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

68103 7590 09/06/2018
Jefferson IP Law, LLP
1130 Connecticut Ave., NW, Suite 420
Washington, DC 20036

EXAMINER
PATEL, HARESH N

ART UNIT	PAPER NUMBER
2493	

DATE MAILED: 09/06/2018

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/350,963	11/14/2016	Hye-Won LEE	0201-1750	1023

TITLE OF INVENTION: METHOD AND APPARATUS FOR DOWNLOADING PROFILE ON EMBEDDED UNIVERSAL INTEGRATED CIRCUIT CARD OF TERMINAL

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	12/06/2018

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: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 02/11)

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (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)

68103 7590 09/06/2018
Jefferson IP Law, LLP
1130 Connecticut Ave., NW, Suite 420
Washington, DC 20036

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 facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/350,963	11/14/2016	Hye-Won LEE	0201-1750	1023

TITLE OF INVENTION: METHOD AND APPARATUS FOR DOWNLOADING PROFILE ON EMBEDDED UNIVERSAL INTEGRATED CIRCUIT CARD OF TERMINAL

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	12/06/2018

EXAMINER	ART UNIT	CLASS-SUBCLASS
PATEL, HARESH N	2493	726-004000

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 03-02 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,
(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.

1_____
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 has been filed for recordation as set forth in 37 CFR 3.11. 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. The following fee(s) are submitted:

❑ Issue Fee

❑ Publication Fee (No small entity discount permitted)

❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

❑ A check is enclosed.

❑ Payment by credit card. Form PTO-2038 is attached.

❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

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. _____

NWO EX2014
Samsung v Network-1, IPR2026-00114
Page 2 of 13

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.
15/350,963	11/14/2016	Hye-Won LEE	0201-1750	1023

68103 7590 09/06/2018
Jefferson IP Law, LLP
1130 Connecticut Ave., NW, Suite 420
Washington, DC 20036

EXAMINER
PATEL, HARESH N

ART UNIT	PAPER NUMBER
2493	

DATE MAILED: 09/06/2018

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.

PTOL-85 (Rev. 02/11)

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 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, 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. 15/350,963	Applicant(s) LEE et al.	
	Examiner HARESH PATEL	Art Unit 2493	AIA 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 6/21/18.
   ☐ 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 21-40 . 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. _____.
5. ☑ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/HARESH N PATEL/
Primary Examiner, Art Unit 2493

Notice of Pre-AIA or AIA Status

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

Priority

1. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Amendments to the Specification

2. Applicant's preliminary amendment to the claims paper dated 6/21/18 is acknowledged.

Drawings

3. The drawings filed on 11/14/16 are acknowledged.

35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. The claims 21-40 are statutory.

5. The claims 21-26 claim a method having several method steps. Claims 32-40 claim an equipment having a circuit card (hardware). The claims are **not** rejected under 35 USC 101 because the claims are **not** directed to an abstract idea (Alice Corp. Pty. Ltd. V. CLS Bank Int'l, 134, S.Ct. 2347 (2014) and Mayo framework (Mayo, 132 S.Ct. at 1294)), as an independent claims 21, 32, claims at least following limitations, transmitting, by the eUICC, a one-time public key of the eUICC to the LPA; transmitting, by

the LPA, a profile package request message including the one-time public key of the eUICC to the server; receiving, by the LPA, from the server, a profile package comprising: encrypted profile information of the profile, and a one-time public key of the server; transmitting, by the LPA, the one-time public key of the server to the eUICC; generating, by the eUICC, a session key using the one-time public key of the server and the one-time private of the eUICC; transmitting, by the LPA, an instruction to store the encrypted profile information to the eUICC; decrypting, by the eUICC, the encrypted profile information using the session key; and storing, by the eUICC, the decrypted information, wherein the encrypted profile information comprises encrypted information related to deleting the profile, which significantly more than an abstract idea. In particular, generating, by the eUICC, a session key using the one-time public key of the server and the one-time private of the eUICC; transmitting, by the LPA, an instruction to store the encrypted profile information to the eUICC; decrypting, by the eUICC, the encrypted profile information using the session key; and storing, by the eUICC, the decrypted information, wherein the encrypted profile information comprises encrypted information related to deleting the profile. Claims 22-26, 32-40 depend upon claims 21, 32. Hence, claims 21-26, 32-40 are statutory.

6. The claims 27-31 claim a method having several method steps. The claims are **not** rejected under 35 USC 101 because the claims are **not** directed to an abstract idea (Alice Corp. Pty. Ltd. V. CLS Bank Int'l, 134, S.Ct. 2347 (2014) and Mayo framework (Mayo, 132 S.Ct. at 1294)), as an independent claim 27 claims at least following limitations, generating a one-time key pair of the server, the one-time key pair comprising: a one-time public key of the server, and a one-time private key of the server; generating a session key using the one-time secret key of the server and the one-time public key of the eUICC; generating a profile package including encrypted profile information of the profile and a one-time public key of the server, by using the session key; and transmitting the profile package to the UE, wherein the encrypted profile information comprises encrypted information related to deleting the profile, which is significantly more than an abstract idea. In particular, generating a session key using the

one-time secret key of the server and the one-time public key of the eUICC; generating a profile package including encrypted profile information of the profile and a one-time public key of the server, by using the session key; and transmitting the profile package to the UE, wherein the encrypted profile information comprises encrypted information related to deleting the profile. Claims 28-31 depend upon claim 27. Hence, claims 27-31 are statutory.

