UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/647,812	**01/12/2022 05:06:30 PM ET**	**63121/0213**

Title of Invention

Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	6784	FILED BY	Victoria Gilmore
PATENT CENTER #	60484666	FILING DATE	-
CUSTOMER #	1912	FIRST NAMED INVENTOR	John A. Nix
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Albert Boardman

Documents

TOTAL DOCUMENTS: 0

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)

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 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.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/647,812	01/12/2022 05:06:30 PM ET	63121/0213

Title of Invention

Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	6784	FILED BY	Victoria Gilmore
PATENT CENTER #	60484666	AUTHORIZED BY	Albert Boardman
CUSTOMER #	1912	FILING DATE	-
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	John A. Nix

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 1077	E20221BH07052477	Victoria Gilmore

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
2081	UTILITY APPL. SIZE FEE > THAN 100 PAGES (FEE X PAGES >= 101 IN 50 PAGE INCREMENTS)	210.00	1	210.00
			TOTAL AMOUNT:	$210.00

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 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.

Doc Code: TRACK1.REQ
Document Description: TrackOne Request

PTO/AIA/424 (04-14)

CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION UNDER 37 CFR 1.102(e) (Page 1 of 1)

First Named Inventor:	John A. Nix	Nonprovisional Application Number (if known):	
Title of Invention:	Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i)(1) and the prioritized examination fee set forth in 37 CFR 1.17(c) have been filed with the request. The publication fee requirement is met because that fee, set forth in 37 CFR 1.18(d), is currently $0. The basic filing fee, search fee, and examination fee are filed with the request or have been already been paid. I understand that any required excess claims fees or application size fee must be paid for the application.

2. I understand that the application may not contain, or be amended to contain, more than four independent claims, more than thirty total claims, or any multiple dependent claims, and that any request for an extension of time will cause an outstanding Track I request to be dismissed.

3. The applicable box is checked below:

I. ☑ Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)

i. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.

---OR---

(b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.

ii. An executed inventor's oath or declaration under 37 CFR 1.63 or 37 CFR 1.64 for each inventor, **or** the application data sheet meeting the conditions specified in 37 CFR 1.53(f)(3)(i) is filed with the application.

II. ☐ Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)

i. A request for continued examination has been filed with, or prior to, this form.
ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature /Albert J. Boardman/	Date 2022-01-12
Name (Print/Typed) Albert J. Boardman	Practitioner Registration Number 70,601

Note: *This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required.**

☑ *Total of 1 forms are submitted.

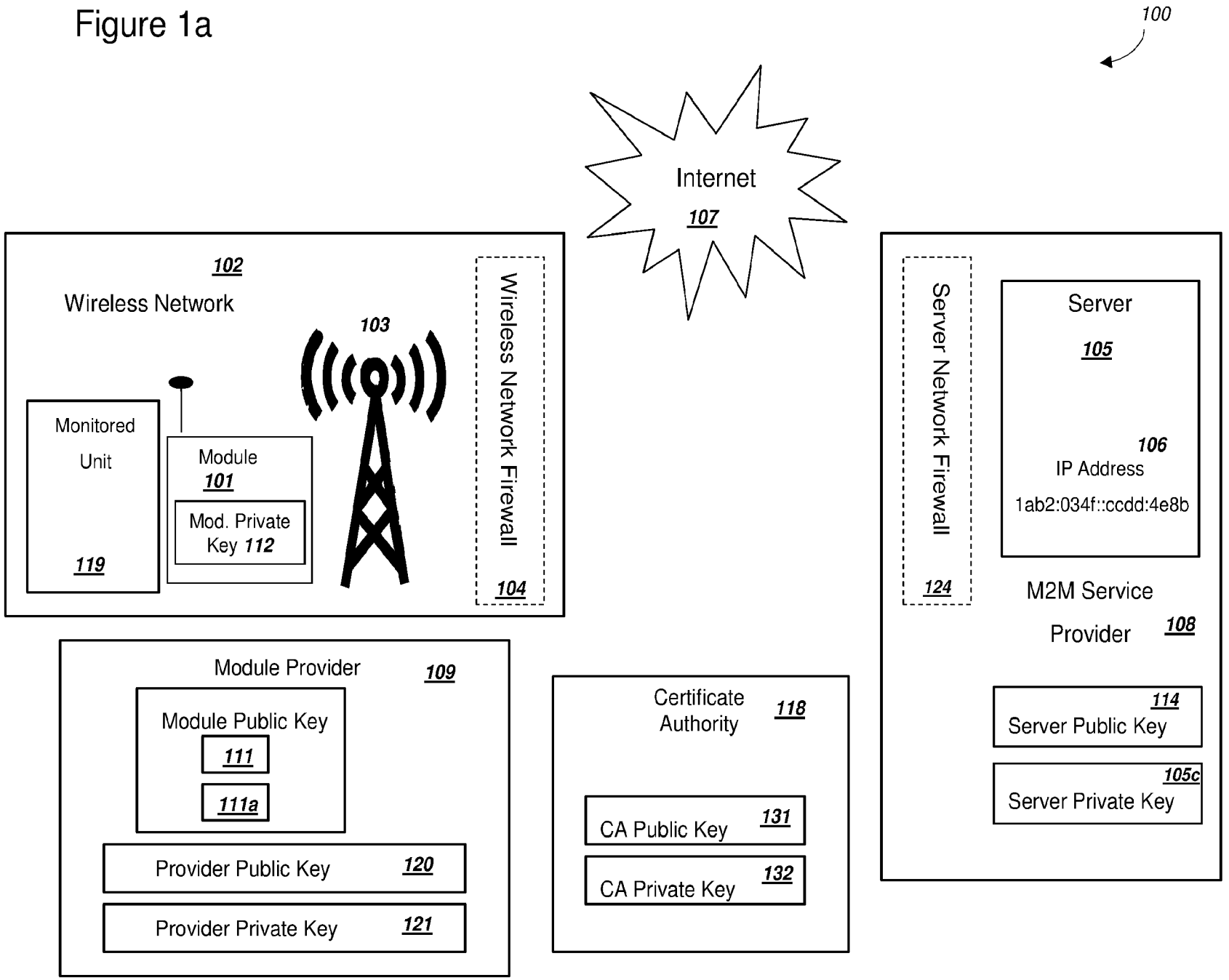
Privacy Act Statement

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

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

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

Figure 1a



Petitioner Samsung Ex-1038, 0007

Atty. Dkt. No. 63121/0213

Figure 1b

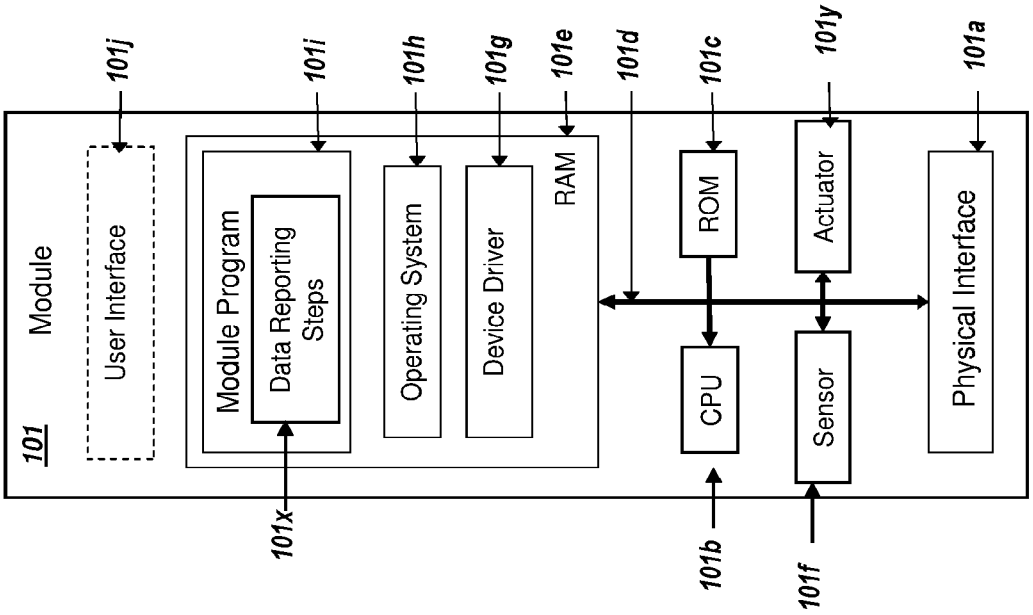


Figure 1c

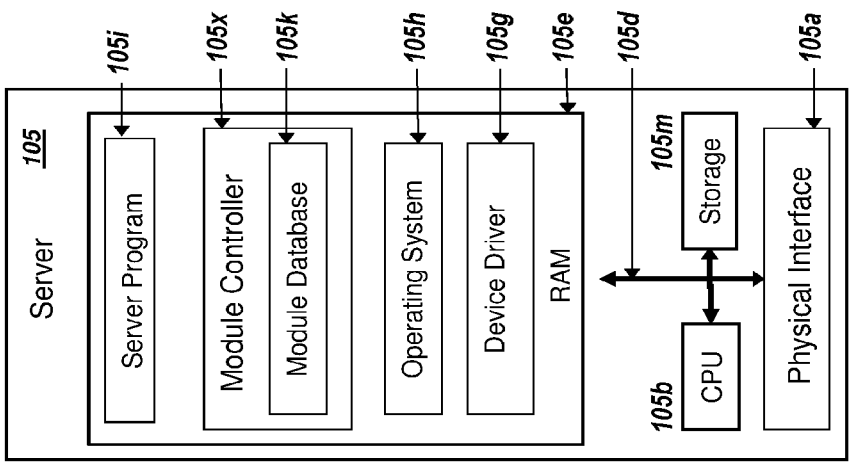


Figure 1d

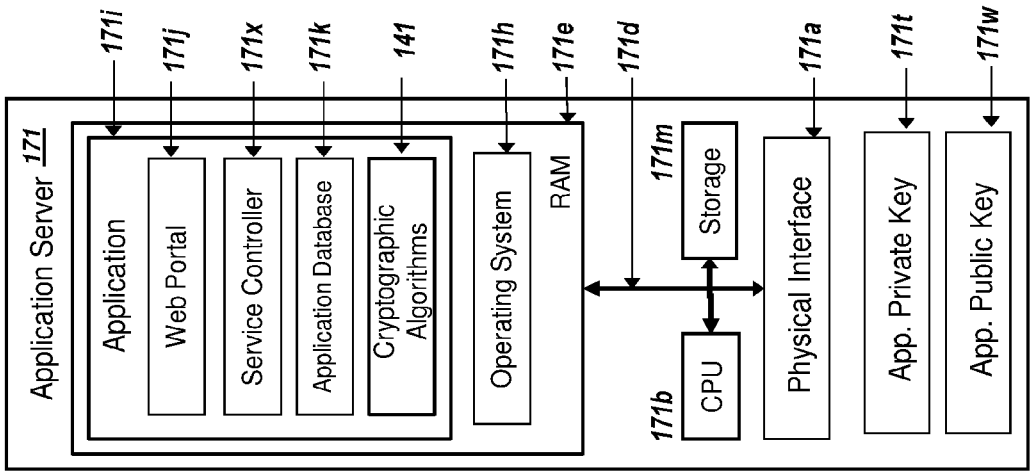


Figure 1e

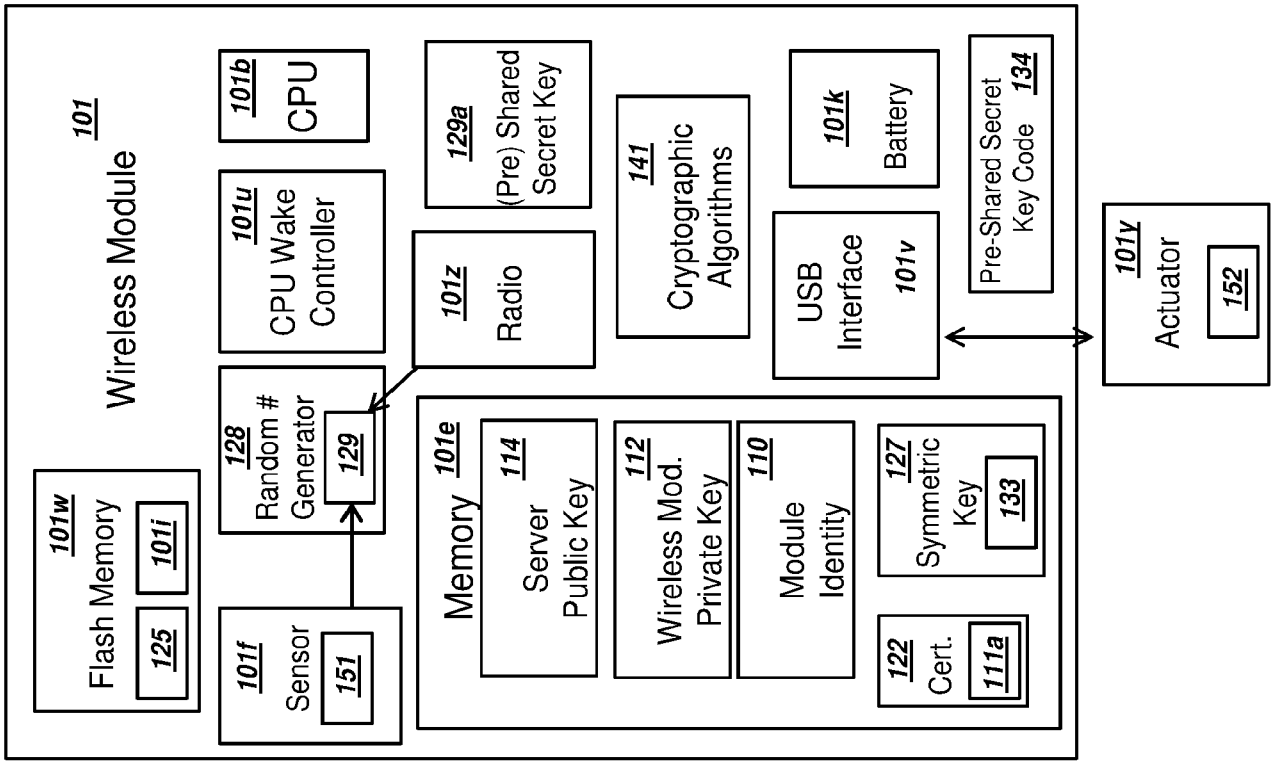
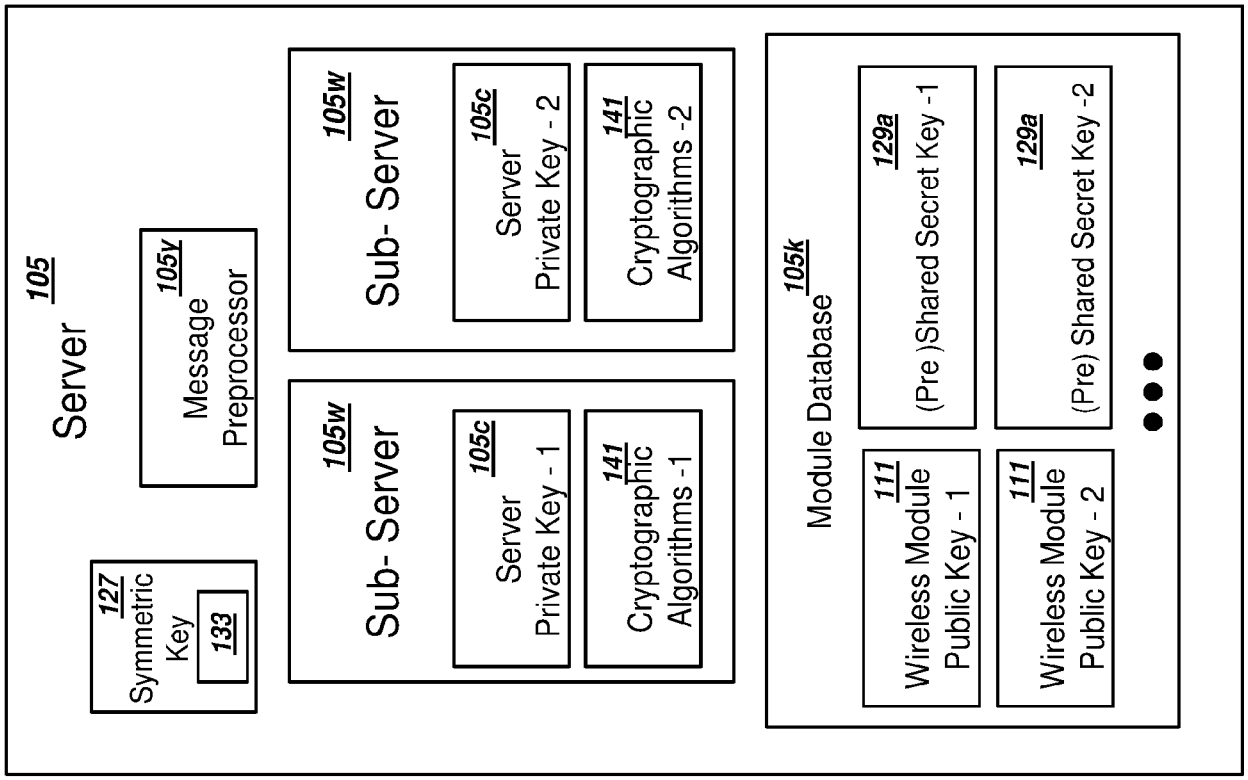


Figure 1f



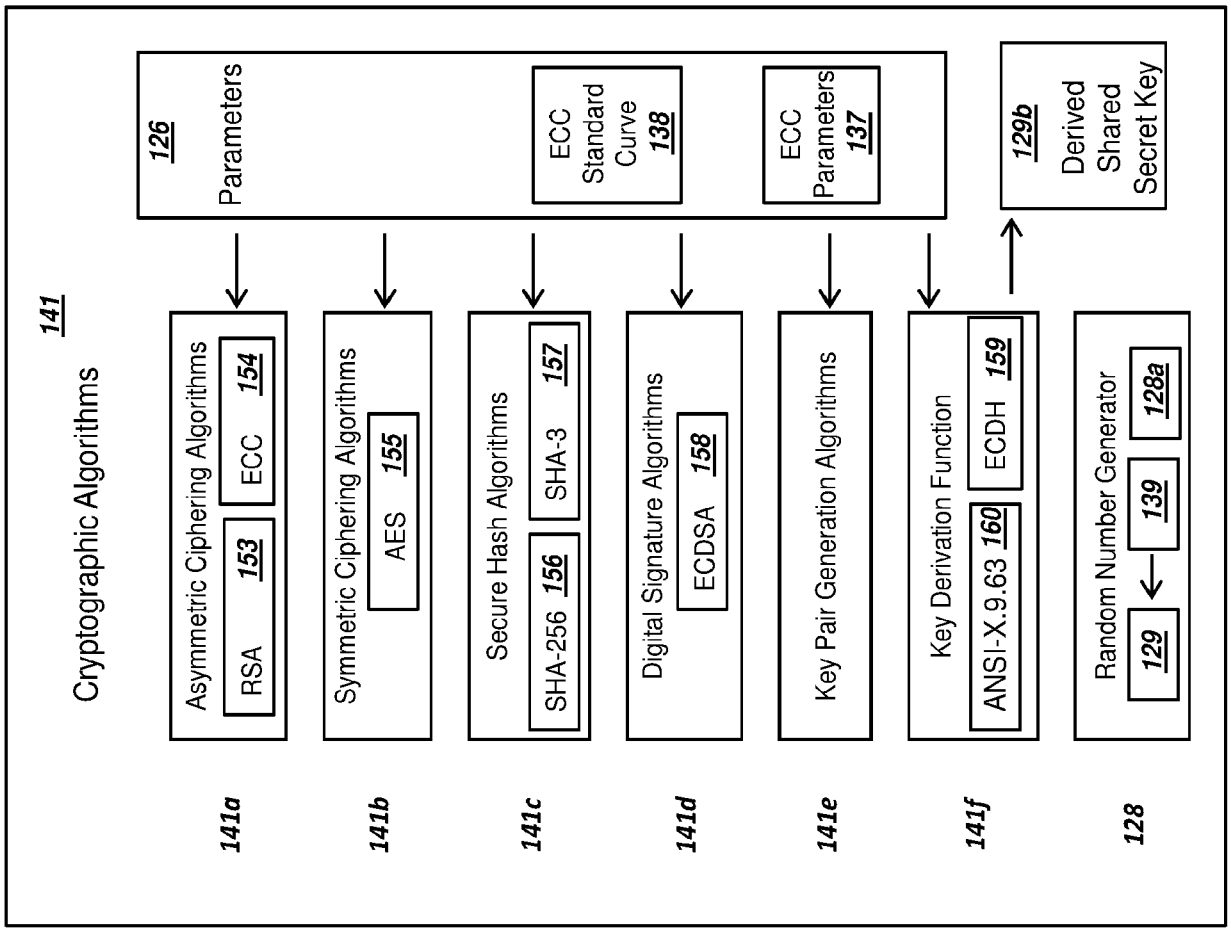
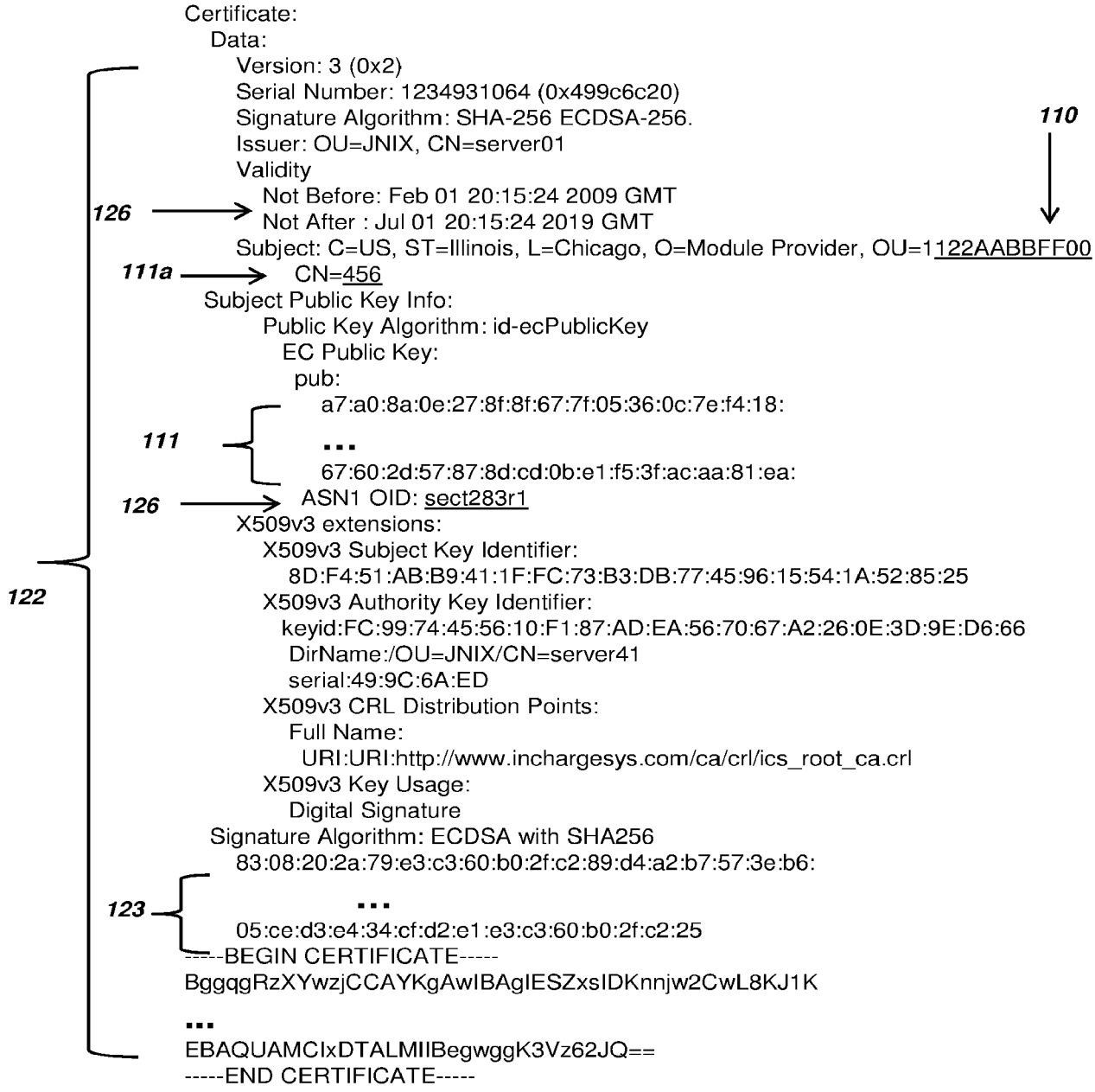

141
Cryptographic Algorithms
126
Parameters
ECC Standard Curve 138
ECC Parameters 137
129b
Derived Shared Secret Key
Asymmetric Ciphering Algorithms
RSA 153
ECC 154
Symmetric Ciphering Algorithms
AES 155
Secure Hash Algorithms
SHA-256 156
SHA-3 157
Digital Signature Algorithms
ECDSA 158
Key Pair Generation Algorithms
Key Derivation Function
ANSI-X.9.63 160
ECDH 159
Random Number Generator
129
139
128a
141a
141b
141c
141d
141e
141f
128

Figure 1g

Figure 1h

283 bit Elliptic Curve Key with SHA 256 Signature ("..." is long text removed)



