (e.g., IMSI) encrypted by one of the methods, an SLF would need to take over the decryption of the MSIN part of the IMSI. Further, the SLF would need to keep a database of all subscribers' profiles with the routing information, i.e., profile should map a subscriber's permanent identity (e.g., IMSI) to one of the HSSs in the network to forward the Authentication Request after decrypting the received (encrypted) IMSI. Therefore, it is advantageous to do the decryption of the encrypted IMSI at the SLF instead of in the HSS.

Hence, instead of an HSS storing the public key, now the SLF would need to store and use the network public key. An SLF is placed in the home operator's domain and considered trusted. In general, an SLF could be assumed in a large operator network. The usage of an SLF simplifies the new privacy management for the HSS/UDM in 5G networks up to the point that HSS/UDM is not changed at all for this protection subscription identifiers over the air interface, but the SLF needs to do the additional functionality of encrypted IMSI decryption and then perform the IMSI-to-HSS resolution.

Accordingly, illustrative embodiments as described herein address the issue of how the HSS/UDM or the SLF can efficiently deal with the newly introduced privacy feature, i.e., that the received attach request needs first to be decrypted. If this is not taken care of, the HSS/UDM or SLF would receive a request and attempt to process it wasting unnecessary computing resources.

Privacy will depend on country specific regulation, therefore HSS/UDM or SLF would need to be implemented to handle both cases of request for authentication vectors, i.e., to process or forward "normal" attach request if the 5G UE hasn't applied privacy or to process a "privacy" attach request.

In a first illustrative embodiment, the 5G UE, if it wants to protect its privacy, adds an identity privacy flag (i.e., privacy indicator) to indicate that the MSIN is provided encrypted.

It could be suggested that the HSS or SLF, even without this privacy indicator, will figure out after the first attempt to solve the request and, if encrypted, to attempt the decryption. But one key reason to have such an indication specified is that this saves processing time and less resources are needed. Thus, in this first illustrative embodiment, the SLF can make the decision on the processing by looking at this flag. If not set, the SLF will assume the provided IMSI is unencrypted, will do the IMSI-to-HSS resolution, and will forward to the correct HSS/UDM, i.e., compatibility with 4G operation is maintained. If the flag is set, the SLF will recognise that the provided IMSI is encrypted and use the network private key to decrypt the MSIN part to form the real unencrypted IMSI, perform the IMSI-to-HSS resolution and then forward the Authentication Request to the correct HSS/UDM. If no SLF is used, the same principle can be used by the HSS/UDM. That is, HSS/UDM has to check whether the 5G UE has set a flag and then decide whether decryption is needed.

This first illustrative embodiment can be applied to a 5G UE attaching via a 5G RAN (Radio Access Network) to a 5G core network (CN). However, 3GPP has identified, as the immediate deployment scenario, that the 5G UE should attach via a 5G RAN to a 4G CN. If the UE sets the indicator, the 4G CN would need to be enhanced to understand the identity privacy indication flag.

From a network architecture perspective for the operator with an evolving 4G network to 5G, both 4G and 5G access and core networks need to be supported for a considerable time. This means that current 4G HSS need to be supported while supporting new 5G HSS functions of decrypting an encrypted MSIN. In accordance with embodiments, placing an SLF capable of identifying an encrypted MSIN and decrypting it before routing the authentication request to an HSS helps to manage the coexistence of 4G and 5G core in an operator network. Enhancing the SLF to support the new identity 5G privacy feature is more advantageous than enhancing the HSS. If the HSS is enhanced, then in a large network with multiple HSSs, all the HSSs need to be updated together with capability to decrypt an encrypted IMSI. This may be more tedious to handle compared to solving the problem in a single central node (e.g., the SLF). Advantageously, with the first illustrative embodiment, a bidding down attack in 5G (to 4G) would not be beneficial if the same feature is also deployed in 4G whereby an enhanced SLF is used to achieve this feature.