Allowable Subject Matter

7. Claims 21-40 are allowed.

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

Claims 21 and 37 recite,

generating, by the eUICC, a one-time key pair, the one-time key pair comprising:

a one-time public key of the eUICC, and a one-time private key of the eUICC;

transmitting, by the eUICC, a one-time public key of the eUICC to the LPA; transmitting, by the LPA, a profile package request message including the one-time public key of the eUICC to the server;

receiving, by the LPA, from the server, a profile package comprising: encrypted profile information of the profile, and a one-time public key of the server;

transmitting, by the LPA, the one-time public key of the server to the eUICC; generating, by the eUICC, a session key using the one-time public key of the server and the one-time private of the eUICC;

transmitting, by the LPA, an instruction to store the encrypted profile information to the eUICC;

decrypting, by the eUICC, the encrypted profile information using the session key; and

storing, by the eUICC, the decrypted information,

wherein the encrypted profile information comprises encrypted information related to deleting the profile.

claim 27 claims at least following limitations, generating a one-time key pair of the server, the one-time key pair comprising: a one-time public key of the server, and a one-time private key of the

server; generating a session key using the one-time secret key of the server and the one-time public key of the eUICC; generating a profile package including encrypted profile information of the profile and a one-time public key of the server, by using the session key; and transmitting the profile package to the UE, wherein the encrypted profile information comprises encrypted information related to deleting the profile

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Truskovsky et al., 2013/0326614 discloses

> [0059] Many secure communication protocols rely on public and private encryption keys to provide confidentiality and integrity, and on a Public Key Infrastructure (PKI) to communicate information that provides authentication and authorization. Data encoded using a private key of a private key/public key pair can only be decoded using the corresponding public key of the pair, and data encoded using a public key of a private key/public key pair can only be decoded using the corresponding private key of the pair. Private key information is not intended to be made public, whereas public key information is typically shared.
>
> [0060] For example, if a sender wishes to send a message to a recipient in encrypted form, the recipient's public key is used to encrypt a message, which can then be decrypted only using the recipient's private key. Alternatively, in some encoding techniques, a one-time session key is generated and used to encrypt the body of a message, typically with a symmetric encryption technique (e.g. Triple DES). The session key is then encrypted using the recipient's public key (e.g. with a public key encryption algorithm such as RSA), which can then be decrypted only using the recipient's private key. The decrypted

session key can then be used to decrypt the message body. The message header may be used to specify the particular encryption scheme that is to be used to decrypt the message. Other encryption techniques based on public key cryptography may be used in variant implementations. However, in each of these cases, only the recipient's private key may be used to facilitate decryption of the message, and in this way, the confidentiality of messages can be maintained.

Yang et al., discloses

[0055] The KEK can be derived based at least in part on a private key associated with the provisioning server 102 and the public key PK.sub.eUICC. The private key associated with the provisioning server 102 can be part of a public-private key pair that can be generated by the provisioning server 102. In some example embodiments, the public-private key pair associated with the provisioning server 102 can be an ephemeral key pair that can be generated for one-time use for provisioning the eSIM to the eUICC 120. In some example embodiments, alternatively, the provisioning server 102 can reuse a key pair for provisioning multiple eSIMs. In embodiments in which the public key PK.sub.eUICC is pre-stored, the pre-stored PK.sub.eUICC value can be used. Additionally or alternatively, in some embodiments, the eUICC 120 can furnish a public key value (e.g., provide the PK.sub.eUICC) to the provisioning server 102 during the provisioning session. The public key value PK.sub.eUICC provided by the eUICC 120 to the provisioning server 102 can be either a one-time "ephemeral" public key generated by the eUICC 120 for use only during the particular provisioning session or a "static" public key that is reused by

the eUICC 120 for multiple provisioning sessions with the provisioning server 102. The use of "ephemeral" public keys provides for a degree of forward secrecy, and in particular, when both the eUICC 120 and the provisioning server 102 each use "ephemeral" public keys, perfect forward secrecy can be achieved. With only one side using an ephemeral public key, partial forward secrecy can be achieved.

Truskovsky, Yang and the additional art of record do not at least teach or suggest decrypting, by the eUICC, the encrypted profile information using the session key, the encrypted profile information comprises encrypted information related to deleting the profile.

Therefore independent claims 21, 32, 37, is allowable over the prior arts of record. Consequently, independent claims 21, 32, 37 and their respective dependent claims are also allowable over the prior arts of record.

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."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HARESH PATEL whose telephone number is (571) 272-3973. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Carl Colin, can be reached at (571) 272-3862. 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).

/HARESH N PATEL/
Primary Examiner, Art Unit 2493

Notice of References Cited	Application/Control No. 15/350,963	Applicant(s)/Patent Under Reexamination LEE et al.	
	Examiner HARESH PATEL	Art Unit 2493	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-20120260086-A1	10-2012	Haggerty; David T.	H04W8/265	713/150
*	B	US-20120331292-A1	12-2012	Haggerty; David T.	H04L63/0272	713/168
*	C	US-20150143125-A1	05-2015	Nix; John A.	H04W4/70	713/171
*	D	US-20120260090-A1	10-2012	Hauck; Jerrold Von	H04L63/0853	713/168
*	E	US-20140143826-A1	05-2014	Sharp; Christopher B.	G06F21/604	726/1
*	F	US-20160352698-A1	12-2016	LONG; Shuiping	H04W12/08	726/1
*	G	US-20130326614-A1	12-2013	Truskovsky; Alexander	G06F21/44	726/19
*	H	US-20170332312-A1	11-2017	Jung; Ha-Kyung	H04W8/20	726/1
*	I	US-20160021484-A1	01-2016	Park; Jong-Han	H04W4/70	455/418
*	J	US-20150341791-A1	11-2015	Yang; Xiangying	H04W12/06	713/159
*	K	US-20020126850-A1	09-2002	Allen, Robert	H04L9/0825	380/277
	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.