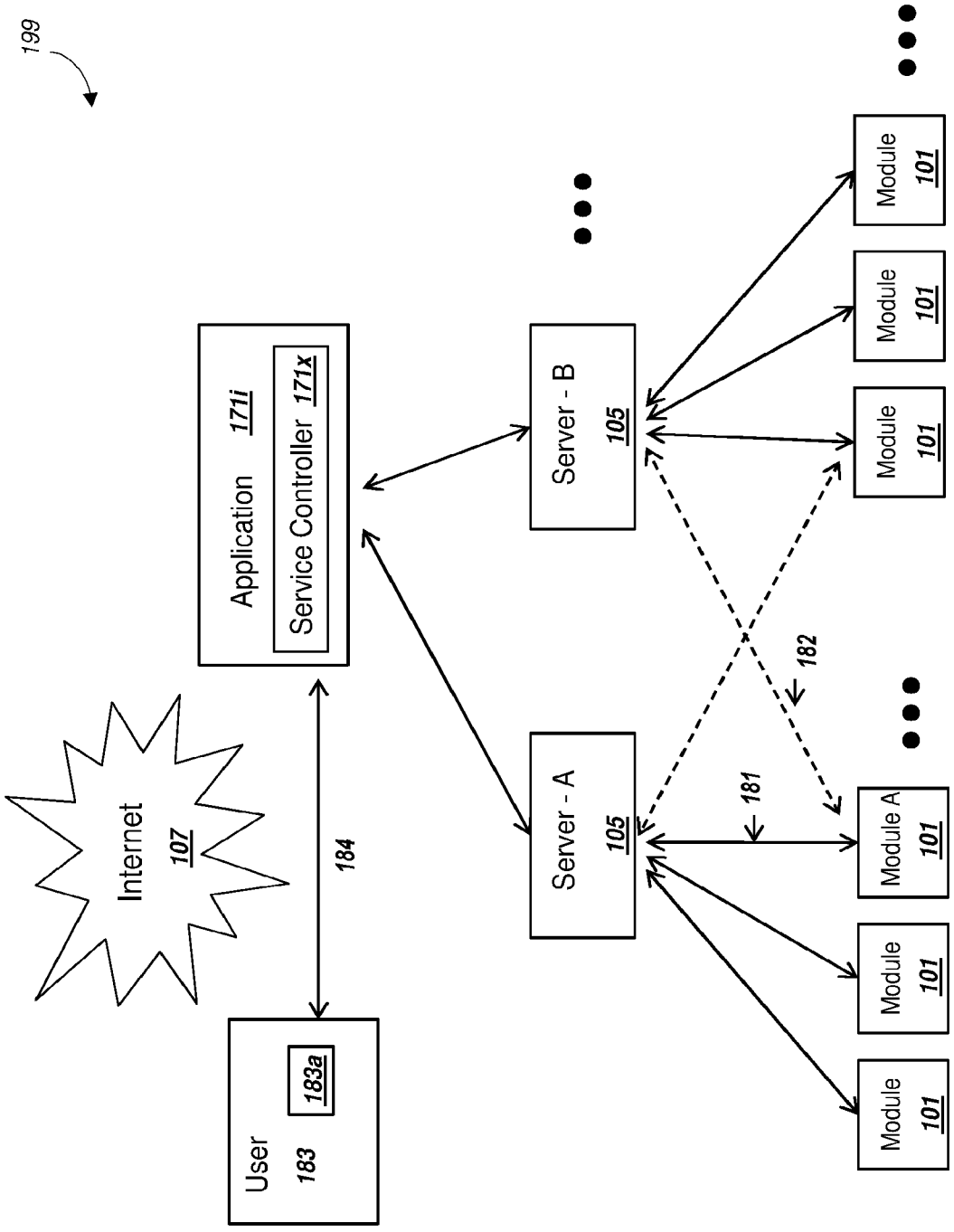
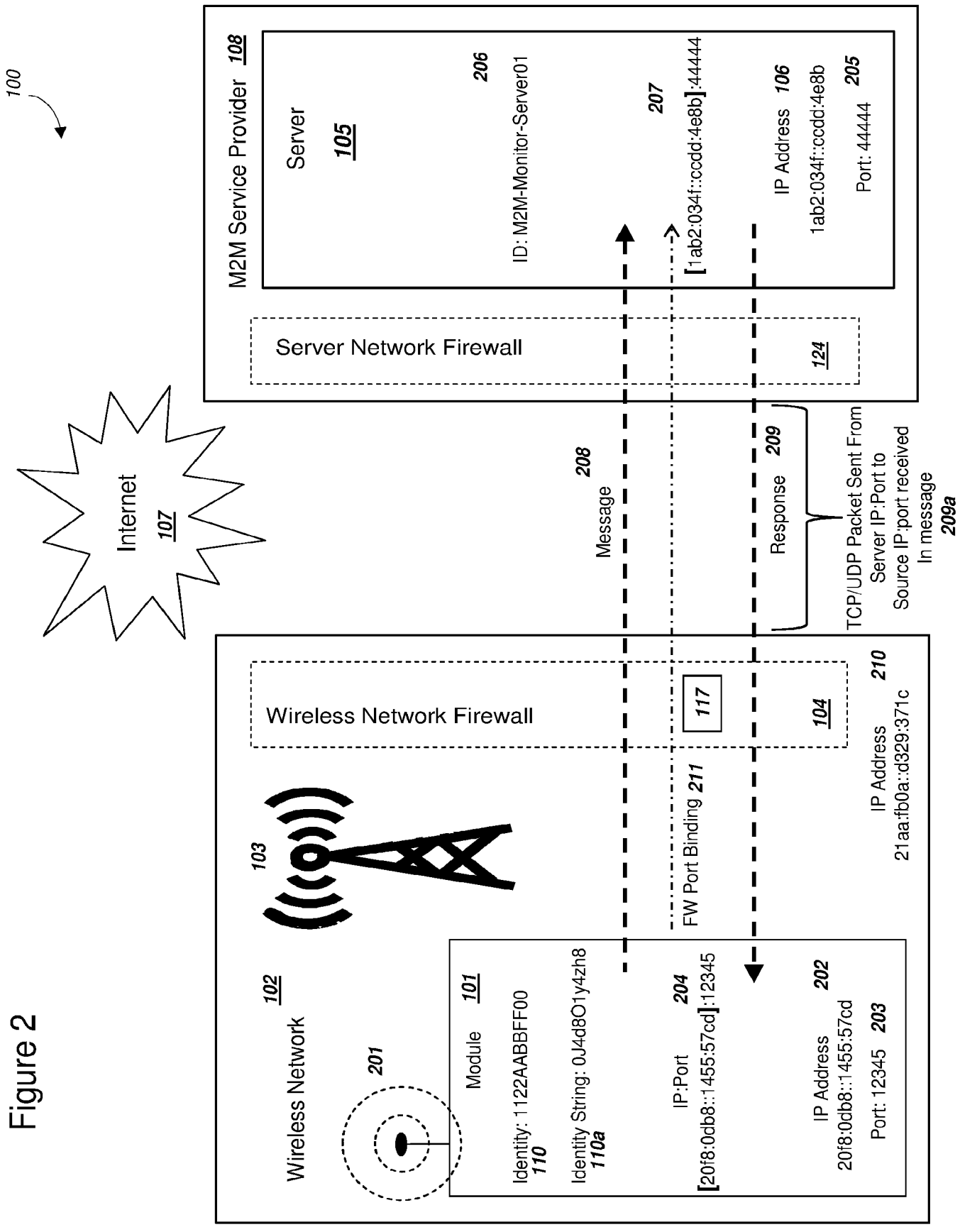

199
Application 171i
Service Controller 171x
Internet 107
184
User 183
183a
Server - A 105
Server - B 105
181
182
Module A 101
Module 101
Module 101
Module 101
Module 101
Module 101

Figure 1i

Figure 2


100
M2M Service Provider 108
Server
105
206
ID: M2M-Monitor-Server01
207
[1ab2:034f::ccdd:4e8b]:44444
IP Address 106
1ab2:034f::ccdd:4e8b
Port: 44444 205
Server Network Firewall
124
Internet
107
208
Message
209
Response
TCP/UDP Packet Sent From
Server IP:Port to
Source IP:port received
In message
209a
Wireless Network Firewall
104
117
FW Port Binding 211
IP Address 210
21aa:fb0a::d329:371c
103
102
Wireless Network
201
Module 101
Identity: 1122AABBFF00
110
Identity String: 0J4d8O1y4zh8
110a
IP:Port 204
[20f8:0db8::1455:57cd]:12345
IP Address 202
20f8:0db8::1455:57cd
Port: 12345 203

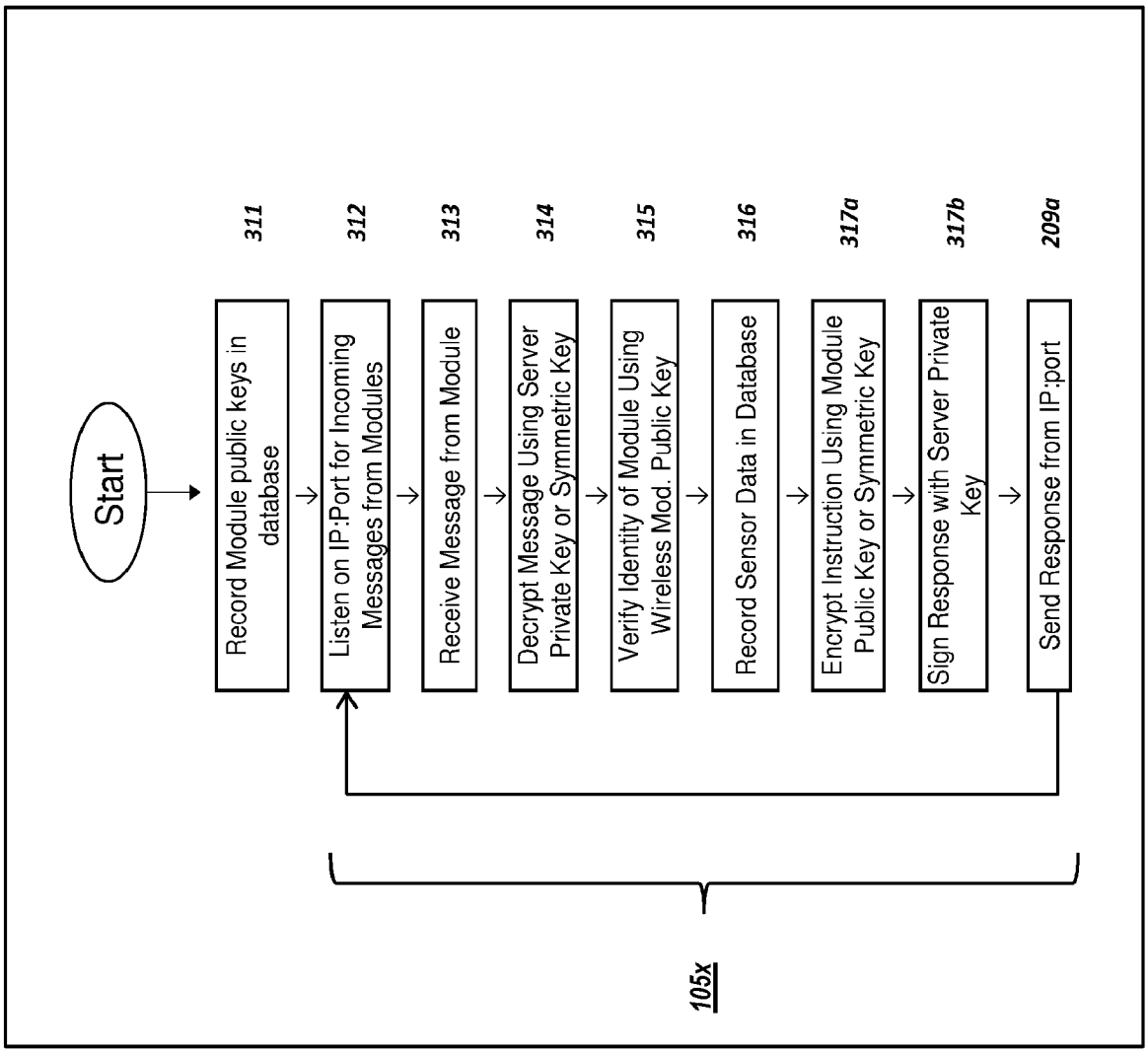

Start
Record Module public keys in database
311
Listen on IP:Port for Incoming Messages from Modules
312
Receive Message from Module
313
Decrypt Message Using Server Private Key or Symmetric Key
314
Verify Identity of Module Using Wireless Mod. Public Key
315
Record Sensor Data in Database
316
Encrypt Instruction Using Module Public Key or Symmetric Key
317a
Sign Response with Server Private Key
317b
Send Response from IP:port
209a
105x

Figure 3

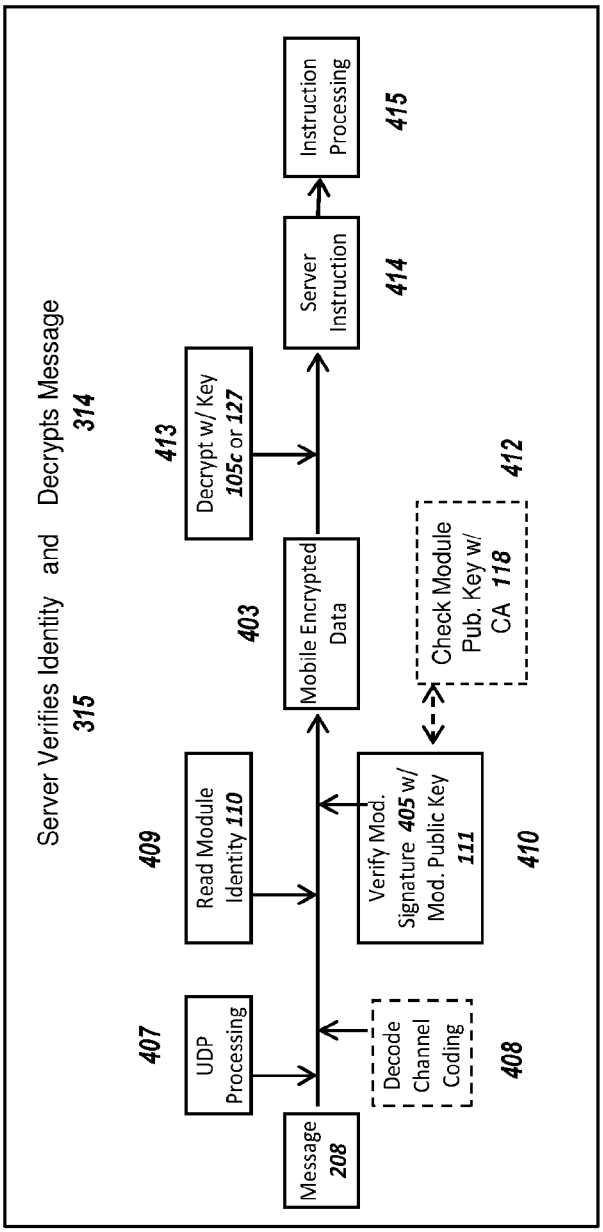


Figure 4

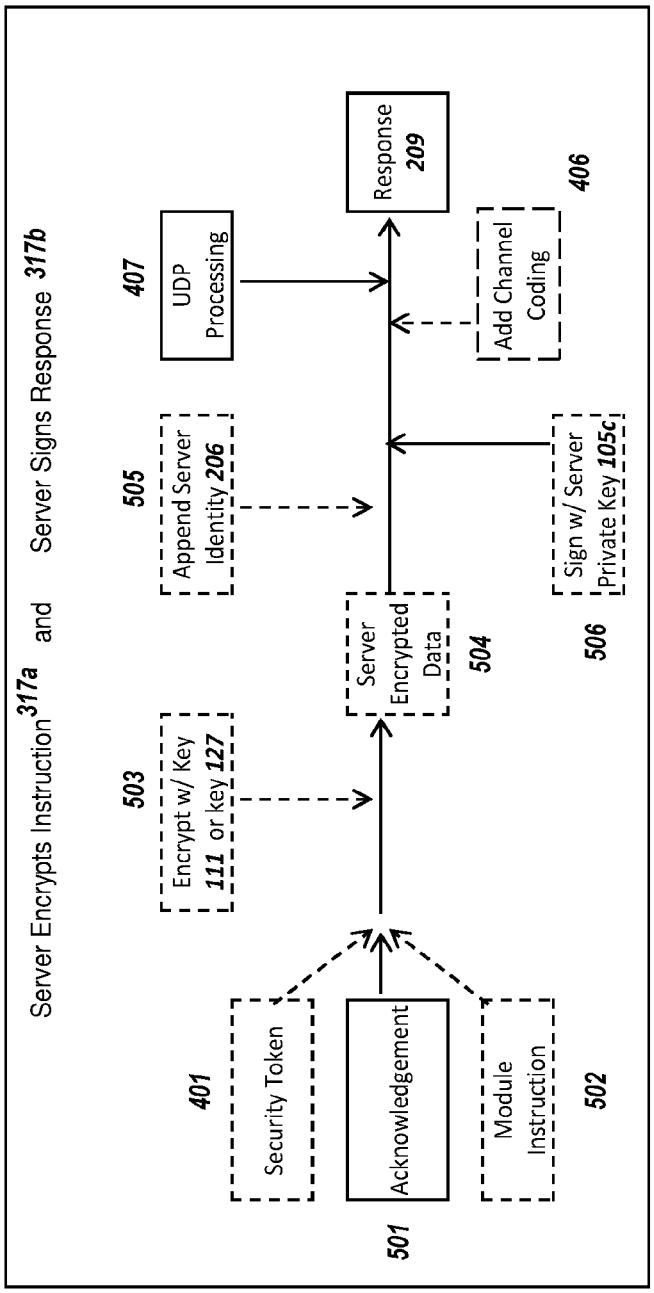


Figure 5a

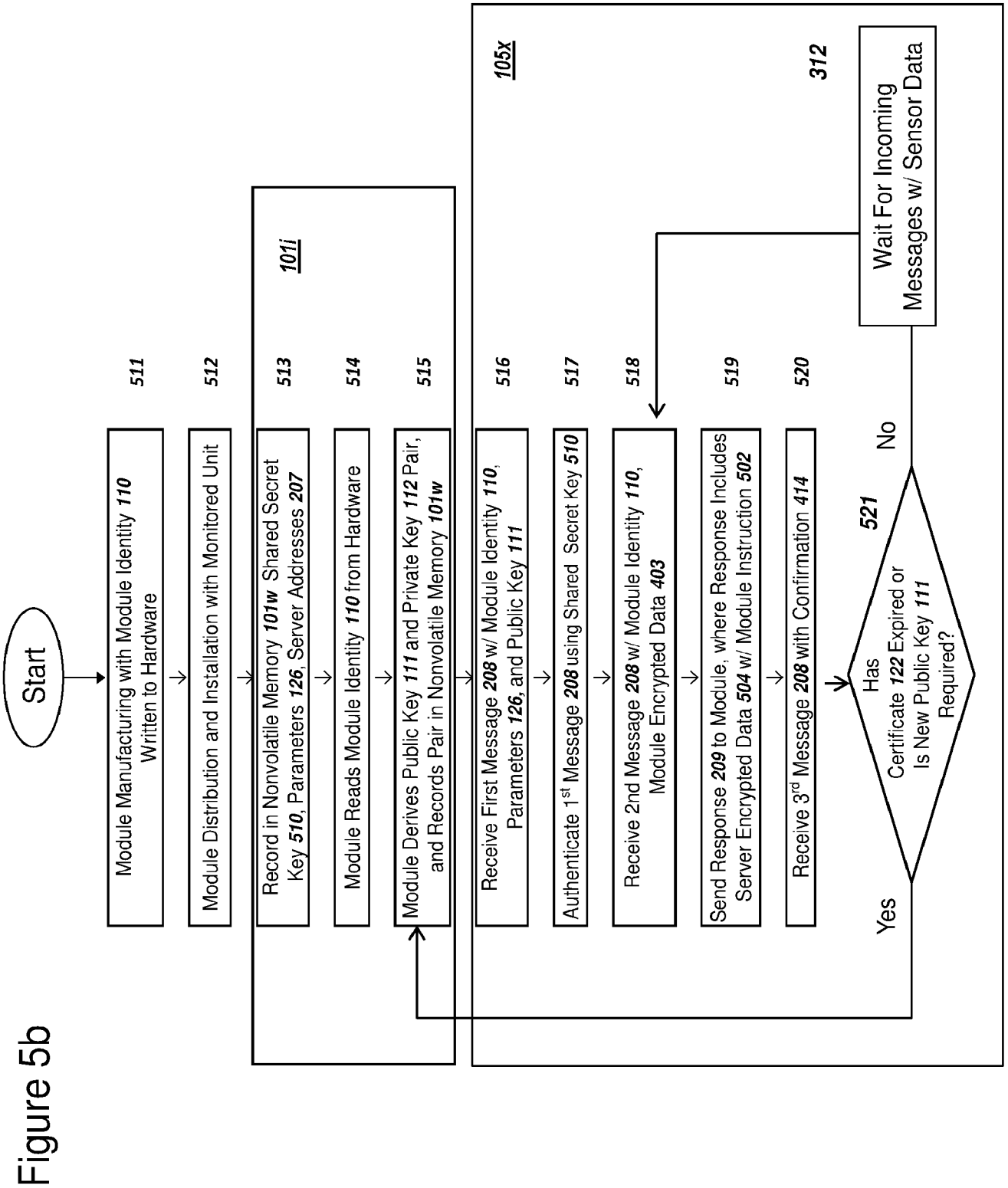

Start
Module Manufacturing with Module Identity 110 Written to Hardware
511
Module Distribution and Installation with Monitored Unit
512
101i
Record in Nonvolatile Memory 101w Shared Secret Key 510, Parameters 126, Server Addresses 207
513
Module Reads Module Identity 110 from Hardware
514
Module Derives Public Key 111 and Private Key 112 Pair, and Records Pair in Nonvolatile Memory 101w
515
105x
Receive First Message 208 w/ Module Identity 110, Parameters 126, and Public Key 111
516
Authenticate 1st Message 208 using Shared Secret Key 510
517
Receive 2nd Message 208 w/ Module Identity 110, Module Encrypted Data 403
518
Send Response 209 to Module, where Response Includes Server Encrypted Data 504 w/ Module Instruction 502
519
Receive 3rd Message 208 with Confirmation 414
520
312
Wait For Incoming Messages w/ Sensor Data
521
Has Certificate 122 Expired or Is New Public Key 111 Required?
No
Yes

Figure 5b

Figure 6a

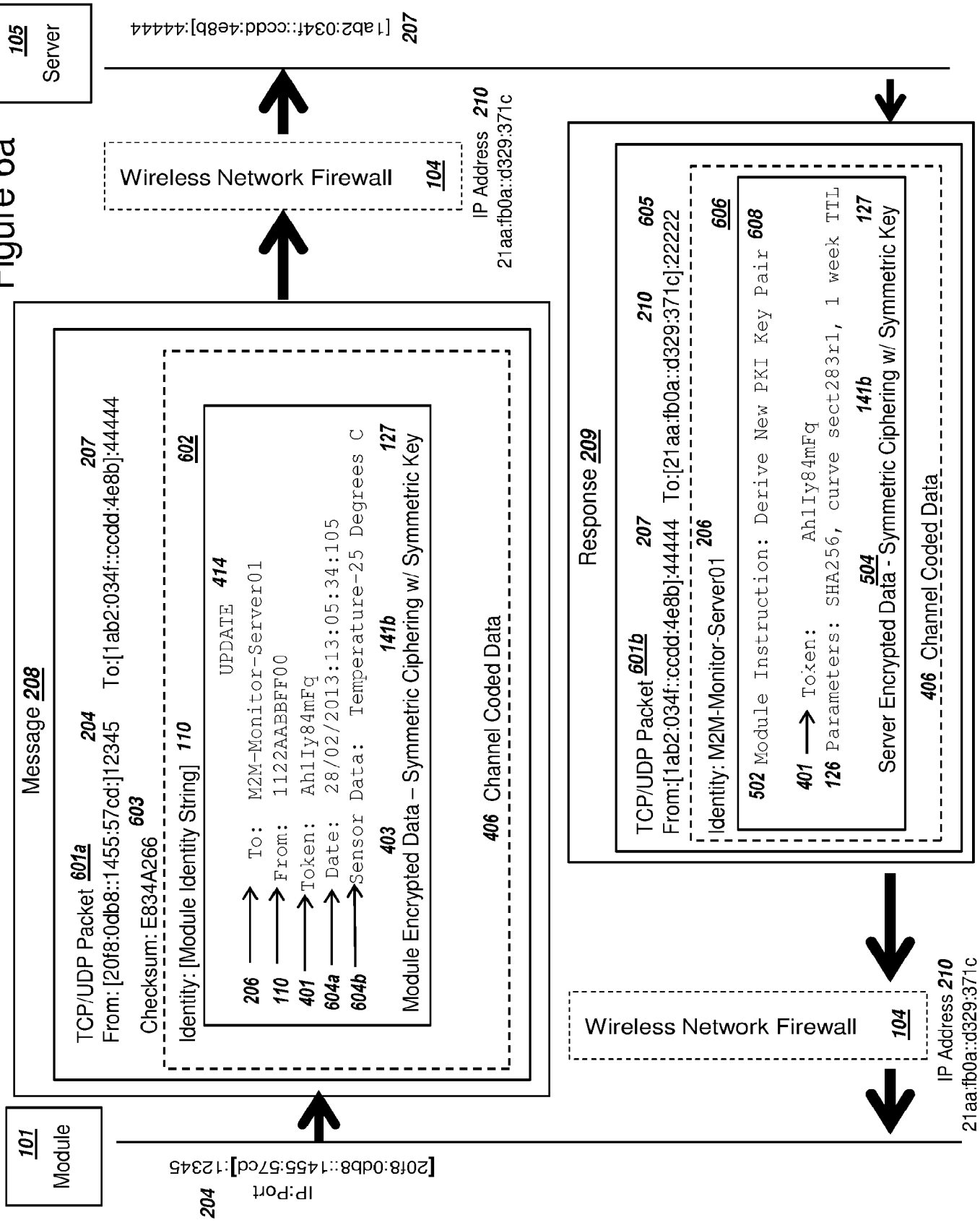

105 Server
[1ab2:034f::ccdd:4e8b]:44444 207
Wireless Network Firewall 104
IP Address 210
21aa:fb0a::d329:371c
Message 208
TCP/UDP Packet 601a 204 207
From: [20f8:0db8::1455:57cd:]12345 To:[1ab2:034f::ccdd:4e8b]:44444
Checksum: E834A266 603
Identity: [Module Identity String] 110 602
206 To: M2M-Monitor-Server01
110 From: 1122AABBFF00
401 Token: Ah1Iy84mFq
604a Date: 28/02/2013:13:05:34:105
604b Sensor Data: Temperature-25 Degrees C
403 Module Encrypted Data – Symmetric Ciphering w/ Symmetric Key 141b 127
406 Channel Coded Data
UPDATE 414
Response 209
TCP/UDP Packet 601b 207 210 605
From:[1ab2:034f::ccdd:4e8b]:44444 To:[21aa:fb0a::d329:371c]:22222
Identity: M2M-Monitor-Server01 206 606
502 Module Instruction: Derive New PKI Key Pair 608
401 Token: Ah1Iy84mFq
126 Parameters: SHA256, curve sect283r1, 1 week TTL
504 Server Encrypted Data - Symmetric Ciphering w/ Symmetric Key 141b 127
406 Channel Coded Data
Wireless Network Firewall 104
IP Address 210
21aa:fb0a::d329:371c
101 Module
IP:Port
[20f8:0db8::1455:57cd]:12345
204