In a second illustrative embodiment, another privacy indicator is provided that the operator could decide to add, e.g., to the network Master Information Block (MIB) / System Information Block (SIB) broadcast, to indicate to the 5G UE that the network will be able to handle a privacy-protected identifier, e.g., a flag that indicates that privacy is expected, possible to process, or desired. It is then up to the 5G UE implemented/configured policy, whether to attach at all to a network, if this indicator is not sent. The indicator on the 4G/5G network side would be to indicate regulation needs per country/region, i.e., switch on/off privacy. Note, while the UE is roaming in a visiting network, even though the UE authentication request from the visiting network is forwarded to the home network, for which the identity privacy indicator (first illustrative embodiment above) is described, there is a need to make adaptations to the serving network as well. The MME/SEAF (SEAF is a Security Anchor Function) has to handle the enhanced initial attach message from the UE, form the UE Authentication Request message,

and route it to the home network for requesting the AV. If the subscription identifier is encrypted, the size of the message field for the encrypted IMSI may be different from today's 4G IMSI field (depending on the solution class chosen).

In a third illustrative embodiment, the UE is configured to manage a privacy indicator that can be set to prohibit a 5G UE from responding to IMSI paging. Thus, if the UE wants to attach to the network and the network requests its real identity, a privacy-configured 5G UE configured with this privacy indicator would not answer.

Given the above-described privacy indicators, a wide variety of network configurations can be employed to implement the privacy indicators. FIGs. 1-7 depict some of these network configurations. However, it is to be appreciated that embodiments are not limited to the network configurations illustrated herein or otherwise described below.

FIG. 1 shows a communication system 100 within which illustrative embodiments are implemented. It is to be understood that the elements shown in communication system 100 are intended to represent main functions provided within the system, e.g., UE access functions, mobility management functions, serving gateway functions, etc. As such, the blocks shown in FIG. 1 reference specific elements in LTE and 5G networks that provide the main functions. However, other network elements may be used to implement some or all of the main functions represented. Also, it is to be understood that not all functions of an LTE or 5G network are depicted in FIG. 1. Rather, functions that facilitate an explanation of illustrative embodiments are represented.

Accordingly, as shown, communication system 100 comprises user equipment (UE) 102 that communicates via an air interface 103 with an access point (eNB/gNB) 104. The UE 102 may be a mobile station, and such a mobile station may comprise, by way of example, a mobile telephone, a computer, or any other type of communication device. In an LTE-V2X implementation, one or more UEs may be deployed in a given vehicle. The term "user equipment" as used herein is therefore intended to be construed broadly, so as to encompass a variety of different types of mobile stations, subscriber stations or, more generally, communication devices, including examples such as a combination of a data card inserted in a laptop or other equipment (e.g., vehicle). Such communication devices are also intended to encompass devices commonly referred to as access terminals.

In one embodiment, UE 102 is comprised of a Universal Integrated Circuit Card (UICC) and Mobile Equipment (ME). The UICC is the user-dependent part of the UE and contains at least one Universal Subscriber Identity Module (USIM) and appropriate application software. The USIM securely stores the International Mobile Subscriber Identity (IMSI) number and its related key which are used to identify and authenticate subscribers to access networks. The ME is the user-independent part of the UE and contains terminal equipment (TE) functions and various mobile termination (MT) functions.

The access point 104 is illustratively part of an access network of the communication system 100. Such an access network may comprise, for example, an E-UTRAN or 5G System (or mixed) having a plurality of base stations and one or more associated radio network control functions. The base stations and radio network control functions may be logically separate entities, but in a given embodiment may be implemented in the same physical network element, such as, for example, a base station router or femto cellular access point.

The access point 104 in this illustrative embodiment is operatively coupled to a mobility management function 106. In an LTE network, the function is typically implemented by a Mobility Management Element (MME), while in a 5G network, the function is implemented by an Access and Mobility Management Function (AMF). Although not expressly shown, SEAF can be implemented with the AMF connecting a UE with the mobility management. A mobility management function, as used herein, is the element or function in the CN part of the communication system that manages, among other network operations, access and authentication operations with the UE (through the access point 104).

The MME/AMF 106 in this illustrative embodiment is operatively coupled to an SLF 107. In illustrative embodiments, SLF 107 is configured as described above to respond to one or more privacy indicators that are set in messages it receives. As described above, SLF 107 may decrypt a subscriber identity or simply forward the encrypted information to the appropriate home network of UE 102, depending on the one or more privacy indicators. Thus, as shown, SLF 107 is operatively coupled to a plurality of HSSs/UDMs 108-1, 108-2, . . . , 108-N. These HSSs/UDMs represent the home networks of UEs that may attach to the communication system 100. SLF 107 is configured to provide the UE information to the appropriate HSS/UDM 108.