Figure 6b

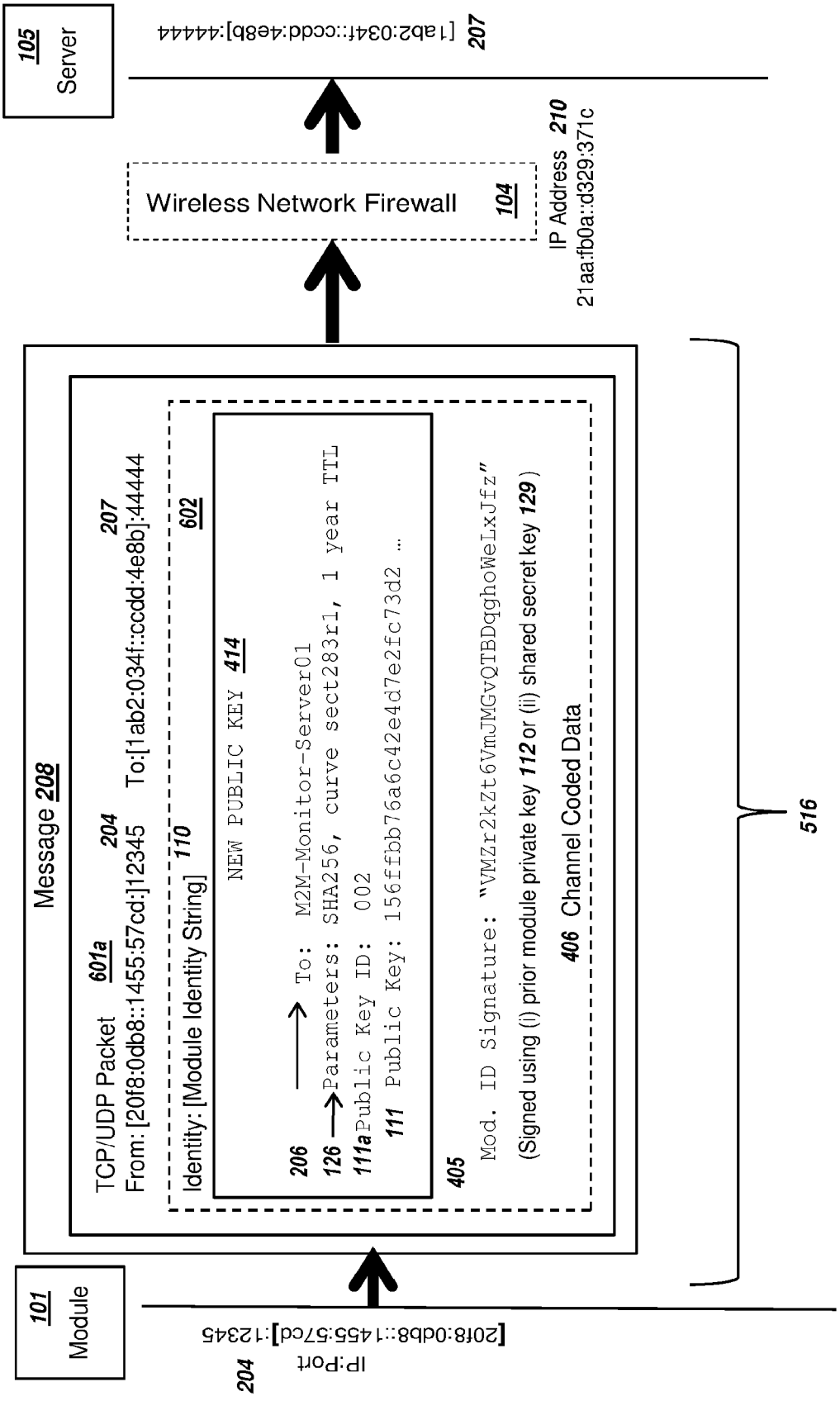

105
Server
[1ab2:034f::ccdd:4e8b]:44444 207
Wireless Network Firewall 104
IP Address 210
21aa:fb0a::d329:371c
Message 208
TCP/UDP Packet 601a 204 207
From: [20f8:0db8::1455:57cd:]12345 To:[1ab2:034f::ccdd:4e8b]:44444
Identity: [Module Identity String] 110 602
NEW PUBLIC KEY 414
206 To: M2M-Monitor-Server01
126 Parameters: SHA256, curve sect283r1, 1 year TTL
111a Public Key ID: 002
111 Public Key: 156ffbb76a6c42e4d7e2fc73d2 …
405
Mod. ID Signature: "VMZr2kZt6VmJMGvQTBDqghoWeLxJfz"
(Signed using (i) prior module private key 112 or (ii) shared secret key 129)
406 Channel Coded Data
516
101
Module
IP:Port
[20f8:0db8::1455:57cd]:12345
204

Figure 7

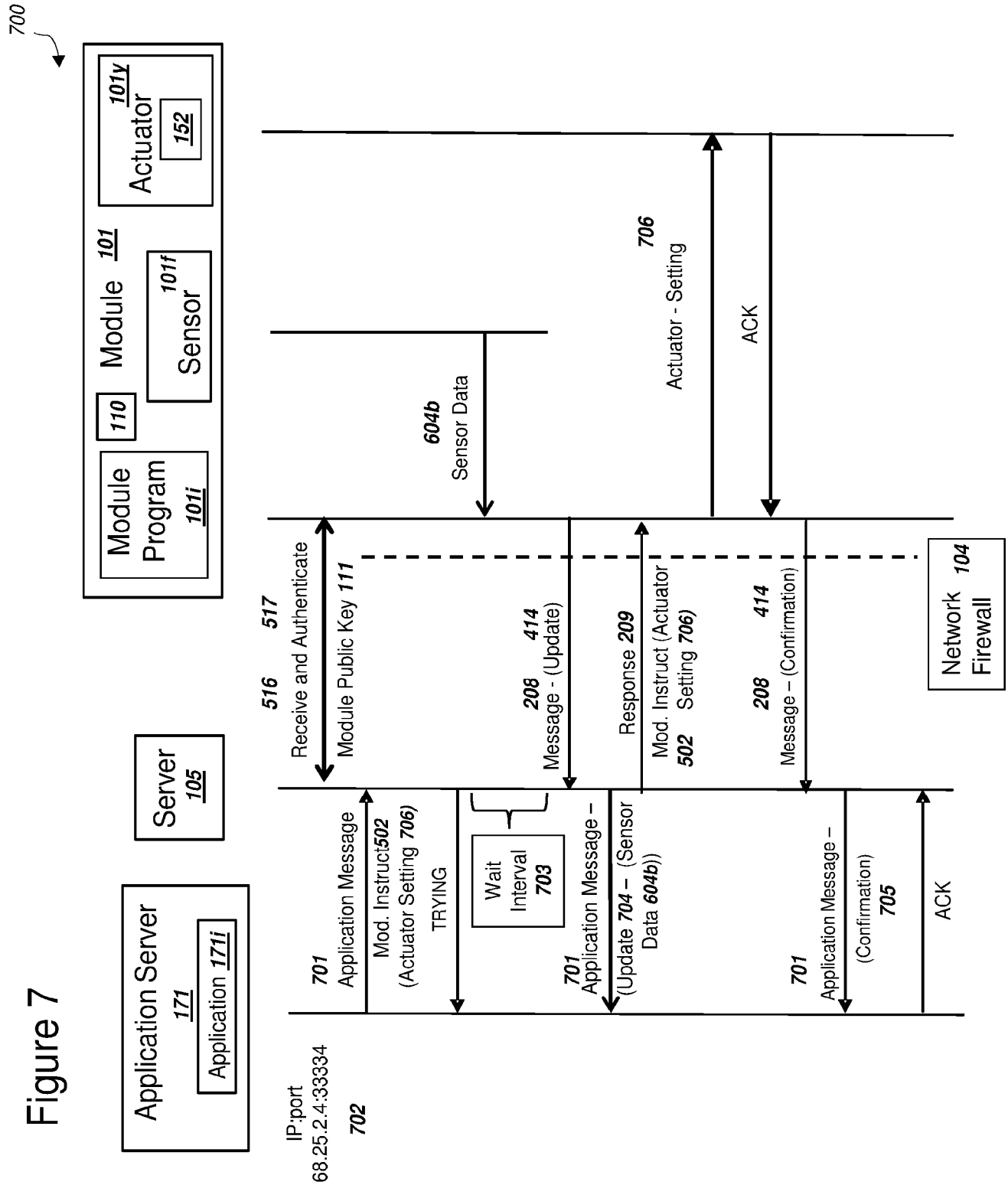
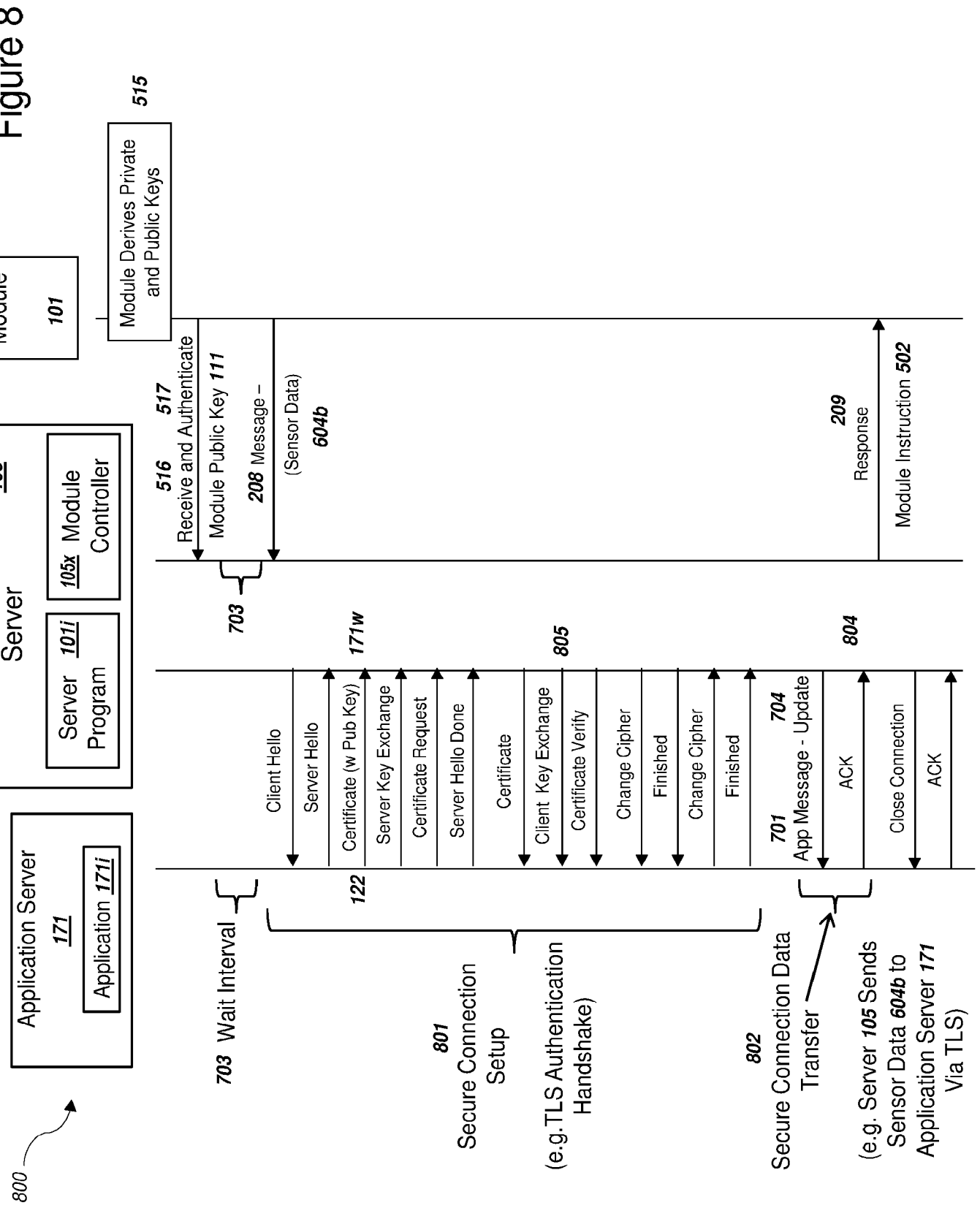

700
Application Server
171
Application 171i
IP:port
68.25.2.4:33334
702
Server
105
Module 101
Module Program 101i
110
Sensor 101f
Actuator 101y
152
Network Firewall 104
516 Receive and Authenticate
517 Module Public Key 111
701 Application Message
Mod. Instruct 502 (Actuator Setting 706)
TRYING
Wait Interval 703
701 Application Message – (Update 704 – (Sensor Data 604b))
604b Sensor Data
208 414 Message - (Update)
Response 209
Mod. Instruct (Actuator 502 Setting 706)
706 Actuator - Setting
ACK
208 414 Message – (Confirmation)
701 Application Message – (Confirmation) 705
ACK

Figure 8


800
Application Server 171
Application 171i
Server 105
Server Program 101i
105x Module Controller
Module 101
Module Derives Private and Public Keys 515
516 Receive and Authenticate
517 Module Public Key 111
208 Message – (Sensor Data) 604b
209 Response
Module Instruction 502
703
703 Wait Interval
171w
805
804
Client Hello
Server Hello
Certificate (w Pub Key)
Server Key Exchange
Certificate Request
Server Hello Done
Certificate
Client Key Exchange
Certificate Verify
Change Cipher
Finished
Change Cipher
Finished
701 App Message - Update
704
ACK
Close Connection
ACK
122
801 Secure Connection Setup (e.g.TLS Authentication Handshake)
802 Secure Connection Data Transfer
(e.g. Server 105 Sends Sensor Data 604b to Application Server 171 Via TLS)

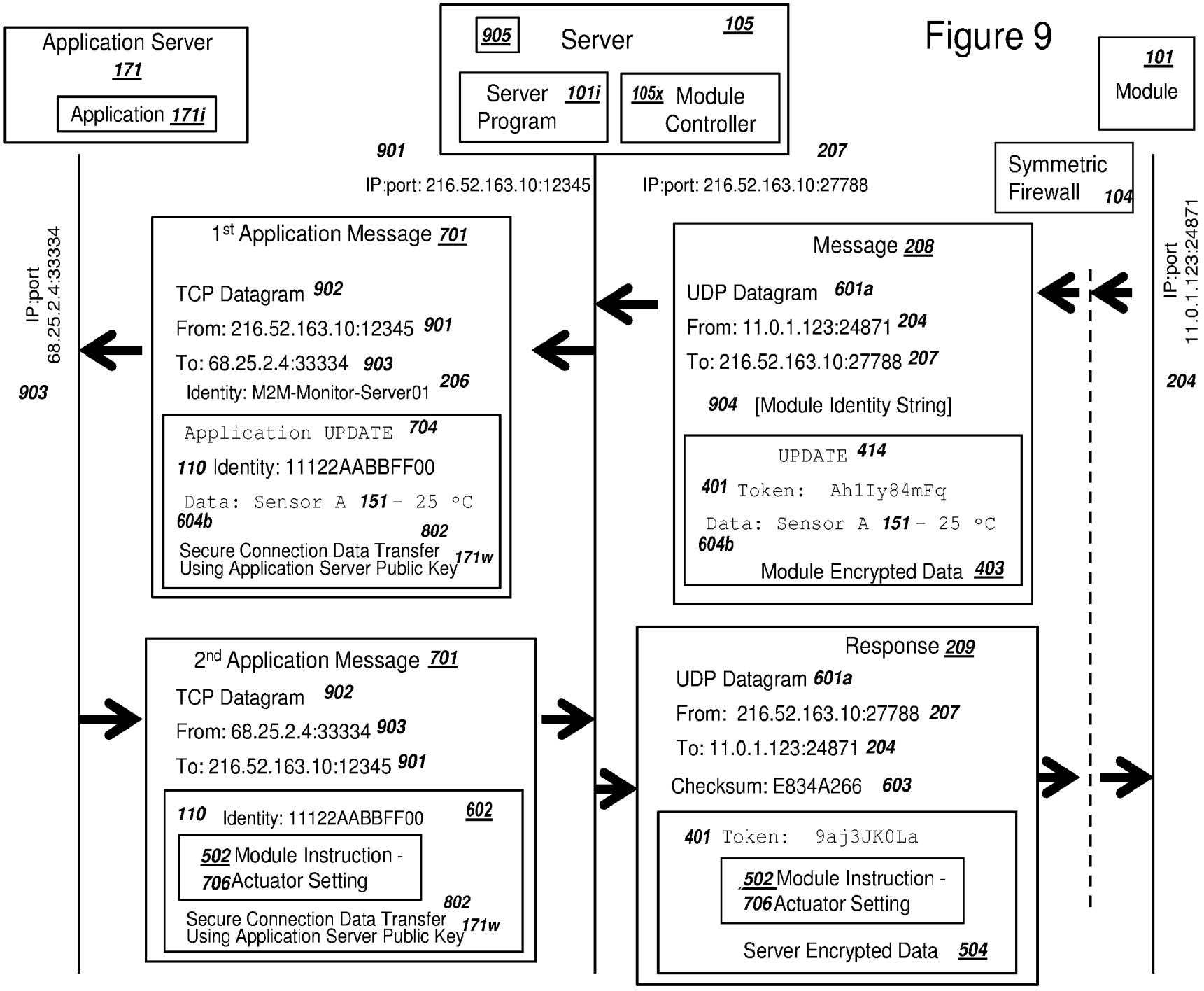


Figure 9

Petitioner Samsung Ex-1038, 0021

Atty. Dkt. No. 63121/0213

Figure 10

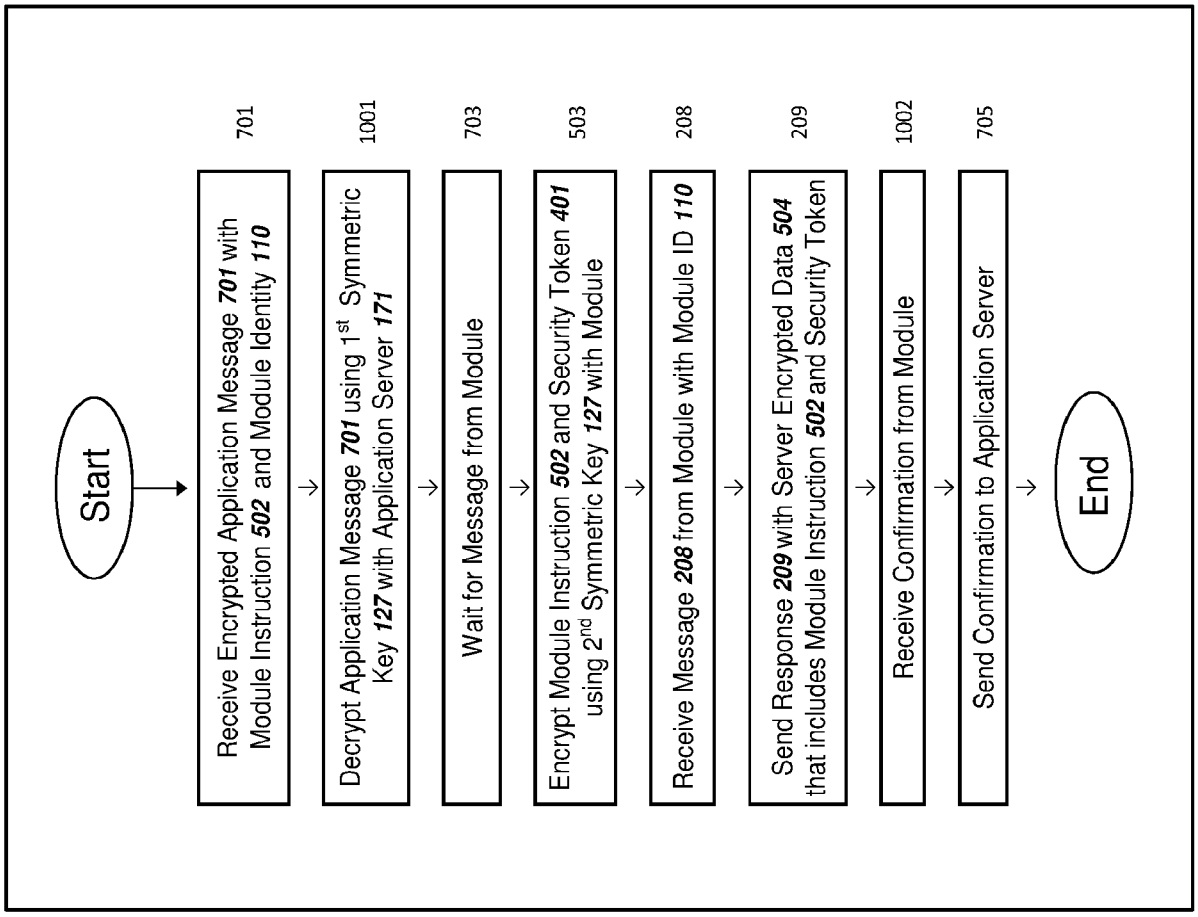
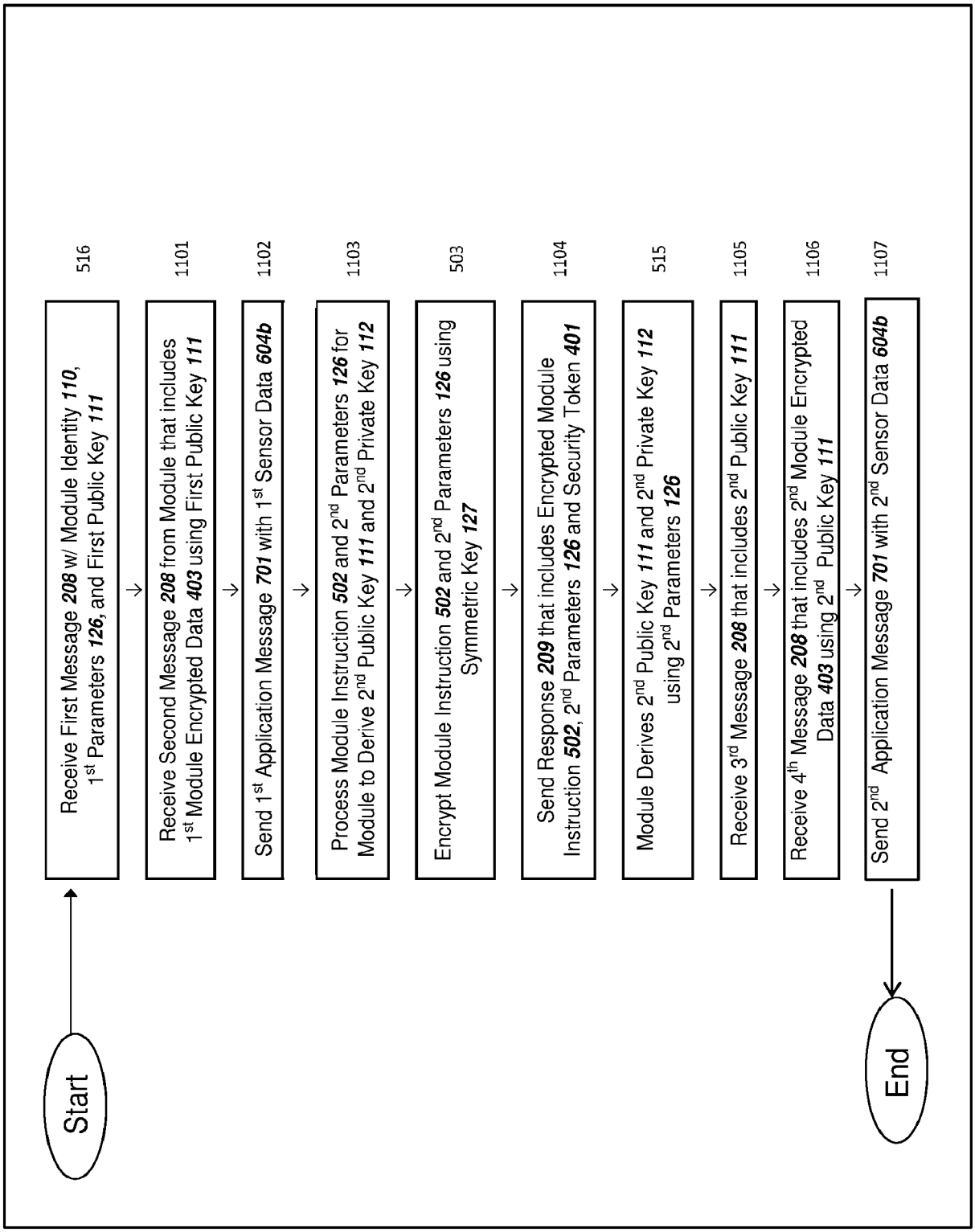

Start
Receive Encrypted Application Message 701 with Module Instruction 502 and Module Identity 110
701
Decrypt Application Message 701 using 1st Symmetric Key 127 with Application Server 171
1001
Wait for Message from Module
703
Encrypt Module Instruction 502 and Security Token 401 using 2nd Symmetric Key 127 with Module
503
Receive Message 208 from Module with Module ID 110
208
Send Response 209 with Server Encrypted Data 504 that includes Module Instruction 502 and Security Token
209
Receive Confirmation from Module
1002
Send Confirmation to Application Server
705
End

Figure 11


Start
Receive First Message 208 w/ Module Identity 110, 1st Parameters 126, and First Public Key 111
516
Receive Second Message 208 from Module that includes 1st Module Encrypted Data 403 using First Public Key 111
1101
Send 1st Application Message 701 with 1st Sensor Data 604b
1102
Process Module Instruction 502 and 2nd Parameters 126 for Module to Derive 2nd Public Key 111 and 2nd Private Key 112
1103
Encrypt Module Instruction 502 and 2nd Parameters 126 using Symmetric Key 127
503
Send Response 209 that includes Encrypted Module Instruction 502, 2nd Parameters 126 and Security Token 401
1104
Module Derives 2nd Public Key 111 and 2nd Private Key 112 using 2nd Parameters 126
515
Receive 3rd Message 208 that includes 2nd Public Key 111
1105
Receive 4th Message 208 that includes 2nd Module Encrypted Data 403 using 2nd Public Key 111
1106
Send 2nd Application Message 701 with 2nd Sensor Data 604b
1107
End

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 01/31/2018. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	
Filing Date	Herewith
First Named Inventor	John A. Nix
Title	Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)
Art Unit	
Examiner Name	
Attorney Docket Number	63121/0213

SIGNATURE of Applicant or Patent Practitioner

Signature	/Albert J. Boardman/	Date (Optional)	2022-01-12
Name	Albert J. Boardman	Registration Number	70,601
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☑ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. 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 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 01912

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

NETWORK-1 TECHNOLOGIES, INC.

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature		Date (Optional)	
Name	Corey M. Horowitz		
Title	Chairman and CEO		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☑ Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. 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 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR UNITED STATES PATENT

Title: **Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)**

Inventor: John A. Nix

Petitioner Samsung Ex-1038, 0026

CROSS-REFERENCE TO RELATED APPLICATIONS

This is a continuation of U.S. Patent Application No. 16/593,561, filed October 4, 2019, which is a continuation of U.S. Patent Application No. 16/036,506 filed July 16, 2018, now U.S. Patent No. 10,530,575, which is a continuation of U.S. Patent Application No. 15/583,968 filed May 1, 2017, now U.S. Patent No. 10,057,059, which is a continuation of U.S. Patent Application No. 15/010,905 filed January 29, 2016, now U.S. Patent No. 9,641,327, which is a continuation of U.S. Patent Application No. 14/055,606 filed October 16, 2013, now U.S. Patent No. 9,276,740, each of which is fully incorporated by reference herein.

The subject matter of this application is related to the subject matter of U.S. Patent Application Serial No. 14/023,181, filed September 10, 2013, which issued as U.S. Patent No. 9,350,550, in the name of John Nix, entitled "Power Management and Security for Wireless Modules in 'Machine-to-Machine' Communications," which is hereby incorporated by reference in its entirety.

The subject matter of this application is also related to the subject matter of U. S. Patent Application Serial No. 14/039,401, filed September 27, 2013, which issued as U.S. Patent No. 9,288,059 in the name of John Nix, entitled "Secure PKI Communications for 'Machine-to-Machine' Modules, including Key Derivation by Modules and Authenticating Public Keys," which is hereby incorporated by reference in its entirety.

BACKGROUND

Technical Field

The present methods and systems relate to communications between wireless modules and a network, and more particularly, to efficient methods and systems for supporting secure, efficient, and flexible communications using Internet Protocol networks, where a server can communicate with both a "machine-to-machine" modules and an application.

Petitioner Samsung Ex-1038, 0027

Description of Related Art

The combination of "machine-to-machine" (M2M) communications and using low-cost sensors, Internet connections, and processors is a promising and growing field. Among many potential benefits, M2M technologies allow the remote monitoring of people, assets, or a location where manual monitoring is not economic, or costs can be significantly reduced by using automated monitoring as opposed to manual techniques. Prominent examples today include vending machines, automobiles, alarm systems, and remote sensors. Fast growing markets for M2M applications today include tracking devices for shipping containers or pallets, health applications such as the remote monitoring of a person's glucose levels or heartbeat, monitoring of industrial equipment deployed in the field, and security systems. Many M2M applications leverage either wired Internet connections or wireless connections, and both types of connections continue to grow rapidly. M2M applications may also be referred to as "the Internet of things".

M2M communications can provide remote control over actuators that may be connected to a M2M device, such as turning on or off a power switch, locking or unlocking a door, adjusting a speed of a motor, or similar remote control. A decision to change or adjust an actuator associated with an M2M device can utilize one or a series of sensor measurements. An M2M device may also be referred to as a "wireless module" or also simply a module. As one example, if a building or room is too cold, then temperature can be reported to a central server by an M2M device and the server can instruct the M2M device to turn on a switch that activates heat or adjusts a thermostat. As the costs for computer and networking hardware continue to decline, together with the growing ease of obtaining either wired or wireless Internet access for small form-factor devices, the number of economically favorable applications for M2M communications grows.

Many M2M applications can leverage wireless networking technologies. Wireless technologies such as wireless local area networks and wireless wide area networks have proliferated around the world over the past 15 years, and usage of these wireless networks is also expected to continue to grow. Wireless local area network (LAN) technologies include WiFi and wireless wide area network (WAN) technologies include 3rd Generation Partnership Project's (3GPP) 3rd Generation (3G) Universal Mobile Telecommunications System (UMTS) and 4th Generation (4G) Long-term Evolution (LTE), LTE Advanced, and the Institute of Electrical and Electronics Engineers' (IEEE) 802.16 standard, also known as WiMax. The use of wireless technologies with

Petitioner Samsung Ex-1038, 0028

"machine-to-machine" communications creates new opportunities for the deployment of M2M modules in locations without fixed-wire Internet access, but also creates a significant new class of problems that need to be solved. First, many wireless wide-area networking standards were designed and optimized for mobile phones, which may be continuously connected to the network during the day (i.e. non-sleeping hours for most subscribers while they may charge phones at night), in order to receive inbound phone calls and messages. In this case, the radio may be in an idle state but utilizing discontinuous reception, but the radio is still active and drawing power in order to receive and process incoming signaling from the network such as a Public Land Mobile Network (PLMN). A need exists in the art to make wireless M2M communications efficient in order to conserve battery life and radio-frequency spectrum resources.

Since the packets transmitted and received by a wireless module will likely traverse the public Internet for many applications, a need exists in the art to (i) prevent eavesdropping at intermediate points along the path of packets transmitted and received, (ii) allow endpoints to verify the identity of the source of packets received. A need exists in the art for a wireless module and a monitoring server to leverage established public key infrastructure (PKI) techniques and algorithms. A need exists in the art for communication to be secured without requiring the established, but relatively processing, bandwidth, and energy intensive security protocols, such as IPSec, Transport Layer Security (TLS), and Secure Socket Layer (SSL). The establishment of theses links requires extra overhead in the form of packet handshakes and/or key exchanges at levels including the network and transport layer of the traditional Open Systems Interconnection (OSI) model. M2M applications frequently require small, periodic messages sent between a wireless module and a monitoring server, where the wireless module sleeps between the messages. M2M applications may leverage wired modules as well which also sleep between messages. During relatively long periods of sleep such as 30 minutes or more, the a wireless or wired network with intermediate firewalls will often tear down the network and/or transport layer connections, which means the wireless module would need to re-negotiate or reestablish the secure tunnels each time the wireless module wakes and seeks to send a relatively small message to a server. A need exists in the art for supporting established security protocols with an external application, without requiring them to be implemented on a module due to the relatively long periods of sleep and other complexities from inactivity in the module.

Petitioner Samsung Ex-1038, 0029

Next, a need exists in the art for the communication between a module and a monitoring server to be highly energy and bandwidth efficient in order to reduce energy consumption over the operating lifetime of a module. A limiting factor for a wireless module for M2M applications deployed or installed into the field is the lifetime of the battery of the wireless module. If the transmission techniques for the wireless module are not energy efficient, the system will require more frequent manual intervention for the replacement or recharging of batteries. If the battery becomes sufficiently low, then communication with the wireless module will be lost, or the frequency would have to be reduced for sensor measurements sent by the wireless module or actuator commands sent by a monitoring server. The energy saving techniques for transmitting and receiving data should leverage established Internet protocols, in order to utilize the public Internet, in addition to the need for secure communications noted above. For wired modules operating for years or decades, a significant cost will be the power consumed from land-line power.

Further, a need exists in the art for the secure, energy efficient communications that support Internet protocols to support intermediate firewalls that may exist along the path of packets sent and received by both a wireless module and a monitoring server. Without support for communication through an intermediate firewall, packets may be blocked by the firewall and the M2M application would not properly function in this case. A need exists in the art for techniques of secure and energy-efficient communications between modules and monitoring servers to support a wide variety of manufacturers of modules and M2M applications. Currently, there are dozens of manufacturers and form-factors of modules, and this diversity will continue to increase for the foreseeable future. By leveraging standards such as the Internet and PKI technologies, an efficient, secure, and highly scalable system of communicating could support the wide variety of modules.

In addition, the utilization of PKI technologies in modules can increase security, but a number of technical challenges must be addressed. These challenges increase if a deployed module required updated private/public key pairs after operation begins. The typical paradigm of "swapping out a SIM card" (which also depend on a pre-shared secret key Ki embedded in the card) with mobile phones may not be applicable or cost effective with modules, where swapping out the SIM card could be burdensome. A need exists in the art to allow for a deployed module to securely and automatically begin using new private and public keys (i.e. without human intervention such as swapping out a SIM card). Newer PKI technologies may offer a wide variety of algorithms for ciphering with public keys, and a need exists in the art for the utilization of new public and private

Petitioner Samsung Ex-1038, 0030

keys to support the wide variety of algorithms, even after a module has been installed. In other words, a system should preferably both be highly secure and also flexible enough to adopt new security keys and standards. A need exists in the art for a scalable and secure method of associating a module identity with a module public key, when the module begins utilizing a new public key. A need exists in the art for a module to efficiently be able to utilize multiple public/private key pairs at the same time, such as with different service providers or different applications simultaneously.

Another desirable feature is for an M2M module to efficiently and securely communicate with applications. Applications can include a web-based interface for users to view status or input settings for a plurality of modules, and the modules may be associated with an M2M service provider. However, a set of PKI algorithms, keys, and communication protocols within used by the module for efficient communications module may not be directly compatible with an application. As one example, the application on a web server may prefer to use a transport layer security (TLS) protocol with transmission control protocol (TCP) datagrams, while for energy efficiency and to conserve battery life, an M2M module may prefer to use user datagram protocol (UDP). A need exists in the art for an intermediate server to securely translate secure communications to/from a module into secure communication from/to an application. As another example, it would be desirable for a module to support elliptic key cryptography (ECC), while the application may support RSA-based cryptography, and therefore a need exists in the art for a server to securely translate between the two cryptographic methods, thereby allowing the M2M module to communicate with the application.

And other needs exist in the art as well, as the list recited above is not meant to be exhaustive but rather illustrative.

Petitioner Samsung Ex-1038, 0031

SUMMARY

Methods and systems are provided for secure and efficient communication using a server to communicate with modules and an application. The modules and application can support "Machine to Machine" communications. The methods and systems contemplated herein can also support other applications as well, including mobile phone handsets connecting to a wireless network. An objective of the invention is to address the challenges noted above for securing the deployment of modules that utilize PKI algorithms and keys, as well as increasing efficiency in order to reduce power consumption, including extending the battery life of a module, if present. More efficient communication can also conserve valuable radio-frequency spectrum, among other benefits. Using a server for secure and reliable communication of data between an application and a module can increase the value and usefulness of modules for a user.

An exemplary embodiment may take the form of methods and systems for a server to securely receive data from a module and forward the data to an application server, and an application may operate on the application server. The application can include a graphical user interface for a user to visually see reports and/or control modules. The module, server, and application can preferably include a set of cryptographic algorithms for use in sending and receiving data. The cryptographic algorithms can include asymmetric ciphering algorithms, symmetric ciphering algorithms, secure hash algorithms, digital signature algorithms, key pair generation algorithms, a key derivation function, and/or a random number generator.

The module can utilize the set of cryptographic algorithms to securely generate or derive a module private key and a module public key. The module private key and module public key can be generated either (i) upon initial use or installation of the module, or (ii) at a subsequent time after initial use such as when a new set of key pairs are required or are useful for continued operation of the module. After deriving the module public key and module private key, the module private key is preferably recorded in a secure or protected location in a nonvolatile memory within the module. The module may then utilize the recorded pre-shared secret key to authenticate with a server that also records or has access to the pre-shared secret key. The authentication could comprise either using message digest with the pre-shared secret key, or using the pre-shared secret key as a symmetric ciphering key, and the authentication may also utilize a second key derived by both the

Petitioner Samsung Ex-1038, 0032

module and the server using the pre-shared secret key. After authentication, the server can authoritatively record the derived module public key with the module identity in a database. Thus, the use of a pre-shared secret key can ensure the submitted module public key is validly associated with the module and module identity. The module can be associated with a monitored unit and the module can use a sensor to collect data regarding the monitored unit. The module may also optionally include an actuator for controlling a state of the monitored unit, although the actuator may optionally be omitted.

The server can include a private key associated with the server and the derived public key associated with the module. The server public key can leverage established public key infrastructure (PKI) standards, such as X.509 v3 certificates and RSA or elliptic curve cryptography (ECC) algorithms and include a digital signature from a certificate authority. The server can use a module controller and an operating system plus a connection to the Internet to monitor a socket for incoming messages from a module. After receiving the module public key, including potentially after a period of sleep or dormancy by the module, the server can receive a message, where the message includes a module identity and a module encrypted data. The module encrypted data can include a server instruction, a security token, and additional data such as a sensor measurement. The server can decrypt the module encrypted data using the received module public key and extract plaintext data from the module encrypted data.

The server can establish a secure connection with the application server using a secure connection setup, which could comprise the initial handshake messages for a transport-layer security protocol such as transport layer security (TLS) or IPSec. The secure connection setup can include the transfer of a server public key and an application server public key. The server can send an application message to the application server using a secure connection data transfer, where the application message includes data received from the module such as a sensor measurement or sensor data. The server can use (i) an RSA-based asymmetric ciphering algorithm and first public key with the application server to securely transfer a first symmetric key to the application server, and (ii) an ECC-based asymmetric ciphering algorithm and second public key with the module to securely transfer a second symmetric key to the module. The server may also preferably use a transmission control protocol (TCP) with the application server and a user datagram protocol (UDP) with the module. The application message to the application server can include a server identity, an encrypted update instruction, and the sensor data. The sensor data may also include a sensor

Petitioner Samsung Ex-1038, 0033

identity. The server can use a first Internet protocol address and port (IP:port) number for receiving the message from the module and a second IP:port number for sending the application message to the application server. The application server can record the sensor data in an application database for subsequent processing and analysis for a user or other business or commercial needs.

In another embodiment, the module may be deployed within a wireless network such as a 4G LTE network or a WiFi network. The module can change state between a sleep state and an active state, wherein the sleep state may utilize a few milliwatts or less and the active state, including transmission of radio signals, may utilize several hundred milliwatts of power or more. After being installed next to a monitored unit, the wireless module can wake from a sleep or dormant state, utilize a sensor to collect data associated with the monitored unit, connect to the wireless network and the Internet, and send the sensor data to a server. During an active period, the module can use a UDP IP:port number to both send a message to the server and receive a response to the server. The message as a UDP datagram can be a UDP Lite datagram and with a checksum only applied to the packet header. A UDP Lite datagram with sensor data can include channel coding for the body of the datagram to mitigate the effect of bit errors. Or, a regular UDP packet could be sent in multiple copies in order to provide forward error correction.

In another embodiment of the present invention, the application server may send an application message to the server using a secure connection data transfer. The application message could be encrypted using a first server public key and could include a module identity and a module instruction. The module instruction can include an actuator setting, and also optionally an actuator identity (since the module may include multiple actuators). The server can decrypt encrypted data within the application message and record the module identity and module instruction in memory or a module database. Since the module can transition between periods of sleep and active states to conserve power, after receiving the application message the server can wait until a next message is received from the module with the module identity before sending the module instruction in a response. After waiting for the next message, the server can send the module instruction to the module in a server encrypted data using a second server public key. The first and second server public keys can use different cryptographic algorithms that are not directly compatible (i.e. the first server public key could be RSA-based and the second server public key could be ECC-based).

Petitioner Samsung Ex-1038, 0034

In another embodiment, the server can securely send the module a set of parameters, where the set of parameters includes values to define an equation for an elliptic curve. The values could comprise constants and variables such that the module can calculate a new elliptic curve, and the elliptic curve can be different than standard, published curves. The set of parameters could be sent from the server to the module in a server encrypted data, where the server encrypted data was processed using any of (i) a first module public key, (ii) a symmetric key, and (iii) a shared secret key. The module can use the set of parameters, a random number generator, and a key generation function within a cryptographic algorithms in order to generate a new key pair, which could comprise a second module public key and a second module private key. The module can securely and/or authoritatively send the second module public key to the server, where the security includes the use of the first module public key and/or the shared secret key.

Continuing with this embodiment, after the server confirms the proper receipt of the second module public key in a response message, the server and the module can begin secure communications between them using the second module public key. By using this exemplary embodiment, security can be further increased with the server and module using an elliptic curve that can be unique, non-standard, or defined between them and security therefore increased. In this exemplary embodiment, the parameters to define the elliptic curve equation are sent securely to the module, so an observer along the flow of data could not observe the elliptic equation being used with a public key.

In yet another embodiment, the server can receive a first message with a module identity and a module encrypted data, where the first module encrypted data includes a first sensor measurement. The server can use a first module public key associated with a first module public key identity to decrypt the first module encrypted data. As one example, (a) the first module encrypted data could be ciphered with a symmetric key, and (b) the symmetric key could have been communicated using the first module public key (including using the first module public key to verify a module digital signature in a session where the symmetric key was transferred), and therefore (c) the module encrypted data could be encrypted using the first module public key. The server can also use a first server public key to decrypt the first module encrypted data, such as the symmetric key being derived using both the first module public key and the first server public key and a key derivation function within a cryptographic algorithms. The server can extract the first sensor measurement and send the data to an application server in an application message. The

Petitioner Samsung Ex-1038, 0035

application message could be encrypted using a second server public key. The first and second server public keys can be different because they could each be associated with a different algorithm or defining equation.

Continuing with this embodiment, the server can send a module instruction and a set of parameters to the module, where the module is instructed to derive a new set of keys, and the module can subsequently derive a second module public key and a second module private key after receiving the module instruction. The module can then send the second module public key, a second module public key identity, and the module identity to the server. The server can receive a second module encrypted data that includes a second sensor data, where the second sensor data is encrypted using the second module public key. As one example, (a) the second module encrypted data could be ciphered with a symmetric key, and (b) the symmetric key could have been communicated using the second module public key (including using the second module public key to verify a module digital signature in a session where the symmetric key was transferred), and therefore (c) the module encrypted data could be encrypted using the second module public key. The server can extract the second sensor data using the second module public key. The server can use the second server public key to send a second application message with the second sensor data to the application server. Note that the module public key can change, but both (i) the second server public key used with the application server and also (ii) keys associated with the application server did not change. In this manner according to this embodiment, a module can derive a new public and private key while a server and application server can continue to communicate using existing public and private keys.

In another embodiment, the application server can use a module public key and an asymmetric ciphering algorithm to encrypt a module instruction. The application server can also include a digital signature of the module instruction using the application server private key. The encrypted module instruction and digital signature can be sent to a server in an application message, and the application message can also include an identity of the application server. The server can wait until a message is received from a module, and then send the encrypted module instruction and digital signature to the module in a response. The module can read receive the response, read the identity of the application server, select a public key of the application server, verify the digital signature of the module instruction, and decrypt the module instruction using the module private key. The module can then apply the module instruction and send a message with a confirmation. In

Petitioner Samsung Ex-1038, 0036

this manner, the module may receive instructions from the application that are not decrypted by the server.

These as well as other aspects and advantages will become apparent to those of ordinary skill in the art by reading the following detailed description, with reference where appropriate to the accompanying drawings.

Petitioner Samsung Ex-1038, 0037

BRIEF DESCRIPTION OF THE DRAWINGS

Various exemplary embodiments are described herein with reference to the following drawings, wherein like numerals denote like entities.

Figure 1a is a graphical illustration of an exemplary system, where a server and a module connect to the Internet, in accordance with exemplary embodiments;

Figure 1b is a graphical illustration of hardware, firmware, and software components for a module, in accordance with exemplary embodiments;

Figure 1c is a graphical illustration of hardware, firmware, and software components for a server, in accordance with exemplary embodiments;

Figure 1d is a graphical illustration of hardware, firmware, and software components for an application server, in accordance with exemplary embodiments;

Figure 1e is a graphical illustration of the components within a module, in accordance with exemplary embodiments;

Figure 1f is a graphical illustration of the components within a server, in accordance with exemplary embodiments;

Figure 1g is a graphical illustration of the components in a set of cryptographic algorithms, in accordance with exemplary embodiments;

Figure 1h is an illustration of a certificate that includes a PKI public key, where the key comprises an elliptic curve cryptography (ECC) key, in accordance with exemplary embodiments;

Figure 1i is a graphical illustration of an exemplary system that includes a user, an application, a set of servers, and a set of modules, in accordance with exemplary embodiments;

Figure 2 is a graphical illustration of an exemplary system, where a module sends a message to a server, and where the server responds to the message, in accordance with exemplary embodiments;

Petitioner Samsung Ex-1038, 0038

Figure 3 is a flow chart illustrating exemplary steps for a server to receive a message from a module, in accordance with exemplary embodiments;

Figure 4 a is a flow chart illustrating exemplary steps for a server to process a message, including verifying a module's identity and decrypting data, in accordance with exemplary embodiments;

Figure 5a is a flow chart illustrating exemplary steps for a server to process a response for a module, including sending and signing an module instruction, in accordance with exemplary embodiments;

Figure 5b is a flow chart illustrating exemplary steps for a server to communicate with a module that has derived a public key and private key, in accordance with exemplary embodiments;

Figure 6a is a simplified message flow diagram illustrating an exemplary message received by a server, and an exemplary response sent from the server, in accordance with exemplary embodiments;

Figure 6b is a simplified message flow diagram illustrating an exemplary message received by a server, wherein the message includes a derived module public key, in accordance with exemplary embodiments;

Figure 7 is a simplified message flow diagram illustrating an exemplary system with exemplary data transferred between a module and an application using a server, in accordance with exemplary embodiments;

Figure 8 is a simplified message flow diagram illustrating an exemplary system with exemplary data transferred between a module and an application using a server, in accordance with exemplary embodiments;

Figure 9 is a simplified message flow diagram illustrating exemplary data transferred between (i) a server and an application and between (ii) a server and a module, in accordance with exemplary embodiments;

Petitioner Samsung Ex-1038, 0039

Figure 10 is a flow chart illustrating exemplary steps for a server to receive a module instruction within an application message, and for the server to send the module instruction to a module, in accordance with exemplary embodiments;

Figure 11 is a flow chart illustrating exemplary steps for a server to communicate with an application and a module, in accordance with exemplary embodiments.

Petitioner Samsung Ex-1038, 0040

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS OF THE INVENTION

Figure 1a

Figure 1a is a graphical illustration of an exemplary system, where a server and a module connect to the Internet, in accordance with exemplary embodiments. The system 100 includes a module 101 operating within a wireless network 102. System 100 can also include a module provider 109, an Internet 107, and an M2M service provider 108, a certificate authority 118, and a monitored unit 119. M2M service provider 108 can include a server 105. System 100 is illustrated without specific packet transmissions between module 101 and M2M service provider 108. Examples of the communications and messages pertaining to the present invention will be illustrated in later Figures. As contemplated herein, machine-to-machine communications may comprise communication between a module 101 and a server 105, such that data can be transferred between the two with minimal manual intervention, although manual intervention can be required to set up system 100 and any occasional manual maintenance required. As contemplated herein, machine-to-machine communications may also be referred to as "the Internet of things" (IoT). Also note that module 101 may comprise a wireless module, such that module 101 can communicate with wireless network 102 using a radio and an antenna. Thus, either a wireless or a wired configuration for module 101 can be utilized in the present invention.

If module 101 operates as a wireless module, module 101 and wireless network 102 can communicate using a base station 103. Module 101 and wireless network 102 can utilize a variety of wireless technologies to communicate, including WiFi, WiMax, a 2nd generation wireless wide area network (WAN) technology such as General Packet Radio Services (GPRS) or Enhanced Data rates for GSM Evolution (EDGE), 3rd Generation Partnership Project (3GPP) technology such as 3G, 4G LTE, or 4G LTE Advanced, and other examples exist as well. A wired module 101 can connect to the Internet 107 via a wired connection such as an Ethernet, a fiber optic, or a Universal Serial Bus (USB) connection (not shown).