The access point 104 is also operatively coupled to a serving gateway function 110 (e.g., Serving Gateway (SGW) in an LTE network, and Session Management Function (SMF) in a 5G network), which is operatively coupled to a Packet Data Network (PDN) Gateway (PGW) 112. PGW 112 is operatively coupled to a Packet Data Network, e.g., Internet 114.

5 MME/AMF 106 and SLF 107 may be considered part of a CN. MME/AMF 106 and SLF 107 can also be part of a serving network. Further typical operations and functions of such network elements are not described here since they are not the focus of the illustrative embodiments and may be found in appropriate 3GPP LTE or 5G documentation.

10 It is to be appreciated that this particular arrangement of system elements is an example only, and other types and arrangements of additional or alternative elements can be used to implement a communication system in other embodiments. For example, in other embodiments, the system 100 may comprise authentication elements, as well as other elements not expressly shown herein.

Accordingly, the FIG. 1 arrangement is just one example configuration of a wireless cellular system, and numerous alternative configurations of system elements may be used. For example, although only single UE, eNB/gNB, MME/AMF, SLF, SGW/SMF and PGW elements are shown in the FIG. 1 embodiment, this is for simplicity and clarity of description only. A given alternative embodiment may of course include larger numbers of such system elements, as well as additional or alternative elements of a type commonly associated with

15 20 conventional system implementations.

It is also to be noted that while FIG. 1 illustrates system elements as singular functional blocks, the various subnetworks that make up the 5G network are partitioned into so-called network slices. Network slices (network partitions) comprise a series of function sets (i.e., function chains) for each corresponding service type using network function virtualization (NFV) on a common physical infrastructure. The network slices are instantiated as needed for

25 a given service, e.g., eMBB service, massive IoT service (e.g., V2X service), and mission-critical IoT service. A network slice or function is thus instantiated when an instance of that network slice or function is created. In some embodiments, this involves installing or otherwise running the network slice or function on one or more host devices of the underlying physical

30 infrastructure. UE 102 is configured to access one or more of these services via eNB/gNB 104.

FIG. 2 shows a more detailed view of SLF 107 and one HSS/UDM 108 in an illustrative embodiment. Each HSS/UDM 108 (108-1, 108-2, . . . , 108-N) in FIG. 1 can be configured as shown in FIG. 2. The SLF 107 comprises a processor 200 coupled to a memory 202 and interface circuitry 204. The processor 200 of the SLF 107 includes an authentication processing module 210 that may be implemented at least in part in the form of software executed by the processor. The processing module 210 performs authentication operations of the processes described in conjunction with subsequent figures and otherwise herein. The memory 202 of the SLF 107 includes an authentication storage module 212 that stores authentication and related data generated or otherwise used during authentication operations.

The HSS/UDM 108 comprises a processor 220 coupled to a memory 222 and interface circuitry 224. The processor 220 of the HSS/UDM 108 includes an authentication processing module 230 that may be implemented at least in part in the form of software executed by the processor. The processing module 230 performs the authentication operations of the processes described in conjunction with subsequent figures and otherwise herein. The memory 222 of the HSS/UDM 108 includes an authentication storage module 232 that stores authentication and related data generated or otherwise used during authentication operations.

The processors 200 and 220 of the respective SLF 107 and HSS/UDM 108 may comprise, for example, microprocessors, application-specific integrated circuits (ASICs), digital signal processors (DSPs) or other types of processing devices, as well as portions or combinations of such elements.

The memories 202 and 222 of the respective SLF 107 and HSS/UDM 108 may be used to store one or more software programs that are executed by the respective processors 200 and 220 to implement at least a portion of the functionality described herein. For example, authentication operations and other functionality as described in conjunction with subsequent figures and otherwise herein may be implemented in a straightforward manner using software code executed by processors 200 and 220.

A given one of the memories 202 or 222 may therefore be viewed as an example of what is more generally referred to herein as a computer program product or still more generally as a processor-readable storage medium that has executable program code embodied therein.

Other examples of processor-readable storage media may include disks or other types of

magnetic or optical media, in any combination. Illustrative embodiments can include articles of manufacture comprising such computer program products or other processor-readable storage media.