Generally, the communication techniques described herein can be independent of the network technologies utilized at the physical and data-link layers, so long as the underlying network provides access to the Internet 107 and supports Internet Protocols (IP). The Internet 107 can be an

Petitioner Samsung Ex-1038, 0041

IPv4 or an IPv6 packet-switched based network that utilizes standards derived from the Internet Engineering Task Force, such as RFC 786 (User Datagram Protocol), RFC 793 (Transmission Control Protocol), and related protocols. The Internet 107 can be the public Internet comprising globally routable IP addresses, or a private network that utilizes private IP addresses. Although Internet 107 is illustrated as the globally routable public Internet in Figure 1, Internet 107 could also be a private Internet that is (i) not globally routable and (ii) only accessible to authorized modules and servers. As one example of a private Internet 107, Internet 107 could use private IP addresses for nodes on the network, and in this case Internet 107 could be referred to as an intranet or private network. Alternatively, Internet 107 could be a private network layered on top of the publicly routable Internet via secured and encrypted connections. The specific numbers for IP addresses and port numbers shown in Figure 1 and other figures are illustrative and any valid IP address or port number can be used, including an IPv4 and an IPv6 address.

When operating in a wireless network configuration, module 101 can access the Internet 107 via the wireless network 102. In the wireless network configuration, module 101 can be a wireless handset, a cellular phone, a smartphone, a tablet computer, a laptop, a computer with a radio, a tracking device, or a circuit board with a radio that accesses wireless network 102. Examples of wireless modules that utilize a wireless WAN such as 2G and 3G networking technologies include the Motorola® G24-l and Huawei® MC323. Example manufacturers of wireless modules in 2012 include Sierra Wireless® and Telit®. In a wired configuration (not shown), module 101 can be a computer, security camera, security monitoring device, networked controller, etc. A more detailed depiction of exemplary components of a module 101 is included in Figure 1b and Figure 1e below. Module 101 could also comprise a "point of presence" payment terminal, such that a sensor associated with module 101 could collect payment information such as an account number from a credit card or similar payment card. Module 101 could communicate with the payment card via a magnetic reader or near-field wireless communications, and in this case the magnetic reader or antenna for near-field communications can function as a sensor. Module 101 could also operate as a "smartcard" such that an end user presents module 101 to merchants for payments.

Wireless network 102 may comprise either a wireless local area network (LAN) such as an 802.11 WLAN, Bluetooth, or Zigbee among other possibilities, and module 101 operating in wireless mode could communicate with a base station 103 of a wireless network 102 using a radio and an antenna. Wireless network 102 could operate as a Mode II device according to FCC

Petitioner Samsung Ex-1038, 0042

Memorandum Opinion and Order (FC-12-36) and related white space regulation documents. If module 101 supports IEEE 802.15.4, then wireless network 102 could be a Zigbee network, an ISA100.11a standards-based network, or a 6LoWPAN network as described by IETF RFC 4944. Other possibilities exist as well for the wireless technology utilized by a wireless network 102 and module 101, operating in a wireless mode, without departing from the scope of the present invention.

Module 101 can collect data regarding a monitored unit 119 and periodically report status to an M2M service provider 108 or a server 105. Examples of a monitored unit 119 can include a vending machine, an alarm system, an automobile or truck, a standard 40-foot or 20-foot shipping container, or industrial equipment such as a transformer on an electrical grid or elevator in a building. Additional examples of a monitored unit 119 include can also include a pallet for shipping or receiving goods, an individual box of pharmaceuticals, a health monitoring device attached to a person such as a pacemaker or glucose monitor, and a gate or door for opening and closing. Other examples exist as well without departing from the scope of the present invention. Module 101 can utilize a sensor to measure and collect data regarding a parameter of monitored unit 119 such as temperature, physical location potentially including geographical coordinates from a Global Positioning System (GPS) receiver, radiation, humidity, surrounding light levels, surrounding RF signals, weight, vibration and/or shock, voltage, current, and/or similar measurements. If monitored unit 119 is a person or a health monitoring device associated with a person, then relevant health data could be recorded by module 101 in order to transmit to a M2M service provider 108, which could be associated with a health service such as a hospital, doctor's office, or a similar health service. Module 101 could also periodically record a picture, image, or video of or around monitored unit 119, using either visible or infrared light.

As illustrated in Figure 1a, wireless network 102 may include a wireless network firewall 104 and M2M service provider 108 may include a server network firewall 124. These firewalls may be used to secure communication at the data link, network, transport, and/or application layers of communications using the Internet 107. Firewalls 104 and 124 could perform network address translation (NAT) routing or operate as symmetric firewalls, and selectively filter packets received through Internet 107 in order to secure system 100. The firewall functionality of firewalls 104 and 124 could be of many possible types, including a symmetric firewall, a network-layer firewall that filters inbound packets according to pre-determined rules, an application-layer firewall, or a NAT

Petitioner Samsung Ex-1038, 0043

router, as examples. Although a single firewall 104 and 124 is illustrated in wireless network 102 and with M2M service provider 108, respectively, firewall 104 and 124 may each comprise multiple firewalls that operate in conjunction and the combined operation may be considered a single firewall 104 and 124, respectively. Firewall 104 and/or firewall 124 can include a firewall port binding timeout value 117 (illustrated in Figure 2), which can represent the time allowed for an inbound packet from the Internet 107 to pass through firewall 104 or firewall 124 after module 101 or server 105, respectively, sends a packet out. Firewall port binding timeout value 117 may be determined on a per-protocol basis, such as an exemplary time of 60 seconds for UDP packets and 8 minutes for TCP packets, although other time values for a firewall port binding timeout value 117 are possible as well. Inbound packets from Internet 107 to module 101 may be dropped by firewall 104 after a time exceeding firewall port binding timeout value 117 has transpired since the last packet transmitted by module 101.

According to a preferred exemplary embodiment, module 101 may preferably record a module private key 112. As described in additional figures below, module 112 can generate a key pair comprising a module private key 112 and a module public key 111, where module private key 112 resides within module 101 and may not be shared or transmitted to other parties. Alternatively, the present invention also contemplates that module 101 does not derive its own module private key 112, and rather module private key 112 is securely loaded or transmitted to module 101. Module 101 may also be associated with a module provider 109. Module provider 109 could be a manufacturer or distributor of module 101, or may also be the company that installs and services module 101 or associates module 101 with monitored unit 119. Although not illustrated in Figure 1a, module provider 109 could deliver module 101 to an end-user, where the end-user associates module 101 with monitored unit 119. Module provider 109 can record a module public key 111 and a certificate 122 (illustrated below in Figure 1e and Figure 1h) for module 101. Module public key 111 may be associated with a module public key identity 111a, which could be an identifier of module public key 111. Module 101 may utilize a plurality of module private keys 112 and module public keys 111 during the operation of a system 100, although the use of a plurality of keys may not be required in order to use some embodiments of the invention contemplated herein.

As discussed below, a module 101 may utilize multiple module public keys 111 over the lifetime of module 101 (including multiple corresponding module private keys 112), and module public key identity 111a can be used to select and/or identify the correct module public key 111.

Petitioner Samsung Ex-1038, 0044

Module public key identity 111a could be a string or sequence number uniquely associated with module public key 111. As illustrated in Figure 1a, module public key identity 111a may preferably not be included in the string or number comprising module public key 111, but rather associated with the string or number comprising module public key 111, and in this case the two together (module public key identity 111a and the string or number for module public key 111) may be used to refer to module public key 111 as contemplated herein.

The module public key 111 can optionally be signed by a certificate authority 118 in order to confirm the identity of module 101 and/or the identity of module provider 109. Alternatively, module provider 109 may have its own provider public key 120 and provider private key 121. Module provider 109 may have its provider public key 120 signed by a certificate authority 118 and recorded in a certificate 122 (with an exemplary certificate 122 illustrated in Figure 1h below), and then module provider 109 could sign module public key 111. In this manner, module provider 109 can also function as a certificate authority 118 for module 101. Thus, the validity of module public key 111 could be checked with module provider 109, and the wireless module provider's 109 provider public key 120 could be checked against certificate authority 118. Other configurations for signing public keys and using certificates with public keys are possible as well without departing from the scope of the present invention.

Public keys and private keys as contemplated in the present invention, including module public key 111 and module private key 112 and additional keys described herein, may leverage established standards for Public Key Infrastructure (PKI). Public keys may be formatted according to the X.509 series of standards, such as X.509 v3 certificates, and subsequent or future versions, and these keys may be considered cryptographic keys. The keys can support standards such as the International Organization for Standardization (ISO) ISO/IEC 9594 series of standards (herein incorporated by reference) and the Internet Engineering Task Force (IETF) RFC 5280 titled "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" (herein incorporated by reference), including future updates to these standards.

Module public key 111 and module private key 112, as well as the other private and public keys described within the present invention, could be generated using standard software tools such as Openssl, and other tools to generate public and private keys exist as well. Public and private keys as contemplated herein could be recorded in a file such as a *.pem file (Privacy-enhanced

Petitioner Samsung Ex-1038, 0045

Electronic Mail), a file formatted according to Basic Encoding Rules (BER), Canonical Encoding Rules (CER), or Distinguished Encoding Rules (DER), or as text or binary file. Other formats for public and private keys may be utilized as well, including proprietary formats, without departing from the scope of the present invention. As contemplated herein, a key may also comprise either a public key or a private key. A public key as contemplated herein may also be considered a certificate or a public certificate. A private key as contemplated herein may also be considered a security key or a secret key.

Other configurations besides the one illustrated in Figure 1a are possible as well. Server 105 could reside within wireless network 102 in a data center managed by wireless network 102. Wireless network 102 could also operate as a module provider 109. Although a single module 101 and server 105 are illustrated in Figure 1a, system 100 could comprise a plurality of each of these elements. Module 101 could also record sensor data pertaining to a plurality of monitored units 119. Module 101 could be mobile, such as physically attached to a truck or a pallet, and module 101 could connect to a series of different wireless networks 102 or base stations 103 as module 101 moves geographically. Other configurations are possible as well without departing from the scope of the present invention.

Figure 1b

Figure 1b is a graphical illustration of hardware, firmware, and software components for a module, in accordance with exemplary embodiments. Figure 1b is illustrated to include many components that can be common within a module 101, and module 101 may also operate in a wireless configuration in order to connect with a wireless network 102. Module 101 may consist of multiple components in order to collect sensor data or control an actuator associated with a monitored unit 119. In a wireless configuration, the physical interface 101a of module 101 may support radio-frequency (RF) communications with networks including a wireless network 102 via standards such as GSM, UMTS, mobile WiMax, CDMA, LTE, LTE Advanced, and/or other mobile-network technologies. In a wireless configuration, the physical interface 101a may also provide connectivity to local networks such as 802.11 WLAN, Bluetooth, or Zigbee among other possibilities. In a wireless configuration, module 101 could use a physical interface 101a be

Petitioner Samsung Ex-1038, 0046

connected with both a wireless WAN and wireless LAN simultaneously. In a wired configuration, the physical interface 101a can provide connectivity to a wired network such as through an Ethernet connection or USB connection.

The physical interface 101a can include associated hardware to provide the connections such as radio-frequency (RF) chipsets, a power amplifier, an antenna, cable connectors, etc., and additional exemplary details regarding these components are described below in Figure 1e. Device driver 101g can communicate with the physical interfaces 101a, providing hardware access to higher-level functions on module 101. Device drivers 101g may also be embedded into hardware or combined with the physical interfaces. Module 101 may preferably include an operating system 101h to manage device drivers 101g and hardware resources within module 101. The operating systems described herein can also manage other resources such as memory and may support multiple software programs operating on module 101 or server 105, respectively, at the same time. The operating system 101h can include Internet protocol stacks such as a User Datagram Protocol (UDP) stack, Transmission Control Protocol (TCP) stack, a domain name system (DNS) stack, etc., and the operating system 101h may include timers and schedulers for managing the access of software to hardware resources. The operating system shown of 101h can be appropriate for a low-power device with limited memory and CPU resources (compared to a server 105). An example operating system 101h for module 101 includes Linux, Android® from Google®, Windows® Mobile, or Open AT® from Sierra Wireless®. Additional example operating systems 101h for module 101 include eCos, uC/OS, LiteOs, and Contiki, and other possibilities exist as well without departing from the scope of the present invention.

A module program 101i may be an application programmed in a language such as C, C++, Java, and/or Python, and could provide functionality to support M2M applications such as remote monitoring of sensors and remote activation of actuators. Module program 101i could also be a software routine, subroutine, linked library, or software module, according to one preferred embodiment. As contemplated herein, a module program 101i may be an application operating within a smartphone, such as an iPhone® or Android®-based smartphone, and in this case module 101 could comprise the smartphone. The application functioning as a module program 101i could be downloaded from an "app store" associated with the smartphone. Module program 101i can include data reporting steps 101x, which can provide the functionality or CPU 101b instructions for

Petitioner Samsung Ex-1038, 0047

collecting sensor data, sending messages to server 105, and receiving responses from server 105, as described in the present invention.

Many of the logical steps for operation of module 101 can be performed in software and hardware by various combinations of sensor 101f, actuator 101y, physical interface 101a, device driver 101g, operating system 101h, module program 101i, and data reporting steps 101x. When module 101 is described herein as performing various actions such as acquiring an IP address, connecting to the wireless network, monitoring a port, transmitting a packet, sending a message, receiving a response, or encrypting or signing data, specifying herein that module 101 performs an action can refer to software, hardware, and/or firmware operating within module 101 illustrated in Figure 1b performing the action. Note that module 101 may also optionally include user interface 101j which may include one or more devices for receiving inputs and/or one or more devices for conveying outputs. User interfaces are known in the art and generally are simple for modules such as a few LED lights or LCD display, and thus user interfaces are not described in detail here. User interface 101j could comprise a touch screen if module 101 operates as a smartphone or mobile phone. As illustrated in Figure 1b, module 101 can optionally omit a user interface 101j, since no user input may be required for many M2M applications, although a user interface 101j could be included with module 101.

Module 101 may be a computing device that includes computer components for the purposes of collecting data from a sensor 101f or triggering an action by an actuator 101y. Module 101 may include a central processing unit (CPU) 101b, a random access memory (RAM) 101e, and a system bus 101d that couples various system components including the random access memory 101e to the processing unit 101b. The system bus 101d may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures including a data bus. Note that the computer components illustrated for the module 101 in Figure 1b may be selected in order to minimize power consumption and thereby maximize battery life, if module 101 includes a battery and is not attached to external power. In addition, the computer components illustrated for the module 101 in Figure 1b may also be selected in order to optimize the system for both long periods of sleep relative to active communications and also may be optimized for predominantly uplink (i.e. device to network) communications with small packets or messages. The computer components illustrated for the

Petitioner Samsung Ex-1038, 0048

module 101 in Figure 1b may also be general-purpose computing components, and specialized components are not required in order to utilize many of the embodiments contemplated herein.

Module 101 may include a read-only memory (ROM) 101c which can contain a boot loader program. Although ROM 101c is illustrated as "read-only memory", ROM 101c could comprise long-term memory storage chipsets or physical units that are designed for writing once and reading many times. As contemplated within the present invention, a read-only address could comprise a ROM 101c memory address or another hardware address for read-only operations accessible via bus 101d. Changing data recorded in a ROM 101c can require a technician have physical access to module 101, such as removing a cover or part of an enclosure, where the technician can subsequently connect equipment to a circuit board in module 101, including replacing ROM 101c. ROM 101c could also comprise a nonvolatile memory, such that data is stored within ROM 101c even if no electrical power is provided to ROM 101c. Although not illustrated in Figure 1b, but illustrated in Figure 1e below, module 101 could also include a flash memory 101w. A primary difference between flash memory 101w and RAM 101e may be that reading and writing operations to flash memory 101w can be slower whereas reading and writing operations to RAM 101e may be faster, and faster reading and writing operations to memory may be required for processing sensor 101f signals and securely communicating with a server 105. For example, module program 101i, data reporting steps 101x, operating system 101h, or device driver 101g could be stored in flash memory 101w within module 101 when the module is powered off. These components and/or instructions could be moved from a flash memory 101w (not shown in Figure 1b but shown in Figure 1e) into RAM 101e when the module is powered on. In addition, portions of a RAM 101e can function as flash memory 101w, such that module program 101i, power control steps 101x, operating system 101h, or device driver 101g remain resident in random access memory even when the mobile module 101 is powered off, or powered off for the first time after module 101 is installed or becomes active in wireless network 102. Note that ROM 101c could be optionally omitted or included in a memory unit within CPU 101b (not shown).

Although the exemplary environment described herein employs ROM 101c and RAM 101e, it should be appreciated by those skilled in the art that other types of computer readable media which can store data that is accessible by a module 101, such as memory cards, subscriber identity module (SIM) cards, local miniaturized hard disks, and the like, may also be used in the exemplary operating environment without departing from the scope of the invention. The memory and

Petitioner Samsung Ex-1038, 0049

associated hardware illustrated in Figure 1b provide nonvolatile storage of computer-executable instructions, data structures, program modules, module program 101i, and other data for computer or module 101. Note the module 101 may include a physical data connection at the physical interface 101a such as a miniaturized universal serial bus adapter, firewire, optical, or other another port and the computer executable instructions such as module program 101i, data reporting steps 101x, operating system 101h, or device driver 101g can be initially loaded into memory such as ROM 101c or RAM 101e through the physical interface 101a before module 101 is given to an end user, shipped by a manufacturer to a distribution channel, or installed by a technician. In addition, the computer executable instructions such as module program 101i, data reporting steps 101x, operating system 101h or device driver 101g could be transferred wirelessly to module 101. In either case (wired or wireless transfer of computer executable instructions), the computer executable instructions such as module program 101i, data reporting steps 101x, operating system 101h, or device driver 101g could be stored remotely on a disk drive, solid state drive, or optical disk (external drives not shown).

A number of program modules may be stored in RAM 101e, ROM 101c, or possibly within CPU 101b, including an operating system 101h, device driver 101g, an http client (not shown), a DNS client, and related software. Program modules include routines, sub-routines, programs, objects, components, data structures, etc., which perform particular tasks or implement particular abstract data types. Aspects of the present invention may be implemented in the form of a module program 101i and/or data reporting steps 101x which are executed by the module 101 in order to provide remote monitoring using a sensor 101f and/or remote control using an actuator 101y. In addition, the module program 101i and/or data reporting steps 101x can include routines, sub-routines, and similar components to support secure and bandwidth and radio-frequency (RF) efficient communication with a server 105 utilizing the techniques described in the present invention. Further, the module program 101i and/or data reporting steps 101x can perform the various actions described in the present invention for the module 101 through instructions the module program 101i and/or data reporting steps 101x provide to the CPU 101b.

A user may enter commands and information into module 101 through an optional user interface 101j, such as a keypad, keyboard (possibly miniaturized for a mobile phone form-factor), and a pointing device. Pointing devices may include a trackball, an electronic pen, or a touch screen. A user interface 101j illustrated in Figure 1b can also comprise the description of a user

Petitioner Samsung Ex-1038, 0050

interface 101j within U.S. Patent Application Serial No. 14/039,401, filed September 27, 2013 in the name of John Nix, which is herein incorporated in its entirety.

The module 101, comprising a computer, may operate in a networked environment using logical connections to one or more remote computers, such as the server 105 illustrated in Figure 1a. Server 105 can also function as a general purpose server to provide files, programs, disk storage, remote memory, and other resources to module 101 usually through a networked connection. Additional details regarding server 105 are provided in Figure 1c below. Additional remote computers with which module 101 communicates may include another module 101 or mobile device, an M2M node within a capillary network, a personal computer, other servers, a client, a router, a network PC, a peer device, a base station 103, or other common network node. The server 105 or a remote computer typically includes many of the elements described above relative to the module 101, including a CPU, memory, and physical interfaces. It will be appreciated that the network connections shown throughout the present invention are exemplary and other means of establishing a wireless or wired communications link may be used between mobile devices, computers, servers, corresponding nodes, and similar computers.

The module program 101i and data reporting steps 101x operating within module 101 illustrated in Figure 1b can provide computer executable instructions to hardware such as CPU 101b through a system bus 101d in order for a module 101 to (i) collect data from a sensor, (ii) change the state of an actuator 101y, and (iii) send or receive packets with a server 105, thus allowing server 105 to remotely monitor or control a monitored unit 119. The module program 101i and/or data reporting steps 101x can enable the module 101 to transmit or send data from sensor 101f or module 101 by recording data in memory such as RAM 101e, where the data can include sensor data, a destination IP:port number, a packet or packet header value, an encryption or ciphering algorithm and key, a digital signature algorithm and key, etc. The data recorded in RAM 101e can be subsequently read by the operating system 101h or the device driver 101g. The operating system 101h or the device driver 101g can write the data to a physical interface 101a using a system bus 101d in order to use a physical interface 101a to send data to a server 105 using the Internet 107. Alternatively, the module program 101i and/or data reporting steps 101x can write the data directly to the physical interface 101a using the system bus 101d.

Petitioner Samsung Ex-1038, 0051

The module program 101i and/or data reporting steps 101x, or operating system 101h can include steps to process the data recorded in memory such as encrypting data, selecting a destination address, or encoding sensor data acquired by (i) a sensor 101f or (ii) through a physical interface 101a such as a thermocouple, shock or vibration sensor, light sensor, or global positioning system (GPS) receiver, etc. The module 101 can use the physical interface 101a such as a radio to transmit or send the data from a sensor to a base station 103. For those skilled in the art, other steps are possible as well for a module program 101i or operating system 101h to collect data from a sensor 101f and send the data in a packet without departing from the scope of the present invention.

Conversely, in order for module 101 to receive a packet or response from server 105, the physical interface 101a can use a radio to receive data from a base station 103. The received data can include information from a server 105 and may comprise a datagram, a source IP:port number, a packet or header value, an instruction for module 101, an acknowledgement to a packet that module 101 sent, a digital signature, and/or encrypted data. The operating system 101h or device driver 101g can use a system bus 101d and CPU 101b to record the received data in memory such as RAM 101e, and the module program 101i or operating system 101h may access the memory in order to process the received data and determine the next step for the module 101 after receiving the data. Processing the received data could include deciphering or decrypting received data with a key, verifying a digital signature with a key, reading an instruction from a server 105, or similar transformations of the received data. The steps within this paragraph may also describe the steps a module program 101i or data reporting steps 101x can perform in order to receive a packet. For those skilled in the art, other steps are possible as well for a module program 101i, data reporting steps 101x, or module 101 to receive a packet or response from a server 105 without departing from the scope of the present invention.

Moreover, those skilled in the art will appreciate that the present invention may be implemented in other computer system configurations, including hand-held devices, netbooks, portable computers, multiprocessor systems, microprocessor based or programmable consumer electronics, network personal computers, minicomputers, mainframe computers, and the like. The invention may also be practiced in distributed computing environments, where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices. In addition, the terms “mobile node”, “mobile station”, “mobile device”, “M2M module”,

Petitioner Samsung Ex-1038, 0052

"M2M device", "networked sensor", or "industrial controller" can be used to refer to module 101 or its functional capabilities of (i) collecting sensor data regarding a monitored unit 119, (ii) changing state of an actuator 101y associated with monitored unit 119, and/or (iii) communicating the data associated with a monitored unit 119 with a wireless network 102. The function of module 101 and sensor 101f could be integrated, and in this case module 101 could also be referred to as a "sensor", "intelligent sensor", or "networked sensor". Further, the term "module" or "monitoring device" can be used to refer to the module program 101i when module program 101i provides functional capabilities such as reporting data from a sensor 101f to a server 105 or receiving instructions for an actuator 101y from a server 105. The device driver 101i, operating system 101i, and/or module program 101i could optionally be combined into an integrated system for providing the module 101 functionality. Other possibilities exist as well for the configuration or combination of components illustrated in Figure 1b without departing from the scope of the present invention.

Figure 1c

Figure 1c is a graphical illustration of hardware, firmware, and software components for a server, in accordance with exemplary embodiments. The illustrated components for the server 105 in Figure 1c include a central processing unit (CPU) 105b, a random access memory (RAM) 105e, a system bus 105d, storage 105m, an operating system 105h, and a module controller 105x. These elements can provide functions equivalent to the central processing unit (CPU) 101b, RAM 101e, system bus 101d, flash memory 101w, and an operating system 101h described above in Figure 1b, respectively. In general, a server 105 can have higher-end components such as a larger CPU 105b and greater RAM 105e in order to support communications with a plurality of modules 101. Server 105 can comprise a general purpose computer such as a rack mounted server within a data center or rack, or could also comprise a desktop computer or laptop. Server 105 could also be a specialized computer, with hardware and software selected for supporting a plurality of modules 101 connecting and communicating simultaneously. Operating system 101h can comprise an operating system appropriate for a server such as Linux, Solaris®, or Windows® Server. Server 105 can preferably have a wired Ethernet connection with high bandwidth that is persistently connected to the Internet 107 illustrated in Figure 1a, while the Internet 107 connection for module 101 may be transient as module 101 changes between sleep and active states. Module controller 105x can

Petitioner Samsung Ex-1038, 0053

provide the server-side logic for managing communications and controlling module 101 using a module database 105k. Server program 105i can provide functionality for communicating with external servers or nodes, such as an application server 171 illustrated in Figure 1d.

A module controller 101x and server program 105i may be applications programmed in a language such as C, C++, Java, or Python and could provide functionality to support M2M applications such as remote monitoring of sensors and remote activation of actuators. Module controller 105x and server program 105i could also be software routines, subroutines, linked libraries, or software modules, according to preferred embodiments. Many of the logical steps for operation of server 105, module controller 105x, and/or server program 105i can be performed in software and hardware by various combinations of physical interface 105a, system bus 105d, device driver 105g, and operating system 105h. When server 105 is described herein as performing various actions such as acquiring an IP address, monitoring a port, transmitting or sending a packet, receiving a message, or encrypting or signing a message, specifying herein that server 105 performs an action can refer to software, hardware, and/or firmware operating within server 105 performing the action.

The server 105 may also include a user interface 105j such as a display (not shown) which could also comprise any type of display devices such as a liquid crystal display (LCD), a plasma display, and an organic light-emitting diode (OLED) display, or a cathode ray tube (CRT). A user interface 105j for the server 105 may optionally be provided remotely such as (i) via a web browser or a secure terminal such as secure shell (SSH) with (ii) another computer operated by an administrator (not shown). A user or administrator may enter commands and information into server 105 through a user interface 105j, such as a keypad, keyboard, and a pointing device. Pointing devices may include a trackball, an electronic pen, or a touch screen. In addition, the server 105 may store computer executable instructions such as module controller 105x or server program 105i on storage 105m. Storage 105m may comprise a disk drive, a solid-state drive, an optical drive, or a disk array. Module controller 101x can manage communications with module 101 and may be downloaded and installed on the server 105. As noted previously and elsewhere herein, module program 101i and module controller 105x can preferably interoperate with each other in order to collect sensor data and control an actuator associated with a monitored unit 119.