5 The memory 202 or 222 may more particularly comprise, for example, an electronic random access memory (RAM) such as static RAM (SRAM), dynamic RAM (DRAM) or other types of volatile or non-volatile electronic memory. The latter may include, for example, non-volatile memories such as flash memory, magnetic RAM (MRAM), phase-change RAM (PC-RAM) or ferroelectric RAM (FRAM). The term “memory” as used herein is intended to be broadly construed, and may additionally or alternatively encompass, for example, a read-only
10 memory (ROM), a disk-based memory, or other type of storage device, as well as portions or combinations of such devices.

The interface circuitries 204 and 224 of the respective SLF 10 and HSS/UDM 108 illustratively comprise transceivers or other communication hardware or firmware that allows the associated system elements to communicate with one another in the manner described
15 herein.

It is apparent from FIG. 2 that SLF 107 is configured for communication with HSS/UDM 108 and vice-versa via their respective interface circuitries 204 and 224. This communication involves SLF 107 sending data to the HSS/UDM 108, and the HSS/UDM 108 sending data to the SLF 107. However, in alternative embodiments, other network elements
20 may be operatively coupled between the SLF and the HSS/UDM. The term “data” as used herein is intended to be construed broadly, so as to encompass any type of information that may be sent between user equipment and a core network via a base station element including, but not limited to, identity data, authentication data, control data, audio, video, multimedia, etc.

It is to be appreciated that the particular arrangement of components shown in FIG. 2
25 is an example only, and numerous alternative configurations may be used in other embodiments. For example, the user equipment and mobility management function can be configured to incorporate additional or alternative components and to support other communication protocols.

Other system elements, such as eNB/gNB 104, MME/AMF 106, SGW/SMF 110, and
30 PGW 112, may each also be configured to include components such as a processor, memory

and network interface. These elements need not be implemented on separate stand-alone processing platforms, but could instead, for example, represent different functional portions of a single common processing platform. Such a processing platform may additionally comprise at least portions of an eNB/gNB and an associated radio network control function.

5 FIGs. 3-7 illustrate message flows and network configurations within which one or more of the above-described privacy indicators can be implemented. These message flows and network configurations are understood to be illustrative embodiments.

FIG. 3 illustrates a high-level UE authentication procedure 300 in LTE using unencrypted IMSI, SLF and multiple HSS, in accordance with one illustrative embodiment.

10 FIG. 4 illustrates a high-level UE authentication procedure 400 in 5G using encrypted IMSI, SLF and multiple UDM. Performing the IMSI decryption at the SLF instead of the UDM helps to maintain the core authentication functions unchanged, in accordance with one illustrative embodiment.

FIG. 5 illustrates a procedure 500 for a mixed core architecture of UDM and HSS to support 4G LTE and 5G networks, in accordance with one illustrative embodiment. IMSI decryption at SLF helps to manage both cores.

FIG. 6 illustrates a high-level UE authentication procedure 600 in 5G using encrypted IMSI, SLF and multiple UDM, in accordance with an illustrative embodiment. Performing the IMSI decryption at the SLF instead of the UDM helps to maintain the core authentication functions unchanged.

FIG. 7 illustrates a procedure 700 for a UE accessing the 5G network via non-3GPP access (WLAN) and authentication, in accordance with an illustrative embodiment. During the registration procedure over the 3GPP or non-3GPP access networks, the AUSF is contacted by the AMF to perform the UE authentication. AUSF decides for authentication type, in N3 case it has to act as an Extensible Authentication Protocol (EAP) server. In 3GPP access type case, optionally EAP AKA* is possible (AKA is Authentication and Key Agreement). Several EAP request/response messages may be required between the UE and AUSF (via the AMF) depending on the chosen EAP authentication method. Upon successful UE authentication, the AUSF provides the AMF with a security key that will be used by the AMF to generate Non-Access Stratum (NAS), Control Plane (CP) and User Plane (UP) specific security keys.

It is to be appreciated that the naming of identifiers mentioned herein, e.g., IMSI, etc., are for illustrative purposes only. That is, an identifier for a UE may have different names or acronyms in different protocols and standards for different communication network technologies. As such, none of the specific names or acronyms given to these identifiers herein
5 are intended to limit embodiments in any manner.

As indicated previously, the embodiments are not limited to the LTE or 5G context and the disclosed techniques can be adapted in a straightforward manner to a wide variety of other communication system contexts including, but not limited to, other 3GPP systems and non-3GPP systems which employ identity (e.g., IMSI or equivalent) in the identity request process.