Petitioner Samsung Ex-1038, 0054

The server program 105i and/or module controller 101x operating within server 105 illustrated in Figure 1c can provide computer executable instructions to hardware such as CPU 105b through a system bus 105d in order to (i) receive a message from the module 101 and (ii) send a response, wherein the message can include sensor 101f data and the response can include an acknowledgement of the message and/or an instruction to the module 101. The module controller 105x can enable the server 105 to send a response to a message from module 101 by recording data associated with module 101 in memory such as RAM 105e, where the data can include an instruction from module 101, a destination IP:port number, a packet or packet header value, and the data can be processed using an encryption or ciphering algorithm or key, a digital signature algorithm or key, etc.

The server program 105i can enable (a) the server 105 to send a datagram, packet, or an application message to an application server 171 by (b) recording data associated (i) a with module 101 or (ii) other M2M service control information in memory such as RAM 105e, where the data can include information from module 101, a destination IP:port number, a packet or packet header value, and the information could be processed using an encryption or ciphering algorithm or key, a digital signature algorithm or key, etc. The operating system 105h or the device driver 105g can write the data from RAM 105e to a physical interface 105a using a system bus 105d and an Ethernet connection in order to send the data via the Internet 107 illustrated in Figure 1a. Alternatively, the software program 105i and/or module controller 105x can write the data directly to the physical interface 105a using the system bus 105d.

The server 105 can utilize the physical interface 105a to receive data from a module 101 and/or application 171i using a local area network such as Ethernet, although the physical interface 105a of server 105 could also utilize a wireless connection. The server 105 can listen for data from the Internet 107 using port number and/or a TCP/UDP socket. The received data from a module 101 can be a message formatted according to an Internet packet or datagram or series of datagrams inside Ethernet packets and include information from a module 101 such as a source IP address and port number, an identity of the module, sensor data that may be encrypted, and/or a digital signature of the module. The received data from application 171i can comprise a series of datagrams formatted according to Internet Protocol and/or datagrams inside Ethernet packets. The received data or message from application 171i can include information regarding application 171i and/or server 105, such as a source IP address and port number associated with application 171i or

Petitioner Samsung Ex-1038, 0055

application server 171, an identity of the server, actuator instructions or commands for a module 101 that may be encrypted, and a digital signature associated with the application 171i.

When server 105 receives messages or data, the operating system 105h or device driver 105g can record the received data from module 101 or application 171i via physical interface 105a into memory such as RAM 105e. The server program 105i or operating system 105h may subsequently access the memory in order to process the data received. The server program 105i and/or module controller 105x, or operating system 105h can include steps to process the data recorded in memory and received from the module 101 or application 171i, such as parsing the received packet, decrypting data, verifying a digital signature with a key, or decoding sensor data included in a message from the module.

The server 105 and/or server program 105i may communicate with application 171i by sending and receiving packets over a LAN or the Internet 107, using a physical interface 105a and a wired connection such as Ethernet or possibly a wireless connection as well. The server 105 can use the physical interface 105a such as an Ethernet connection to send and receive the data from the Internet 107. For those skilled in the art, other steps are possible as well for a server program 105i or operating system 105h within a server 105 to (i) send/receive a packet or message to/from a module 101 and (ii) send/receive a packet or message to/from an application 171i without departing from the scope of the present invention. Server program 105i and module controller 105x may optionally be combined within a server 105, or alternatively distributed across different physical computers and function in a coordinated manner using a network.

The device drivers 105g, operating systems 105h, and/or module controller 105x could also optionally be combined into an integrated system for providing the server 105 functionality. Although a single physical interface 105a, device-driver set 105g, operating system 105h, module controller 105x, server program 105i, and user interface 105j are illustrated in Figure 1c for server 105, server 105 may contain multiple physical interfaces, device drivers, operating systems, software programs, module programs, and/or user interfaces. Server 105 may operate in a distributed environment, such that multiple computers operate in conjunction through a network to provide the functionality of server 105. Also, server 105 may operate in a "virtualized" environment, where server 105 shares physical resources such as a physical CPU 105b with other

Petitioner Samsung Ex-1038, 0056

processes operating on the same computer. And other arrangements could be used as well, without departing from the invention.

Figure 1d

Figure 1d is a graphical illustration of hardware, firmware, and software components for an application server, in accordance with exemplary embodiments. Application server 171 can include application 171i. Application 171i can comprise a computer program or collection of computer programs, for managing a plurality of modules 101 using one or more servers 105. Application 171i can include a web portal 171j, service controller 171x, an application database 171k, and cryptographic algorithms 141. During operation, such as when application 171i processes data from/to modules 101 through server 105, application 171i may reside in RAM 171e within an application server 171. Application 171i and the associated computer programs may be recorded in storage 171m so that they may be loaded by operating system 171h upon the startup of application server 171. Web portal 171j can comprise a web server such as Apache and can provide a user interface for a remote user accessing application 171i via an Internet 107. The web portal 171j could include web pages for viewing reports from modules 101 and/or servers 105, and also inputting settings for modules 101 by a user. The web pages could include PHP, active server pages, or Java components, in addition to other elements. Data input and stored by application 171i can be recorded in application database 171k. The data could be inserted or queried using structured query language (SQL) statements. Cryptographic algorithms 141 which may comprise a suite of algorithms or subroutines that can be utilized for (i) deriving a pair of keys comprising a public key and a private key, (ii) encrypting data using public keys, (iii) decrypting data using private keys, (iv) processing secure hash signatures using private keys, and (v) verifying secure hash signatures using public keys, and related software, firmware, or subroutines for implementing a cryptographic system, and cryptographic algorithms 141 are also depicted and described in connection with Figure 1g below.

Application 171i may be processed by an application server 171 using a CPU 171b. The illustrated components for the application server 171 in Figure 1d include a central processing unit

Petitioner Samsung Ex-1038, 0057

(CPU) 171b, a random access memory (RAM) 171e, a system bus 171d, storage 171m, an operating system 171h, and an application 171i. These elements can provide functions equivalent to the central processing unit (CPU) 105b, RAM 105e, system bus 105d, storage 105m, and an operating system 105h described above in Figure 1c, respectively. Application server 171 can comprise a general purpose computer such as a rack mounted server within a data center or rack, or could also comprise a desktop computer or laptop. Application server 171 could also be a specialized computer, with hardware and software selected for supporting a plurality of servers 105 or modules 101 connecting and communicating simultaneously. Operating system 171h can comprise an operating system appropriate for a server such as Linux, Solaris®, or Windows® Server. Application server 171 can preferably have a wired Ethernet connection with high bandwidth that is persistently connected to the Internet 107.

An application 171i and/or service controller 171x may be an application programmed in a language such as C, C++, Java, or Python and could provide functionality to support M2M applications such as remote monitoring of sensors and remote activation of actuators. Application 171i can include a service controller 171x. Application 171i and/or service controller 171x could also be a software routine, subroutine, linked library, or software module, according to one preferred embodiment. Application 171i can include a service controller 171x, which can provide the functionality or CPU 171b instructions for the service controller 171x described in the present invention. Service controller 171x can include (i) logic for processing alarms from a module 101 (such as sending out and email or text message to a user), (ii) logic for adjusting actuator 101y settings based upon data from sensor 101f, (iii) accepting user input (possibly via web portal 171j) and then making an associated change in an actuator 101y setting. Service controller 171x can also accept input from external applications (not shown) in order to make decisions regarding module 101, sensor 101f, and/or actuator 101y.

Service controller 171x could be included within an enterprise resource planning (ERP) solution such as SAP® or Oracle® ERP. An external application (not shown) can communicate with the application server 171. As one example, a group of modules 101 could be installed within a manufacturing plant, and when a customer order was entered into the external application such as ERP, the service controller 171x could provide instructions for a group of modules 101 to server 105, such as changing actuators 101y to operate a production line. Other possibilities for service controller 171x exist as well without departing from the scope of the present invention. In general,

Petitioner Samsung Ex-1038, 0058

service controller 171x can manage the overall function of a group of modules 101 through server 105. Service controller 171x may operate at the "user layer" and/or "application layer" of the traditional OSI model.

Many of the logical steps for operation of application server 171 or application 171i can be performed in software by various combinations of physical interface 171a, device driver 171g, operating system 171h, and module controller 105i, where application 171i communicates with module controller 105i over a network. Application 171i and module controller 105i can communicate using an application message 701 (illustrated in Figure 7 below). When application 171i is described herein as performing various actions such as acquiring an IP address, monitoring a port, transmitting or sending a packet or message, or encrypting or signing a message, receiving a packet or message, specifying herein that application 171i and/or application server 171 performs an action can refer to software, hardware, and/or firmware operating within application server 171 performing the action. Application server 171 or application 171i can send or transmit a message, packet, or data using the steps depicted and described in connection with Figure 1c for a server 105 to send or transmit a message, packet, or data. Application server 171 or application 171i can receive a message, packet, or data using the steps depicted and described in connection with Figure 1c for a server 105 to receive a message, packet, or data. Application server 171 can utilize hardware components similar to server 105, such as storage 171m can be similar to storage 105m, CPU 171b can be similar to CPU 105b, and physical interface 171a can be similar to physical interface 105a. Application server 171 can use a system bus 171d to connect the hardware components shown within application server 171, and system bus 171d can be similar to system bus 105d depicted and described in connection with Figure 1c above.

Application server 171 may also comprise a collection of individual computers, where the individual computers could be either centrally located or geographically dispersed, but the individual computers may function in a coordinated manner over a network to operate as an application server 171. In a similar manner, application 171i may be distributed across a plurality of computers, such as in a cloud computing configuration. Application server 171 may be a "virtualized" server, with computing resources shared with other processes operating on a computer.

Petitioner Samsung Ex-1038, 0059

Figure 1e

Figure 1e is a graphical illustration of the components within a module, in accordance with exemplary embodiments. Figure 1e is illustrated to show a combination of components useful for leveraging the efficient and secure communication techniques described in the present invention. In addition to the components illustrated in Figure 1b above, module 101 can include a battery 101k, a server public key 114, a wireless module private key 112, a connection to an actuator 101y, a USB interface 101v, a CPU wake controller 101u, a flash memory 101w, a symmetric key 127, a pre-shared secret key 129a, a random number generator 128, cryptographic algorithms 141, a radio 101z, and other components illustrated in Figure 1e. Not all of the components illustrated in Figure 1e are required for many exemplary embodiments, and some of the components illustrated in Figure 1e may also be optionally omitted in exemplary embodiments.

The CPU 101b can comprise a general purpose processor appropriate for the low power consumption requirements of a module 101, and may also function as a microcontroller. In a preferred exemplary embodiment, the CPU 101b is responsible for maintaining a state machine for network and transport layer commands with an external network such as the wireless network 102 illustrated in Figure 1a, where CPU 101b can manage the overall connection of radio 101z with a wireless network 102. CPU 101b can include additional elements not shown, such as registers, cache memory, an arithmetic logic unit (ALU), which performs arithmetic and logical operations, and a control unit (CU), which extracts instructions from memory and decodes and executes them, calling on the ALU when necessary.

The CPU 101b wake and dormant or sleep states may be controlled by a CPU wake controller 101u to put the module 101 in a dormant state in order to conserve (i) battery life in battery 101k, or (ii) power consumption if land-line power is available, when sensor measurements, actuator control, or radio communications are not needed. The CPU wake controller 101u could optionally be integrated into CPU 101b. The CPU wake controller 101u can also include a timer to periodically wake the CPU 101b in order to perform sensor measurements or communicate with a wireless network 102 or server 105. The flash memory 101w can be a non-volatile memory and may contain a bootloader program 125 and a module program 101i. Bootloader program 125 can comprise a software program or application that is initially read by CPU 101b upon power up of

Petitioner Samsung Ex-1038, 0060

module 101 in order to configure interfaces and begin operations including loading module program 101i. Module program 101i is depicted and described in connection with Figure 1b above. If module 101 operates as a payment card, then CPU wake controller 101u could wake CPU 101b when a radio 101z detects an RF signal from a payment terminal.

Note that CPU wake controller 101u can monitor sensor 101f in order to determine a wake condition for CPU 101b, wherein the CPU 101b remains dormant until sensor 101f reads a state that requires sending a message to a server 105. An example could be sensor 101f comprising a shock and vibration detector or a temperature measuring device such as a thermocouple, and other examples exist as well. The CPU wake controller 101u can leave CPU 101b in a dormant state until a certain threshold of shock and vibration or temperature is recorded by the sensor 101f, and in this manner battery 101k can be conserved so that CPU 101b wakes when a threshold sensor measurement or an alarm condition is reported. The exemplary certain threshold of shock and vibration or temperature recorded by the sensor 101f can also comprise an alarm condition. When CPU 101b is dormant, CPU wake controller 101u can monitor a voltage level output by sensor 101f, and once a threshold voltage level is read by CPU wake controller 101u, CPU wake controller 101u can change CPU 101b from the dormant state to an active state in order to run a module program 101i.

Even without an alarm condition, CPU wake controller 101u can periodically wake CPU 101b to collect sensor data, connect to an external network such as a wireless network 102, and send sensor data to server 105. CPU 101b can include one or more cores of the processor, where each core is an independent actual central processing unit, and the cores can be the units that read and execute program instructions. The instructions can be ordinary CPU instructions such as add, move data, and branch. The dormant state of CPU 101b can comprise a sleep state where a power level used by a core in the processor is less than 0.010 milliwatts during a one second measurement sample, such as when the power supply is essentially removed from the core but power is supplied to memory 101e in order to allow a rapid waking of the CPU 101b or core.

Sensor 101f could be a device to collect environmental data or data regarding a monitored unit 119. Sensor 101f could collect data such as temperature, humidity, pressure, visible light levels, radiation, shock and/or vibration, voltage, current, weight, pH levels, orientation/motion, or the presence of specific chemicals. Sensor 101f could also be a microphone. Sensor 101f could be

Petitioner Samsung Ex-1038, 0061

a magnetic strip reader for credit cards and similar cards, or an antenna for either near-field RF communications, such as reading an RF identity tag. An antenna for a sensor 101f could also collect longer-range RF signals, such as reading long-range radio frequency identity tags. Sensor 101f could also collect biometric data such as heart rate, glucose levels, body temperature, or other health measurements and in this case monitored unit 119 could be a person. The sensor 101f can provide data to the CPU 101b in the form of analog or digital data, which can be communicated via a system bus 101d or physical interface 101a and other electrical interfaces are possible as well. A sensor measurement can comprise the analog or digital data collected by CPU 101b from sensor 101f. A sensor measurement can include processing of the analog or digital data input CPU 101b by sensor 101f, such as averaging over time, using mathematic formulas to convert the raw data from sensor 101f into a usable form. Module 101 may also collect sensor data or sensor values using a sensor 101f and CPU 101b, where the data or values are derived from electrical signals output by a sensor 101f. A sensor measurement can comprise the sensor data or sensor values. If module 101 comprises a "point of presence" payment terminal, then a sensor measurement could comprise data read from a payment card.

As contemplated herein, the terms "sensor measurement" and "sensor data" can be used interchangeably, and can also be considered functionally equivalent. Although a single sensor 101f is shown in Figure 1e, a module 101 could include multiple sensors. Each of the multiple sensors 101f could include a sensor identity 151, which could comprise a number or string to identify the sensor 101f. Or, a sensor identity 151 could also be used with a single sensor 101f. In addition, although sensor 101f is shown as integrated into module 101, sensor 101f could be external to module 101, and connected via an external interface such as through a USB interface 101v or other wired or wireless configuration.

Note that sensor 101f could also connect to module 101 via a WiFi or similar wireless LAN connection such as Zigbee. Radio 101z within module 101 can operate as a WiFi base station (in addition to radio 101z connecting to a wireless network 102), and sensor 101f could contain its own radio and WiFi chipset, such that sensor 101f could send sensor data to module 101 via the WiFi connection (or other wireless LAN connection). In this manner, by utilizing WiFi to connect with sensor 101f, module 101 could connect with a plurality of sensors 101f located in a vicinity of module 101, such as within an exemplary 50 meters. In addition to the WiFi network described, sensor 101f and/or actuator 101y could connect with module 101 via any suitable wireless local area

Petitioner Samsung Ex-1038, 0062

networking technology including, IEEE 802.11, IEEE 802.15.4, an ISA100.11a standards-based network, Bluetooth, and/or a 6LoWPAN.

Actuator 101y could be a device to control a parameter or state for a monitored unit 119, such as changing a voltage or current, activating a switch or relay, turning on or off a microphone or speaker, activating or deactivating a light, and other examples are well known in the art. Actuator 101y could also be a speaker. Actuator 101y could be controlled by module 101 via a digital or analog output from CPU 101b, which could also be transmitted or sent via system bus 101d or a physical interface 101a. Although actuator 101y is illustrated as external to wireless module 101 in Figure 1e, actuator 101y could also be internal to module 101, and module 101 could include multiple actuators 101y.

Although a single actuator 101y is shown in Figure 1e, a module 101 could include multiple actuators 101y. Each of the multiple actuators 101y could include an actuator identity 152, which could comprise a number or string to identify the actuator 101y. Or, an actuator identity 152 could also be used with a single actuator 101y. If module 101 comprises a "point of presence" payment terminal, then an actuator 101y could be a printer for printing a receipt. If module101 comprises a payment card for end users to make payments to merchants, then actuator 101y could be an LED light that turns on upon submission of a payment. Sensors and actuators are well known to those of ordinary skill in the art, and thus are not described in additional detail herein.

Module 101 can include a Universal Serial Bus (USB) interface 101v, which could provide a general and standards-based interface for external connection to a wide variety of sensors 101f, actuators 101y, and external computers such as laptops or mobile phones. Module 101 could also obtain power or recharge a battery 101k through the USB interface 101v. Software programs or instructions to wireless module 101 could be provided locally through USB interface 101v, including the initial loading of a pre-shared secret key 129a and/or shared secret key 510 described in Figure 5b below. Module program 101i, operating system 101h, or module private key 112 could be loaded into module 101 via USB interface 101v, another physical interface 101a, or radio 101z. In order to support a preferred small form factor of a module 101, the USB interface 101v could preferably utilize either a micro-USB or mini-USB physical interface, or future similar miniature USB interfaces related to these standard interfaces. Although a USB interface 101v is illustrated in Figure 1e, alternative interfaces for external communication could be provided, such as a Joint Test

Petitioner Samsung Ex-1038, 0063

Action Group (JTAG) connection, optical, or a proprietary interface such as a "Lightning" connection from Apple, Inc. USB interface 101v and similar hardware interfaces could also be optionally omitted. According to an exemplary embodiment, module 101 uses only a radio 101z to transmit and receive data externally to module 101.

In accordance with an exemplary embodiment, module 101 can comprise a wireless module and include a radio 101z. Note that the use of a radio 101z is not required for module 101, which could also obtain a connection to the Internet 107 via a wired line such as Ethernet. Although not illustrated, radio 101z could include antennas for reception and transmission of RF signals, and even multiple antennas could be used. Although a single radio 101z is illustrated in module 101, module 101 could also contain multiple radios 101z, such that a first radio 101z connects with a WiFi network or functions as a WiFi base station or WiFi client, a second radio 101z connects with a PLMN mobile network such as a wireless network 102, and a third radio 101z connects with a wireless network 102 operating in white-space spectrum, etc. Or, a single radio 101z could be utilized to connect with multiple wireless networks 102 operating in different frequencies with different RF modulation techniques and/or different RF standards.

Radio 101z could also comprise a software defined radio, such that radio 101z could be programmed to change RF protocols and modulation schemes without having to change hardware within a radio 101z. Thus, according to a preferred exemplary embodiment, module 101 can utilize a software defined radio for radio 101z in order allow module 101 to communicate with different wireless networks 102, including new or future standards for a wireless network 102, where the standard was not defined when module 101 was installed. In this manner, module 101 can continue to operate over an extended period such as years by upgrading the software defined radio in a radio 101z as standards used by a wireless network 102 changes, thereby reducing costs for changing a module 101 or a radio 101z within a module in a system 100.

Radio 101z can support wireless LAN standards such as WiFi, Bluetooth, and Zigbee, or similar wireless LAN standards. Radio 101z, if present in a module 101, could also support communication through "white space" spectrum white space spectrum recently approved for use by the Federal Communications Commission (FCC), and in this case radio 101z in module 101 could operate as a Mode I or Mode II device according to FCC Memorandum Opinion and Order (FC-12-36) and related white space regulation documents. Radio 101z illustrated in Figure 1e can comprise

Petitioner Samsung Ex-1038, 0064

a radio 101z depicted and described in connection with Figure 1d of U.S. Patent Application Serial No. 14/039,401, filed September 27, 2013 in the name of John Nix, the contents of which are herein incorporated in their entirety. .

Note that module 101 may also operate as a base station in a wireless LAN, such as an 802.11 base station. When module 101 operates a wireless LAN, radio 101z can function as either a client/node or a base station 103 to support communication from other wireless nodes in physical proximity, such as other nodes within an exemplary 50 meters. The other wireless nodes could comprise a sensor 101f and/or actuator 101y, and in this case a sensor could be referred to as a "networked sensor" and an actuator could be referred to as a "networked actuator". When radio 101z functions as a base station 103, module 101 can operate as a gateway, providing Internet access to these other nodes or modules 101 within the wireless LAN. Radio 101z can simultaneously function (i) as a base station in a wireless LAN, such as WiFi, and (ii) a client/subscriber on a wireless WAN such as a PLMN. Radio 101z can be selected to support multiple different wireless LAN technologies in addition to WiFi, such as the IEEE 802.15.4 standard or Bluetooth. If radio 101z supports IEEE 802.15.4, then wireless network 102 could be a Zigbee network, an ISA100.11a standards-based network, or a 6LoWPAN network as described by IETF RFC 4944.

In accordance with exemplary embodiments, module 101 can store module private key 112, server public key 114, and module identity 110, and a symmetric key 127 in memory/RAM 101e during operation, such as when CPU 101b is active and the module 101 is connected to a network such as a wireless network 102 during data transmissions. Module private key 112 preferably is recorded in nonvolatile memory such as flash memory 101w, so that module 101 has access to its private key 112 after the private key has been derived or loaded, including times when a battery 101k has been fully drained or removed from module 101 (if module 101 does not utilize a persistent power source such as land-line power). Module private key 112 and module identity 110 could be written into ROM 101c upon manufacture or distribution of module 101, although module 101 can also derive module private key 112 in accordance with exemplary embodiments and store the module private key 112 in a flash memory 101w.

The CPU 101b preferably moves module private key 112 and module identity 110 from nonvolatile memory into volatile memory, including possibly a cache memory within CPU 101b,

Petitioner Samsung Ex-1038, 0065

before sending data through an Internet 107 illustrated in Figure 1a, in order to speed computations. As a minimum, module private key 112 and module identity 110 will need to be loaded into registers of CPU 101b during computations or use of cryptographic algorithms 141 that require module private key 112 and/or module identity 110, and this move of the data into registers of CPU 101b constitutes a move or copy of module private key 112 and module identity 110 into volatile memory.

Symmetric key 127 can be a secure, shared private key for use with symmetric encryption or symmetric ciphering algorithms 141b (in Figure 1g below). Symmetric key 127 can be derived by using module public key 111 and/or server public key 114, possibly through the use of a key derivation function 141f (also in Figure 1g below). Symmetric key 127 can be used for both encryption and decryption with symmetric cryptographic algorithms 141b described in Figure 1g below, where a shared secret key can be used to both encrypt/cipher and decrypt/decipher. Symmetric key 127 may also include an expiration time 133, such that symmetric key 127 may only be used by module 101 during a limited period of time, such symmetric key 127 remaining only valid for a day, or a week, or during a session (where the session comprises multiple messages and/or responses between a module 101 and a server 105), etc. Module 101 can also derive symmetric key 127 according the Elliptic Curve Integrated Encryption Scheme (ECIES) and/or ECDH 159, discussed in Figure 1g below, using module public key 111, server public key 114, and a random number from random number generator 128. ECIES could be included in cryptographic algorithms 141. A summary of ECIES shared key derivation is described the Wikipedia article "Integrated Encryption Scheme" from September 18, 2013 (herein incorporated by reference). Other possibilities for shared key derivation function using public keys are possible as well, including a Diffie–Hellman key exchange. Using a derived symmetric key from the exemplary key derivation function ECIES, module 101 could derive a second symmetric key 127 after the expiration time 133 of the first symmetric key 127 had transpired.

Note that a key derivation function using public keys is not required to generate a shared symmetric key 127, and alternatively a shared symmetric key 127 could be generated by any of module 101, server 105, module provider 109, or M2M service provider 108. If module 101 generates shared symmetric key 127 for symmetric ciphering 141b within a cryptographic algorithms 141, then module 101 can send shared symmetric key 127 to server 105 using an asymmetric ciphering depicted and described in connection with Figure 4 below. In this case,

Petitioner Samsung Ex-1038, 0066

module 101 preferably uses a random number generator 128 to generate a random number 128a (illustrated in Figure 1g) for input into cryptographic algorithms 141, and the seed 129 in random number generator 128 could utilize data from a sensor 101f in order to generate a random number 128a with high entropy in the creation of symmetric key 127. In exemplary embodiments, random number 128a can also comprise a string output of random number generator 128, and thus random number 128a may be recorded in a format other than a number. Thus, the output of a random number generator 128 can comprise a string in addition to numbers, or the output of random number generator 128 could be a binary number or a series of binary numbers that could be encoded into a string. If server 105 or M2M service provider 108 generates the symmetric key 127, server 105 can send module 101 the symmetric key 127 securely using asymmetric ciphering 141a depicted and described in connection with Figure 5a and Figure 1g below.

Module identity 110 is preferably a unique identifier of module 101, and could comprise a number or string such as a serial number, an international mobile subscriber identity number (IMSI), international mobile equipment identity (IMEI), or an Ethernet media access control (MAC) address. According to an exemplary embodiment, module identity 110 can also comprise a serial number or string that is written into hardware of module 101 upon manufacturing or distribution of module 101. In this case, module identity 110 could be recorded in a read only memory 101c, where read only memory 101c could not be easily erased or otherwise tampered with. Or, module 101 could read module identity 110, which could be written into hardware by a manufacturer, distributor, or module provider 109, by using a device driver 101g that reads a hardware address containing the module identity 110 using the bus 101d. Module 101 can read the module identity 110 by accessing a read-only address using the bus 101d. In either case, module identity 110 may preferably be permanently or persistently associated with the physical hardware of module 101, which can be helpful for the security procedures contemplated herein. Module identity 110 can function as a basic identifier for services from M2M service provider 108, server 105, and/or application 171i in order to properly identify module 101 among a plurality of modules. Module private key 112 and module public key 111 could be unique to module 101 and uniquely associated with module identity 110, according to a preferred embodiment.

As contemplated herein, a module identity 110 can also have more than one use. A first module identity 110 could comprise a serial number for the physical hardware of module 101, as described in the paragraph above. A second module identity 110 could also comprise a session

Petitioner Samsung Ex-1038, 0067

identifier, for data sessions between module 101 and server 105, where the session identifier can be uniquely associated by a server 105 to module 101. In the case where module identity 110 has more than one use, format, or representation, the module identity 110 associated with or written into hardware of module 101 (and potentially read from a read-only address in module 101) would preferably comprise the module identity 110 used in a certificate 122. Since a module 101 may utilize multiple module public keys 111 and module private keys 112 over its lifetime, a certificate 122 for module 101 can preferably include both (i) the module identity 110 (such as a serial number for the physical hardware of module 101) and (ii) a module public key identity 111a in order to specify the particular module public key 111 associated with certificate 122. The use of a module public key identity 111a in a certificate 122 is also described in Figure 1h below. Since a module 101 may also have multiple public keys 111 for different purposes (such as one for creating digital signatures, another for asymmetric ciphering, another for use with a second wireless network 102, etc.), then module 101 may also potentially have multiple valid certificates 122 concurrently.

Further, as contemplated herein, a module identity 110 could also comprise more than one physical string or number, such as a first string when module 101 connects with a first M2M service provider 108 or first wireless network 102, and module identity 110 could comprise a second string when module 101 connects with a second M2M service provider 108 or second wireless network 102. The first M2M service provider 108 or first wireless network 102 may have a first requirement or specification for the format, length, structure, etc. of module identity 110, and the second M2M service provider 108 or second wireless network 102 may have a second requirement or specification for the format, length, structure, etc. of module identity 110.

Server public key 114 in module 101 could be obtained from downloading the key over the Internet 107, or optionally also written into nonvolatile memory of module 101 upon manufacture or distribution. Server public key 114 could be obtained using a domain name or Internet address that is recorded in nonvolatile memory upon the configuration of module 101, such as during installation or distribution, and module 101 could fetch the server public key 114 upon connecting to a wireless network 102 or other connection to the Internet 107. Server public key 114 can be the public key associated with server 105 or M2M service provider 108. Although a single server public key 114 is illustrated in Figure 1e, module 101 could record a plurality of server public keys 114, where each server public key 114 is associated with a different server 105. Server public key 114 can optionally be signed by a certificate authority 118 in Figure 1a, such that when module 101

Petitioner Samsung Ex-1038, 0068

communicates with server 105, module 101 can verify a signature 123 (shown in Figure 1h) within a certificate 122 associated with server 105. Successful verification of the signature 123 can provide a high level of certainty that server 105 is properly identified and belongs to M2M service provider 108, as opposed to being an imposter or part of a "man in the middle" attack.

Module 101 may also contain cryptographic algorithms 141, which may comprise a suite of algorithms or subroutines that can be utilized for (i) deriving a pair of keys comprising a public key and a private key, (ii) encrypting data using public keys, (iii) decrypting data using private keys, (iv) processing secure hash signatures using private keys, and (v) verifying secure hash signatures using public keys, and related software, firmware, or subroutines for implementing a cryptographic system, including symmetric ciphering algorithms. Cryptographic algorithms 141 (also described below in Figure 1g) could utilize publicly available software libraries within tools such as OpenSSL maintained by The OpenSSL Project (http://www.openssl.org/), libgcrypt maintained by The Free Software Foundation (http://www.gnu.org/software/libgcrypt/), and similar libraries such as libmcrypt and Crypto++. Note that cryptographic algorithms 141 could also use proprietary cryptographic libraries as well. In addition to implementing asymmetric encryption/ciphering, such as used with RSA and ECC cryptography, cryptographic algorithms 141 can provide symmetric ciphering where a shared private key is utilized to both encrypt and decrypt, such as with the Advanced Encryption Standard (AES) cipher suite.

As illustrated in Figure 1e, module 101 may also contain a random number generator 128. Random number generator 128 may contain a seed 129. The creation of random numbers with a high degree of entropy may be important the use of cryptographic algorithms 141. However, obtaining random numbers with high entropy in module 101 with limited processing resources may be a challenge using conventional technology. Since much of the operation of module 101 requires a CPU 101b following a pre-determined series of steps, such as the programmatic steps in an operating system 101h, module program 101i, etc., the random number generator seed 129 should preferably be populated with data that is close to random "noise" and not subject to replay. According to a preferred exemplary embodiment, module 101 utilizes data input from sensor 101f and/or radio 101z into a seed 129 within a random number generator 128. As one example, the sensor data input into seed 129 could comprise the least significant digits of a sensor measurement or series of sensor measurements, where the least significant digits would otherwise be effectively considered "noise".

Petitioner Samsung Ex-1038, 0069

In this exemplary embodiment of using a sensor to collect a "noisy" signal for input into a random number generator 128 or seed 129, if sensor 101f comprised a temperature measuring device such as a thermocouple or thermistor with a stated accuracy of 0.1 degrees, module 101 could take a series of measurements with 0.0001 degree resolution and utilize the last two digits appended from a series of measurements for input into a seed 129 in order to generate a random number 128a. Random number generator 128 could also utilize data input from the other components illustrated in Figure 1e in order to generate a random number 128a, where the data input from the other components comprise a signal with a high level of "noise" or high entropy. The seed 129 could comprise multiple seeds 129 or also a random number generator 128 could derive a random number 128a using input from other components illustrated in Figure 1e and without using a seed 129.

Other possibilities exist as well, such as if sensor 101f was a camera, module 101 could take a series of pictures and process the image to input data from the image into a seed 129. Likewise, module 101 could utilize numerous radio-frequency (RF) measurements from radio 101z in order to populate seed 129, including "noise" measurements on unused frequencies, or other data received by a radio 101z, including apparently random RF data. Although not illustrated in Figure 1e, module 101 preferably includes a timing source such as a clock, and the clock could also be utilized to input data into a seed 129. Data from radio 101z, a clock (not shown), and/or sensor 101f, and/or radio 101z could be combined in order to input data into a seed 129. Additional input into the seed 129 could include measurements or states within memory 101e and 101w, operating system 101h states and files, and reading data from hardware through a bus 101d. A state can comprise a list or set of constants, variables, values, and/or data at a point in time or over an interval of time.

A plurality of the data as a source for a random number seed 129 could be appended together into a "module random seed file" 139 (illustrated in Figure 1g) with a combined series or list of states (i.e. a plurality of sensor 101f measurements, radio 101z measurements, clock times, memory 101e or memory 101w states, operating system 101h states, actuator 101y states, and/or hardware 101a or 101d states). Note that values or data for each of the elements listed in the previous sentence could be utilized in a "module random seed file" 139 instead of or in addition to a state. The "module random seed file" 139 can then be input into the secure hash algorithm 141c described in Figure 1g below, and the output of the secure hash algorithm 141c could then be used in the input as a seed 129 within random number generator 128. Also, this combined data

Petitioner Samsung Ex-1038, 0070

(including in the form of a "module random seed file" 139) could be utilized by random number generator 128 directly in order to process a random number 128a. Other possibilities exist as well without departing from the scope of the present invention.

Note that the term "public key" as contemplated herein includes a key that may be shared with other elements, where the other elements may not be under the direct control of the same entity that holds the corresponding private key. However, the term "public key" as used herein does not require that the public key is made available to the general public or is publicly disclosed. An additional layer of security may be maintained in the present invention by preferably only sharing public keys on a confidential basis with other entities. For example, module public key 111 may be created by module 101 when generating module private key 112, and module 101 may share module public key 111 with M2M service provider 108 in order to record module public key 111 in server 105, but module 101 could choose to not share module public key 111 with other entities, such as wireless network 102 or make a certificate 122 with module public key 111 available on the Internet 107. The benefits of confidentially sharing module public key 111 with server 105 are also further described in connection with Figure 10 below.

Although a single public key and private key for (i) module 101 and (ii) server 105 are illustrated in Figure 1e and also Figure 1f below, respectively, both module 101 and server 105 may each utilize several different pairs of public keys and private keys. As one example, module 101 may record a first private key 112 used for creating a digital signature and a second private key 112 for decryption using asymmetric ciphering algorithms 141a. In this example, a server 105 could utilize a first module public key 111 to verify the digital signature, and a second module public key 111 could be utilized to encrypt messages sent to module 101. Similarly, either module 101 or server 105 may use private key 112 or 105c, respectively, to derive secondary shared keys such as a derived shared key 129b below. Thus, one key pair could be used with digital signatures, a second key pair used for asymmetric ciphering, and a third key pair to derive shared secret keys. Each of the three illustrated pairs of keys could comprise a set of keys, and each of the illustrated pairs of keys could also use a different set of parameters 126, although the parameters 126 for the various pairs of keys could also be the same.

In addition, module 101 could utilize a first set of keys to communicate with a first server 105 and a second set of keys to communicate with a second server 105. The first set of keys could

Petitioner Samsung Ex-1038, 0071

use or be associated with a first set of parameters 126 and the second set of keys could use or be associated with a second set of parameters 126. Likewise, M2M service provider 108 illustrated in Figure 1a could utilize a first pair of secondary private and public keys with a first server 105, and a second pair of secondary private and public keys with a second server 105. As contemplated herein, the term "private key" can also refer to secondary non-shared keys derived from a "parent" private key such as key 112 or key 105c, and the term "public key" can also refer to (i) secondary, shared keys derived using a private key such as key 112, or (ii) secondary, shared keys associated with a public key such as key 111. Other possibilities exist as well for a key to represent derived or associated keys without departing from the scope of the present invention.

According to exemplary embodiments, module 101 may also include a pre-shared secret key 129a. Pre-shared secret key 129a can comprise a secret key that is shared between module 101 and server 105 before module 101 begins (i) communicating with server 105 and/or a certificate authority 118, (ii) or utilizing PKI-based encryption and authentication to communicate with M2M service provider 108. As illustrated in Figure 1f below, server 105 could also record the pre-shared secret key 129a, and a pre-shared secret key 129a can be associated with each module 101 using a module identity 110. A pre-shared secret key 129a could be a secure key comprising a string or number loaded into a nonvolatile memory 101w of module 101 by a manufacturer, distributer, installer, or end user of module 101. Pre-shared secret key 129a can be moved by CPU 101b from the nonvolatile memory 101w into a RAM 101e for further processing during the use of cryptographic algorithms 141.

Note that pre-shared secret key 129a can be different than a pre-shared secret key used with conventional technology such as SIM cards in PLMN networks, such as the key Ki, where the pre-shared secret key in a SIM card is designed to not be available for movement or loading into a RAM 101e for processing by CPU 101b. Alternatively, pre-shared secret key 129a could be derived using a second pre-shared secret key Ki within a SIM card, but then server 105 would need to be able to derive the same pre-shared secret key 129a, even though server 105 may not have pre-shared secret key Ki available. Although not shown in Figure 1e, a module 101 may also include a SIM card that includes a pre-shared secret key 129a, wherein the pre-shared secret key 129a in a SIM card is different than pre-shared secret key Ki, since the pre-shared secret key in the SIM card cannot be moved into RAM 101e for processing with a cryptographic algorithms.

Petitioner Samsung Ex-1038, 0072

Pre-shared secret key 129a as illustrated in Figure 1e can be loaded by a manufacturer, distributor, installer, or end user of module 101 using a physical interface 101a, such as (i) a USB interface 101v, or (ii) a local WiFi network if module 101 includes a WiFi client. Pre-shared secret key 129a may optionally be uniquely bound to module identity 110, such that another module 101 with a different module identity 110 could not utilize pre-shared secret key 129a. Or, pre-shared secret key 129a could be used by any module 101, but only used one time and thus a second module 101 could not utilize the exact same key within a pre-shared secret key 129a for authentication with server 105 at a subsequent time. Alternatively, pre-shared secret key 129a could be shared by a plurality of modules 101, and for example compiled into a module program 101i, such that multiple modules utilize the same pre-shared secret key 129a.

Pre-shared secret key 129a could be obtained by a distributor, installer, or end user of module 101 by (i) using a local computer to access a web page from a web portal 171j, where the web page can be user password protected, (ii) entering, submitting, or typing information including a module identity 110 into the web page, and subsequently (iii) downloading pre-shared secret key 129a from the web portal 171j. A different web server could be utilized besides the web portal 171j illustrated in Figure 1d. The web server could be operated by an entity such as module provider 109, M2M service provider 108, or even certificate authority 118 (since pre-shared secret key 129a could be used to authenticate the submission of module public key 111). Note that the pre-shared secret key 129a could also be presented visually on a response web page to the submission, and the a manufacturer, distributor, installer, or end user could record the pre-shared secret key 129a visually presented on the response web page. Pre-shared secret key 129a could comprise a string of an exemplary set of characters or numbers such as 10 – 16 digits or characters, although other lengths for pre-shared secret key 129a could be possible as well.

According to a preferred exemplary embodiment, in order to obtain the pre-shared secret key 129a from a web page as described in the above paragraph, the distributor, installer, or end user of module 101 could read a pre-shared secret key code 134. Pre-shared secret key code 134 could be physically printed on module 101, such as next to a serial number printed on the enclosure of the device. Pre-shared secret key code 134 could be a unique and/or randomized string such as an exemplary 8 byte number or 10 character string (and other possibilities exist as well), where upon (a) successful submission to a web page of both the pre-shared secret key code 134 with a module identity 110, then (b) the release of pre-shared secret key 129a would be authorized for the

Petitioner Samsung Ex-1038, 0073

distributor, installer, or end user of module 101. Pre-shared secret key 129a could be transmitted through a secure web session such as SSL or TLS from a web portal 171j to a computer operated by the distributor, installer, or end-user. The distributor, installer, or end-user could then load the pre-shared secret key 129a into the nonvolatile memory of the module using (i) a LAN connection such as WiFi to the module (and in this case radio 101z in module 101 could support an 802.11 type connection) or (ii) a USB interface 101v.

Pre-shared secret key 129a could be utilized by a module 101 (i) as a shared secret key 510 in Figure 5b, or (ii) to derive a shared secret key 510 also recorded by a server 105 in Figure 5b below. Note that module program 101i preferably includes a verification process for any pre-shared secret key 129a loaded by a distributor, installer, or end user, where a hash value or combination of the pre-shared secret key 129a and module identity 110 could be verified. As one example, the last few digits or characters in a pre-shared secret key 129a could comprise a checksum for a string comprising both module identity 110 and pre-shared secret key 129a, such that module 101 could calculate the checksum after entry of pre-shared secret key 129a, and module 101 can reject the pre-shared secret key 129a if the checksum failed. In this manner, or through the use of similar techniques, system 100 can be designed so that pre-shared secret key 129a can only reasonably be utilized by a correct module 101 with the correct module identity 110 for the pre-shared secret key 129a.

Since module 101 may have multiple module identities 110, a first module identity 110 could be used with a pre-shared secret key code 134 and printed on an enclosure of module 101, while a second and more secure (i.e. longer length or more randomized bits) module identity 110 could be used as a module identity 110 in a message 208 as described in Figure 2 below. Note that when using the exemplary embodiment illustrated in Figure 5b below, (x) the module identity 110 submitted with a web page and pre-shared secret key code 134 is preferably different than (y) an unencrypted module identity 110 within a message 208 illustrated in Figure 6a and Figure 6b. A module identity 110 submitted by a distributor, installer, or end user in a web page could preferably be easy to manually type into a web page, such as 10 or 12 decimal digits or characters, while an unencrypted module identity 110 within a message 208 could be significantly longer, such as 16 or 24 extended ASCI characters, and other possibilities exist as well without departing from the scope of the present invention.

Petitioner Samsung Ex-1038, 0074

Application server 171 running web portal 171j could (i) record a table of triplets including module identities 110, pre-shared secret key codes 134, and pre-shared secret keys 129a, and (ii) return via a web page the pre-shared secret key 129a upon a successful match and entry of the submitted pre-shared secret key code 134 and module identity 110. Once the pre-shared secret key 129a has been utilized to authenticate or verify a module public key 111 with a server 105 (such as using subsequent steps 517 in Figure 5b below), then that particular pre-shared secret key 129a may be "discarded" and not used again for security purposes contemplated herein. After module 101 obtains an initial secure connection to server 105, using the techniques illustrated in Figure 3 through Figure 6b, then server 105 can securely send keys for use with future communication including a symmetric key 127 or other shared secret keys for authorizing any subsequent submission of a new module public key 111 with module identity 110 by module 101 in a step 517 illustrated in Figure 5b.

Note that the use of a pre-shared secret key 129a and pre-shared secret key code 134 is also optional, such that a module program 101i could cipher of obfuscate the initial submission of a derived module public key 111 and module identity to a server 105, so that server 105 could be reasonably assured only a valid module 101 submitted the module public key 111. Alternatively, the module manufacturer could load the pre-shared secret key 129a in non-volatile memory such as flash 101w upon manufacturing, and in this case a distributor, installer, or end-user may not need to access or load the pre-shared secret key 129a. However, the steps for a distributor, installer, or end-user to read a pre-shared secret key code 134 and submit the code to a web portal 171j to obtain pre-shared secret key 129a may still be useful, such as if module 101 needs the equivalent of a "factory reset" after deployment, reconfiguration such as loading new firmware, or otherwise reset or returned to a default state.

Although (A) a pre-shared secret key 129a may be useful for sending module public key 111 to server 105 or other entities connected to the Internet 107, such as a certificate authority 118, (B) pre-shared secret key 129a could be used for other purposes as well, such as input into a key derivation function 141f shown in Figure 1g so that module 101 and server 105 could obtain common derived shared secret keys 129b. In this case, a derived shared secret key 129b could be utilized as a shared secret key 510 depicted and described in connection with Figure 5b below. In addition, after the first use of pre-shared secret key 129a, a manufacturer, distributor, installer, or

Petitioner Samsung Ex-1038, 0075

end user may also upload a second pre-shared key 129a into module 101 at a future date, such as upon reconfiguration of a module 101.

According to a preferred exemplary embodiment, module 101 can derive its own module private key 112 and module public key 111, and utilize pre-shared secret key 129a in order to securely and/or authoritatively communicate the derived module public key 111 with server 105 and/or a certificate authority 118. The use of pre-shared secret key 129a can be particularly useful if module 101 has already been deployed with a monitored unit 119 and connects to server 105 though the Internet 107 for the very first time. Server 105 could preferably utilize pre-shared secret key 129a in order to confirm that a received module public key 111 and module identity 110 from module 101 authoritatively belong to module 101, as opposed to being an unauthorized or even fraudulent submission of module public key 111 and module identity 110.

Server 105 could utilize a pre-shared secret key 129a and the steps depicted and described in connection with Figure 4 below in order to securely receive module public key 111 and module identity 110 from module 101, including the first time module 101 sends module public key 111 to server 105. As one example, pre-shared secret key 129a could be utilized as a symmetric ciphering 141b key, described in Figure 1g below. After the first submission of module public key 111 to server 105, any subsequent submissions of new module public keys 111 derived by module 101 could either (i) continue to use the pre-shared secret key 129a, or (ii) use a symmetric key 127 derived after the first module public key 111 has been received. Securing the submission of module public key 111 with server 105, including both the first submission and subsequent submissions, is also depicted and described in connection with Figure 5b below.

Figure 1f

Figure 1f is a graphical illustration of the components within a server, in accordance with exemplary embodiments. Server 105 can include a module database 105k, a sub-server 105w, and a message preprocessor 105y. In an exemplary embodiment, the elements illustrated within a server 105 in Figure 1f may be stored in volatile memory such as RAM 105e, and/or storage 105m, and may also be accessible to a processor CPU 105b. In another exemplary embodiment, the module database 105k, sub-server 105w, and message processor 105y can comprise separate computers.

Petitioner Samsung Ex-1038, 0076

Module database 105k, sub-server 105w, and message preprocessor 105y could represent either different processes or threads operating on a server 105, or physically separate computers operating in conjunction over a network to perform the functions of a server 105. Since server 105 can preferably support communications with a plurality of modules 101, server 105 can utilize module database 105k to store and query data regarding a plurality of modules 101, monitored units 119, and the overall M2M service. The server 105 can store a plurality of module public keys 111 associated with a plurality of devices in the module database 105k. The server 105 can use the module identity 110 of device 101, received in a message such as a UDP packet, to query the module database 105k and select the public key 111 or symmetric key 127 associated with the module 101.

Although not illustrated in Figure 1f, module database 105k can also record a pre-shared secret key code 134, a set of parameters 126, and a module identity 110 for each module 101, along with the pre-shared secret key 129a shown in Figure 1f. In addition, although not illustrated in Figure 1f, module database 105k could store a symmetric key 127 for each module 101, if cryptographic algorithms 141 utilize a symmetric cipher 141b such as AES for communication with module 101. Examples of module database 105k could include MySQL, Oracle®, SQLite, hash tables, distributed hash tables, text files, etc. Module database 105k could reside within RAM 105e or storage 105m. Server 105 may also record a symmetric key 127, where the symmetric key 127 can be associated with an expiration time 133. Symmetric key 127 can also be recorded in a module database 105k or a sub-server 105w.

Message preprocessor 105y can process incoming packets and route them to an appropriate sub-server 105w using information contained in an incoming message, such as a module identity 110, a server identity 206 illustrated in Figure 2 below, and/or a destination IP address. Message preprocessor 105y can include rules for processing and routing, such a dropping malformed incoming messages or incoming messages without correct cryptographic data. Message preprocessor 105y could also optionally be combined with a server firewall 124 in order to provide firewall functionality and security at the network layer. Message preprocessor 105y may preferably remain "silent" to incoming packets without proper cryptographic data contained in an incoming message, such as one example of a properly formatted message 208 illustrated in Figure 6a below.

Petitioner Samsung Ex-1038, 0077

Sub-server 105w can include a server private key 105c and cryptographic algorithms 141. A plurality of sub-servers 105w can be utilized by a server 105 in order to support communication with a plurality of wireless modules 101. The server private key 105c and module public key 111 can be utilized by server 105 to secure communication with module 101, including the steps depicted and described in connection with Figures 4 and Figure 5a below. Cryptographic algorithms 141 may comprise a suite of algorithms or subroutines and can be utilized for (i) encrypting data using public keys, (ii) decrypting data using private keys, (iii) processing secure hash signatures using private keys, and (iv) verifying secure hash signatures using public keys.

A first sub-server 105w can process messages and responses with a first module 101 using a first set of security keys and algorithms, such as using RSA-based security, and a second sub-server 105w can process messages and responses with a second module 101 using a second set of security keys and algorithms, such as using ECC-based security. Consequently, message pre-processor 105y could route incoming messages to the appropriate sub-server 105w depending on the encryption algorithm used in the incoming message (which could be determined by message pre-processor 105y by querying the module database 105k using a module identity 110 in the incoming message 208). Sub-servers 105w may utilize separate server private keys 105c, or the sub-servers 105w can share a common private key 105c. Sub-servers 105w may utilize separate cryptographic algorithms 141, or the sub-servers 105x can share common cryptographic algorithms 141. Although separate sub-servers 105w are illustrated in Figure 1f, the sub-servers may optionally be combined with a server 105, or omitted, with the corresponding server private key 105c and cryptographic algorithms 141 stored directly in a server 105.

Server 105 may also comprise a collection of individual computers, where the individual computers could be either centrally located or geographically dispersed, but the individual computers may function in a coordinated manner over a network to operate as a server 105. Server 105 may be a "virtualized" server, with computing resources shared with other processes operating on a computer.

Petitioner Samsung Ex-1038, 0078

Figure 1g

Figure 1g is a graphical illustration of the components in a set of cryptographic algorithms, in accordance with exemplary embodiments. As contemplated herein, communications between (i) a module 101 and a server 105, and (ii) between application 171i and server 105 can be secured by using cryptographic algorithms 141. The cryptographic algorithms 141 used by module 101, server 105, application server 171, and/or application 171i can comprise a set of steps, procedures, or software routines for accomplishing steps to cipher, decipher, sign, and verify messages, including the generation of public keys, private keys, and derived shared keys. Cryptographic algorithms 141 can be implemented in software operating on (i) module 101 in the form of a module program 101i, (ii) server 105 in the form of a module controller 105x, or (iii) application server 171 in the form of an application 171i. Example software for a cryptographic algorithms 141 includes the libraries within the openssl, libmcrypt, and/or and Crypto++ discussed in Figure 1e. Other possibilities for the location of cryptographic algorithms within a module 101, server 105, or application 171i exist as well, including possibly module operating system 101h, server operating system 105h, and application server operating system 171h, respectively.