10 The processor, memory, controller and other components of a user equipment or base station element of a communication system as disclosed herein may include well-known circuitry suitably modified to implement at least a portion of the identity request functionality described above.

As mentioned above, embodiments may be implemented in the form of articles of
15 manufacture each comprising one or more software programs that are executed by processing circuitry of user equipment, base stations or other elements of a communication system. Conventional aspects of such circuitry are well known to those skilled in the art and therefore will not be described in detail herein. Also, embodiments may be implemented in one or more ASICS, FPGAs or other types of integrated circuit devices, in any combination. Such
20 integrated circuit devices, as well as portions or combinations thereof, are examples of “circuitry” as that term is used herein. A wide variety of other arrangements of hardware and associated software or firmware may be used in implementing the illustrative embodiments.

It should therefore again be emphasized that the various embodiments described herein are presented by way of illustrative example only, and should not be construed as limiting the
25 scope of the claims. For example, alternative embodiments can utilize different communication system configurations, user equipment configurations, base station configurations, identity request processes, messaging protocols and message formats than those described above in the context of the illustrative embodiments. These and numerous other alternative embodiments within the scope of the appended claims will be readily apparent to
30 those skilled in the art.

PRIVACY INDICATORS FOR CONTROLLING AUTHENTICATION REQUESTS**Abstract**

Techniques provide one or more privacy indicators for authentication requests in
5 communication systems. For example, such privacy indicators can be controlled (e.g., set) by
using one or more bits in an information element or flag that is transmitted to elements of a
communication system. Furthermore, methods and mechanisms are provided that address how
the home network of user equipment and other elements/functions in the core network (e.g., a
server location function) can efficiently process the one or more privacy indicators.
10 Advantageously, the one or more privacy indicators save wasted computing resources in the
one or more network configurations in which they are implemented.

Electronic Patent Application Fee Transmittal

Application Number:				
Filing Date:				
Title of Invention:	PRIVACY INDICATORS FOR CONTROLLING AUTHENTICATION REQUESTS			
First Named Inventor/Applicant Name:	Suresh P. Nair			
Filer:	William Edward Lewis			
Attorney Docket Number:	820662-US-PSP			
Filed as Large Entity				
Filing Fees for Provisional				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
PROVISIONAL APPLICATION FILING	1005	1	260	260
Pages:				
Claims:				
Miscellaneous-Filing:				
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 (\$)				260

Electronic Acknowledgement Receipt

EFS ID:	29131466
Application Number:	62502266
International Application Number:	
Confirmation Number:	6444
Title of Invention:	PRIVACY INDICATORS FOR CONTROLLING AUTHENTICATION REQUESTS
First Named Inventor/Applicant Name:	Suresh P. Nair
Customer Number:	46304
Filer:	William Edward Lewis
Filer Authorized By:	
Attorney Docket Number:	820662-US-PSP
Receipt Date:	05-MAY-2017
Filing Date:	
Time Stamp:	17:05:22
Application Type:	Provisional

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$ 260
RAM confirmation Number	050817INTEFSW17062000
Deposit Account	500762
Authorized User	Lisa Vulpis

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

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

Lenovo Ex. 1008

Page 38

37 CFR 1.19 (Document supply fees)
 37 CFR 1.20 (Post Issuance fees)
 37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	1200-1460_ADS.pdf	1584373	no	8
			6c837319fedfd4fd561b14c79de573239ccc391f		
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
2	Provisional Cover Sheet (SB16)	1200-1460_CVR.pdf	410301	no	2
			e532659fc3f42fa34e855b1a566fd083d02ce372		
Warnings:					
This is not a USPTO supplied Provisional Cover Sheet SB16 form.					
Information:					
3	Drawings-only black and white line drawings	1200-1460_FIGS.pdf	1410723	no	7
			5f054f8b629f73c3bf620e0dfb070fc4469b2ebb		
Warnings:					
Information:					
4	Specification	1200-1460_APP.pdf	138640	no	15
			de92ab9cff9acc644cba11ab9986a4f33a6cd15ac		
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	29794	no	2
			79e4356e62853f2656f809e4cb12764370dd663e8		
Warnings:					
Information:					
Total Files Size (in bytes):			3573831		

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.