In addition, cryptographic algorithms 141 may be implemented in hardware or firmware on any of module 101, server 105, or application 171i. Note that module 101, server 105 and application 171i could each utilize a different set of cryptographic algorithms 141, although the sets of algorithms should preferably be fully interoperable (i.e. ciphering with a first symmetric ciphering algorithm 141b and a symmetric key 127 on module 101 could be deciphered by a second symmetric ciphering algorithm 141b on server 105 using the symmetric key 127, etc.). As illustrated in Figure 1g, cryptographic algorithms 141 may comprise an asymmetric ciphering algorithm 141a, a symmetric ciphering algorithm 141b, a secure hash algorithm 141c, a digital signature algorithm 141d, a key pair generation algorithm 141e, a key derivation function 141f, and a random number generator 128.

Asymmetric ciphering algorithms 141a can comprise algorithms utilizing public key infrastructure (PKI) techniques for both (i) encrypting with a public key and (ii) decrypting with a private key. Example algorithms within asymmetric algorithms 141a include the RSA algorithms 153 and the Elliptic Curve Cryptography (ECC) algorithms 154, and other asymmetric algorithms could be utilized as well. For example, either the ECC algorithms 154 or RSA algorithms 153 can

Petitioner Samsung Ex-1038, 0079

be used for encryption and decryption, including (i) encryption element 503 discussed below, as well as (ii) decryption element 413 discussed below. A set of parameters 126 can include input into asymmetric ciphering algorithms 141a, such as specifying key lengths, elliptic curves to utilize (if ECC), modulus (if RSA) or other parameters or settings required. As contemplated herein and described in additional detail below, the algorithms illustrated in Figure 1g can perform both ciphering and deciphering, using the appropriate keys.

The use and application of RSA algorithms and cryptography are described within IETF RFC 3447 titled "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", herein incorporated by reference, among other published standards for the use of RSA algorithms 153. The use of an RSA algorithm 153 for encryption and decryption, including with cryptographic algorithm and other description of encryption or decryption algorithms, can also be processed according to the description of the RSA algorithm according to the Wikipedia entry for "RSA (algorithm)" as of September 9, 2013, which is incorporated by reference herein.

The use and application of ECC algorithms 154 for asymmetric ciphering algorithms 141a within cryptographic algorithms 141 are described within IETF RFC 6090 titled "Fundamental Elliptic Curve Cryptography Algorithms" (herein incorporated by reference), among other published standards using ECC. ECC algorithms 154 can also utilize elliptic curve cryptography algorithms to the Wikipedia entry for "Elliptic curve cryptography" as of September 9, 2013, which is incorporated by reference herein. ECC algorithms 154 may utilized according to exemplary preferred embodiments in order to maintain high security with smaller key lengths, compared to RSA, thereby helping to comparably reduce the message lengths, radio frequency spectrum utilization, and processing power required by module 101. Thus, the use of ECC algorithms 154 within various steps requiring ciphering or digital signatures may help conserve battery life of module 101 while maintaining the objective of securing system 100. Note that as contemplated herein, other algorithms besides with ECC algorithms 154 and RSA algorithms 153 may be also be used in asymmetric algorithms 141a.

Cryptographic algorithms 141 may also include a set of symmetric ciphering algorithms 141b. Symmetric ciphering algorithms 141b can utilize a symmetric key 127 by one node such as a module 101 to encrypt or cipher data, and the encrypted data can be decrypted or deciphered by

Petitioner Samsung Ex-1038, 0080

server 105 also using the symmetric key 127. Examples of symmetric ciphers include Advanced Encryption Standard 155 (AES), as specified in Federal Information Processing Standards (FIPS) Publication 197, and Triple Data Encryption Standard (Triple DES), as described in NIST Special Publication 800-67 Revision 1, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher (Revised January 2012)". Parameters 126 input into symmetric ciphering algorithms 141b can include symmetric key 127 length, such as the selection of 128, 192, or 256 bits with AES 155 symmetric ciphering, and parameters 126 could also select a symmetric ciphering algorithm in a collections of symmetric ciphering algorithms 141b. Other examples of symmetric ciphering algorithms 141b may be utilized as well within cryptographic algorithms 141. Also note that as contemplated herein, the term "symmetric ciphering" contemplates the use of a symmetric ciphering algorithm 141b in order to encrypt or cipher data with a symmetric ciphering algorithm 141b, and "asymmetric ciphering" contemplated the use of an asymmetric ciphering algorithm 141a to encrypt or cipher data with a public key, such as module public key 111 or server public key 114.

Cryptographic algorithms 141 may also include a set of secure hash algorithms 141c in order to compute and output a secure hash value or number based on a string or file input into the secure hash algorithms 141c. Example secure hash algorithms include SHA256 156 (also known as SHA-2) and SHA-3 157. SHA256 156 is specified in the National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS PUB) 180-2 titled "Secure Hash Standard". SHA-3 157 is scheduled to be published in FIPS PUB 180-5. Parameters 126 input into secure hash algorithms 141c can include the selection of the length of the secure hash, such as using 224, 256, or 512 bits with either SHA-2 or SHA-3, and other possibilities exist as well.

Cryptographic algorithms 141 may also include a set of digital signature algorithms 141d, in order to sign and verify messages between (i) module 101 and server 105 or (ii) server 105 and application 171i. Digital signature algorithms 141d can also verify signatures such as comparing that (i) a first secure hash value in the form of a digital signature in a certificate (not shown) using a certificate authority public key 132 matches (ii) a second secure hash value in the certificate (not shown). Digital signature algorithms 141d can utilize algorithms in National Institute of Standards (NIST) "FIPS 186-4: Digital Signature Standard", or IETF RFC 6979 titled "Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)".

Petitioner Samsung Ex-1038, 0081

The use of ECDSA algorithm 158 within a set of digital signature algorithms 141d may be preferred if keys such as module public key 111 and server public key 114 are based on elliptic curve cryptography. Other PKI standards or proprietary techniques for securely verifying digital signatures may be utilized as well in digital signature algorithms 141d. Parameters 126 input into digital signature algorithms 141d can include the selection of a secure hash algorithms 141c to utilize with digital signature algorithms 141d, or the algorithm to utilize, such as ECDSA shown or an RSA-based alternative for digital signatures is possible as well. Parameters input into digital signature algorithms 141d can also include a padding scheme for use with a digital signature algorithms 141d. Digital signature algorithms 141d could also include an RSA digital signature algorithm for use with RSA-based public and private keys.

Cryptographic algorithms 141 may also include key pair generation algorithms 141e, a key derivation function 141f, and a random number generator 128. Key pair generation algorithms 141e can be utilized by module 101, server 105, or application 171i to securely generate private and public keys. The key pair generation algorithms 141e can also use input from a parameters 126, such as the desired key lengths, or an ECC curve if the public key will support ECC algorithms 154. According to an exemplary preferred embodiment, module 101 can derive a pair of module public key 111 and module private key 112 using key pair generation algorithms 141e. Software tools such as openssl and libcrypt include libraries for the generation key pairs, and these and similar libraries can be used in a key pair generation algorithm 141e.

Key derivation function 141f can be used by module 101, server 105, and/or application 171i in order to determine a common derived shared secret key 129, using at least two respective public keys as input, and may also include the input of a private key. A key exchange to share a common symmetric key 127 can be performed using a key derivation function 141f and parameters 126. An exemplary algorithm within a key derivation function 141f can be the Diffie-Hellman key exchange, which is used by tools such as secure socket layer (SSL) with RSA algorithms 153. When using ECC algorithms 154, module 101 and server 105 can utilize Elliptic Curve Diffie-Hellman (ECDH) algorithms 159, and a summary of ECDH is included in the Wikipedia article titled "Elliptic Curve Diffie-Hellman" (http://en.wikipedia.org/wiki/Elliptic_curve_Diffie%E2%80%93Hellman" from September 24, 2013, which is herein incorporated by reference. Other algorithms to derive a shared secret key 129b using public keys and a private key may also be utilized in a key derivation function 141f,

Petitioner Samsung Ex-1038, 0082

such as the American National Standards Institute (ANSI) standard X-9.63 160. Parameters 126 used with key derivation function 141f with elliptic curve cryptography can include a common base point G for two node using the key derivation function 141f and public keys. The base point G in a parameters 126 can be transmitted or sent from a module 101 to a server 105 in a message 208, and the base point G can be sent from a server 105 to a module 101 in a response 209, and other possibilities exist as well. Parameters 126 can also include other or additional information for using a key derivation function 141f in order to derive a commonly shared symmetric key 127.

Parameters 126 input into key pair generation algorithms 141e can include the type of asymmetric ciphering algorithms 141a used with the keys, the key length in bits, an elliptic curve utilized for ECC, a time-to-live for a public key that is derived, and similar settings. Additional parameters 126 for a public key can include a supported point formats extension, where the supported point formats extension could comprise uncompressed, compressed prime, or "compressed char2" formats, as specified in ANSI X-9.62. In other words, an ECC public key can have several formats and a set of parameters 126 can be useful to specify the format. Although a set of parameters 126 is illustrated in Figure 1g as internal to cryptographic algorithms 141, parameters 126 could be recorded in other locations in a module 101 or a system 100. As one example, parameters 126 could be recorded in a server 105 and downloaded by module 101 using the Internet 107. The various algorithms within cryptographic algorithms 141 may utilize a random number generator 128, which is also depicted and described in connection with Figure 1e above.

According to a preferred exemplary embodiment, parameters 126 can include values to define an elliptic curve and/or use ECC algorithms 154. The values could be constants or variables in a defining equation for an elliptic curve, or the parameters could simply name an existing, defined curve such as the standard named curve illustrated in parameters 126 in Figure 1h. Parameters 126 could include a set of ECC parameters 137 for using elliptic curve cryptography in ECC algorithms 154, where the ECC parameters 137 can include the ECC parameters in section 3.3 of IETF RFC 6090, including: (i) a prime number p that indicates the order of a field Fp, (ii) a value "a" used in a curve equation, (iii) a value "b" used in the curve equation, (iii) a generator "g" of the subgroup, and (iv) an order "n" of the subgroup generated by "g". Further, the ECC parameters 137 could include values used for elliptic curve cryptography as specified in IETF RFC 5639 titled "Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation", section 3: (i) a "p" value for the prime specifying the base field, (ii) "A" and "B" are coefficients for an

Petitioner Samsung Ex-1038, 0083

equation such as y^2 = x^3 + A*x + B mod p defining the elliptic curve, (iii) "G" = (x,y) as the base point, i.e., a point in E of prime order, (iv) "q" as the prime order of the group generated by G, and (v) "h" as the cofactor of G in E, i.e., #E(GF(p))/q. Other possibilities exist as well for an ECC parameters 137 that can be used in a cryptographic algorithms. Parameters 126 could also include an ECC standard curve 138, which could comprise a name and/or values for a standardized curve, such as the list of named curves included in section 5.1.1 of IETF RFC 4492 titled "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)."

As contemplated herein, a set of cryptographic algorithms 141 may operate using either strings or numbers, and parameters 126 could include either strings or numbers as well. The processing of cryptographic algorithms within a module 101 can take place within a CPU 101b, or module 101 could also process cryptographic algorithms in a cryptographic processing unit (not shown) connected to the system bus 101d. According to an exemplary embodiment, a module 101 or a server 105 could include a cryptographic processing unit (not shown) separate from the CPU 101b in order to speed cryptographic computations and/or reduce energy required for supporting the use of cryptography through a system 100. Alternatively, cryptographic algorithms can be implemented entirely in software within a module 101 and/or server 105.

Figure 1h

Figure 1h is an illustration of a certificate that includes a PKI public key, where the key comprises an elliptic curve cryptography key, in accordance with exemplary embodiments. Public and private keys in system 100 can utilize PKI techniques other than RSA, such as the elliptic curve cryptography (ECC) public key 111 illustrated in Figure 1h. One benefit of using ECC is that an equivalent level of security can be obtained for a much smaller key length. Also, energy may be conserved using ECC algorithms 154 compared to RSA algorithms 153. An analysis of the energy conserved for ciphering, deciphering, signing, and verifying messages using ECC versus RSA is included in the paper titled "Energy Analysis of Public-Key Cryptography on Small Wireless Devices" by Wander et al (herein incorporated by reference). Smaller key lengths save bandwidth, memory, processing resources, and power, which are all valuable for a module 101 to conserve a battery 101k and usage of radio-frequency spectrum. For example, an ECC key length of 283 bits

Petitioner Samsung Ex-1038, 0084

provides security similar to an RSA key length of approximately 2048 bits. Module public key 111 can comprise an ECC key in an X.509 certificate, as illustrated in Figure 1h. Another benefit of using ECC algorithms 154 is that many different defining equations for elliptic curves could be utilized, and the defining equations could also be kept confidential, such that a defining equation for an elliptic curve used in ECC algorithms may optionally be omitted from a certificate 122. In this case, if a public key such as module public key 111 is recorded in a certificate 122, a name or identifying value for the elliptic curve used with a public key could be recorded in a certificate 122, but the underlying defining curve for an elliptic curve could remain confidential. The values to determine an elliptic curve defining equation could be stored in a parameters 126, and the defining equation could also optionally be disclosed.

Certificate 122 could include a signature 123, where signature 123 can be signed using ECC signature techniques, such as the Elliptic Curve Digital Signature Algorithm (ECDSA) 158 with a secure hash such as SHA256 156. In order to generate signature 123, the private key associated with either CA 118 or module provider 109 may also be an ECC-based private key. Note that the public key 111 in a certificate 122 could use a different asymmetric ciphering algorithm 141a than the algorithm used for signing, such that the public key 111 can be an ECC key, while the signature 123 could be generated with RSA algorithm 153 and/or key. Certificate 122 may also include parameters 126, where parameters 126 can specify an elliptic curve utilized with the module public key 111. Parameters 126 could also include the start and end times for the validity of either public key 111 or certificate 122. Other parameters 126 can be utilized in a certificate 122 as well, and a parameters 126 may specify values that are not included or external to a certificate 122.

Certificate 122 illustrated in Figure 1h also illustrates an exemplary embodiment of the present invention. Over the lifetime of a module 101, which could be a decade or longer, multiple module public keys 111 may be utilized. The potential use of multiple different module public keys 111 include (i) the expiration of a certificate 122 (including expiration of a public key associated with a certificate authority used in signature 123), (ii) a need to change an elliptic curve specified in a parameters 126, (iii) adding a new public/private key pair for connection with a different wireless network 102, (iv) as increasing a key length utilized in a public/private key pair, (v) the transfer of ownership or control of module 101, and/or (vi) module 101 connecting to a new server that utilizes a different asymmetric ciphering algorithm (i.e. RSA instead of ECC). Other possibilities exist as well for reasons a module to derive a new module public key 111. Note that the multiple module

Petitioner Samsung Ex-1038, 0085

public keys 111 may also be utilized concurrently, such that (i) a first module public key 111 in a first certificate 122 can be utilized with a first server 105, and (ii) a second module public key 111 (possibly derived using a different set of parameters 126 including using a different elliptic curve) can be utilized with a second server 105 and/or wireless network 102.

In either case of (i) module 101 using multiple module public keys 111 concurrently, or (ii) module 101 using different module public keys 111 in sequence, a certificate 122 can preferably include a module public key identity 111a to specify the module public key 111 utilized in a certificate 122. As illustrated in Figure 1a, the module public key identity 111a could be included in the "Common Name" (CN) field, and the module identity 110 can be included in the "Organizational Unit" (OU) field. Alternatively, the module public key identity 111a and module identity 110 can be appended together and used in the CN field. In this manner and according to preferred exemplary embodiments, a module public key identity 111a is utilized with both a module identity 110 and a module public key 111 within a certificate 122. Also, as noted previously herein, the use of a certificate 122 may optionally be omitted, such that module 101 and server 105 share public keys without using certificates 122. The module identity 110, or a value associated with the module identity 110 can also be included in certificate 122, such as the "Common Name" (CN) field of a X.509 certificate 122, as illustrated in Figure 1h.

Note that the use of a certificate 122 is not required for the format of a public or shared key, and the public keys could optionally omit a signature from a certificate authority 118. In this case, the public keys such as module public key 111 and/or server public key 114 could be recorded in the format of a string, without the additional fields illustrated in Figure 1h. Server public key 114 may also be recorded in a certificate 122 with a signature 123 from a certificate authority 118. Other possibilities exist as well without departing from the scope of the present invention.

Figure 1i

Figure 1i is a graphical illustration of an exemplary system that includes a user, an application, a set of servers, and a set of modules, in accordance with exemplary embodiments. System 199 illustrated in Figure 1i can include a user 183, an application 171i, a set of servers 105, and a set of modules 101, which can communicate as illustrated using the Internet 107. Each of a

Petitioner Samsung Ex-1038, 0086

server 105 A and server 105 B and additional servers can communicate with a plurality of modules. An application 171i can communicate with a plurality of servers 105. Although the servers 105 an application 171i in system 100 in Figure 1i are illustrated as being separate, application 171i and server 105 may optionally be combined into a single node, such that the application 171i and server 105 operate as separate processes or programs on the same computer, or on a computer operating in a distributed environment such as a cloud configuration. In addition, even though a single application 171i and a single user 183 are illustrated in Figure 1i, a system 199 could include multiple applications 171i and multiple users 183.

User 183 can comprise an individual, business manager, network engineer, systems administrator, other employee with functional responsibilities for a system 199 (or components within a system 199 or system 100) accessing application 171i using a computer with a user interface such as a web browser 183a. Application 171i could also send an email or text message to user 183 if an alarm condition is detected in system 199, such as if a sensor 101f measurement exceeds a prescribed threshold value. The web browser 183a could use a connection 184 to access a web portal 171j operating on application 171i. Connection 184 could include hypertext markup language (HTML) messages, and could be through a secure connection such as TLS or IPsec, although other possibilities exist as well to those of ordinary skill in the art. Any module 101, such as Module 101 A, could use the Internet 107 and establish a primary connection 181 with server 105 A, and also module 101 A could establish a backup connection 182 with server 105 B if the primary connection 181 is not available. Alternatively, any module 101, such as module 101 A, could communicate with more than one server 105 concurrently or in sequence, such that module 101 A communicates with both server 105 A and server 105 B. According to exemplary embodiments, during an active state between periods of sleep or being dormant, module 101 may communicate with more than one server 105, such as a first server 105 A and a second server 105 B. Other possibilities for a plurality of modules 101 to communicate with a plurality of servers 105 exist without departing from the scope of the present invention.

Petitioner Samsung Ex-1038, 0087

Figure 2

Figure 2 is a graphical illustration of an exemplary system, where a module sends a message to a server, and where the server responds to the message, in accordance with exemplary embodiments. Module 101 as depicted and described in Figure 2 can operate as a wireless module 101, although a wired connection to the Internet 107 could alternatively be utilized. System 100 as illustrated in Figure 2 includes RF signals 201, module IP address 202, port number 203, module IP:port 204, server port number 205, server ID 206, server IP:port number 207, message 208, response 209, wireless network firewall address 210, and firewall port binding packet 211. Many of the elements illustrated within system 100 in Figure 2 are also depicted and described in connection with Figure 2 of U.S. patent application Ser. No. 14/039,401 (the contents of which are hereby incorporated by reference in their entirety). As contemplated herein, a wireless module 101 can comprise a module 101, or in other words a wireless module 101 may be a module 101 that is wireless. Functions described as being performed by a wireless module 101 may also be performed by a wired module 101 (where connection to a wired network would be used instead of connection to a wireless network 102). Also as contemplated herein and illustrated in Figure 2, the wording "module 101 sends a message 208" can also be considered equivalent to "server 105 receives a message 208". Likewise, the wording "server 105 sends a response 209" can be considered equivalent to "module 101 receives a response 209".

A wireless module 101 can wake from a dormant state in order perform (i) remote and automated monitoring and (ii) control functions such as collecting a sensor 101f measurement, communicating with server 105, and controlling an actuator 101y. If module 101 is connected to land-line power or a long-lasting external power source such solar power, then module 101 may remain in an active state and bypass a dormant state, although transmitting RF signals 201 may preferably only be utilized when communicating with wireless network 102 or sending data to and receiving data from server 105. Upon waking from the dormant state and starting communication with a server 105, a wireless module 101 can begin transmitting RF signals 201 to base station 103. The wireless module can acquire an IP address 202 from the wireless network 102. IP address 202 is illustrated as being an IPv6 address, but IP address 202 could also be an IPv4 address. IP address 202 could also be a subset of IPv6 addresses such as the last 32 or 64 bits in a full 128 bit IPv6 address, and wireless network 102 could append the beginning 96 or 64 bits, respectively, of the IPv6 address when wireless module 101 sends packets to the Internet 107.

Petitioner Samsung Ex-1038, 0088

In order to transmit or send data from wireless module 101 to server 105, a wireless module 101 can use module program 101i to collect data from a sensor 101f in order to update server 105. Module program 101i can request a port number 203 from operating system 101h in order to have a source IP:port for sending data using IP protocols such as TCP and UDP. The terminology "IP:port" as described herein refers to combining an IP address with a port number. Wireless module IP address 202 and port number 203 can be combined to form IP:port number 204. IP:port number 204 can be utilized as a source IP:port number for packets transmitted from wireless module 101, as well as a destination IP:port number for packets received by wireless module 101, when communicating with server 105.

In order to utilize Internet 107, module 101 may also need a destination IP address and port number in order to send packets to server 105. Before sending data to server 105, wireless module 101 preferably retrieves server IP address 106 and server port number 205 from RAM 101e. Server IP address 106 could be recorded in RAM 101e via (i) a DNS query using server name 206 or (ii) queries to M2M service provider 108 or wireless network 102. CPU 101b may copy server IP address 106 and server port number 205 from nonvolatile memory into volatile memory such as a register for processing to send a packet to server 105. Server name 206 could also be a server identity. (A) Server IP address 106 or server name 206 and (B) server port number 205 could be recorded in a nonvolatile memory such as flash memory 101w so that wireless module 101 can store the proper destination of packets transmitted or sent even when wireless module is dormant or shutdown, which avoids the processing and bandwidth requirements of obtaining server IP address 106 and server port number 205 every time the wireless module 101 wakes from the dormant or shutdown state. Server IP address 106 and server port number 205 can be combined into a server IP:port number 207.

After collecting data from a sensor, module 101 can send a packet from IP:port 204 to IP:port 207, and the packet could comprise a message 208 that may include the data from a sensor 101f. Note that message 208 does not need to include sensor data, and message could potentially be a periodic registration message or keep-alive message. As contemplated herein, the term "sensor measurement" can refer to data associated with or derived from a sensor 101f. A sensor measurement, can comprise a string containing data regarding a parameter of a monitored unit 119 and collected by a sensor 101f. The sensor measurement as sent in a message 208 can also represent a string (alphanumeric, binary, text, hexadecimal, etc.), where the string comprises a

Petitioner Samsung Ex-1038, 0089

transformation or processing of sensor data collected by a CPU 101b, such including formatting, compressing, or encrypting, encoding, etc. of sensor data.

In order to minimize bandwidth and time required for RF signals 201 to be active, module 101 can send the message 208 as a single UDP datagram in accordance with a preferred exemplary embodiment. The single UDP datagram in this embodiment can preferably be the only packet sent from module 101 to server 105 or M2M service provider 108 during a wake state for the module 101 when the radio 101z is active and transmitting, such as in a radio resource control (RRC) connected state. In other words, according to this preferred exemplary embodiment, the message 208 sent by module 101 can preferably be the only message or packet sent by the wireless module to the server 105 between dormant periods of module 101. By sending message 208 as a single UDP datagram, both a battery 101k is conserved and utilization of valuable RF spectrum is reduced. Message 208 could also comprise a series of associated UDP messages.

Also, as contemplated herein, message 208 could comprise a related series of packets, so that message 208 could comprise multiple datagrams. As one example, if TCP is utilized as the transport protocol for message 208, then the series of TCP messages including the initial handshake, one or more packets of payload data, and the closing of the connection could together comprise message 208. As another example, if UDP or UDP Lite is utilized for the transport protocol, and payload data exceeds a maximum transmission unit (MTU) size for the UDP packet and the payload data is spread across multiple packets, then the multiple packets would comprise a message 208. Further, a related series of packets comprising a message 208 could be identified by using the same source port number for module 101. In addition, a related series of packets comprising a first message 208 could be identified as a series of packets sent by module 101 before receiving a response 209 from a server, and packets sent after receiving a response 209 could comprise a second message 208. Other possibilities for a message 208 to comprise multiple packets or datagrams may exist without departing from the scope of the present invention.

The UDP datagram for message 208 could also be formatted according to the UDP Lite protocol, as specified in IETF RFC 3828, which is also incorporated by reference herein. The term "UDP Lite" described in the present invention may also refer to any connectionless protocol widely supported on Internet 107 where checksums may be partially disabled, thereby supporting the transfer of bit errors within a datagram. The advantages of UDP over TCP is that UDP can be

Petitioner Samsung Ex-1038, 0090

quickly sent, while TCP requires a "handshake" with the server which requires more time and bandwidth, which would utilize more energy from battery 101k. Weak or "noisy" RF signals between wireless module 101 and wireless network 102 may degrade or slow TCP transmissions, resulting in unwanted and unnecessary retransmission of individual TCP messages in the standard TCP "handshake" and connection close procedures. Also, the sensor data from a sensor 101f may be relatively small, such as a dozens of bytes in an exemplary embodiment, and UDP can provide significantly less signaling overhead than TCP, especially with small messages for the duration of the session. However, some M2M applications may prefer or require TCP and in this case message 208 can be formatted according to TCP. Thus, according to an exemplary embodiment, both message 208 and response 209 can be TCP messages. In this exemplary embodiment, message 208 and response 209 could each comprise a series of TCP messages that can include a TCP SYN, SYN ACK, ACK, ACK w/ data, FIN ACK, etc.

According to an exemplary embodiment, module 101 sends the same sensor data in multiple copies of the same UDP packet. Each of the multiple copies of the same UDP packet can also optionally be formatted according to the UDP Lite protocol. As one example, wireless module sends three identical copies of the UDP or UDP Lite packet that include the same sensor data. The benefit of sending three copies of UDP Lite include (i) the RF signals 201 received by the base station 103 could include bit errors, which could result in a regular (RFC 768) UDP packet being dropped, since a bit error could result in a UDP checksum mismatch, as received and processed by wireless network 102. Note that the use of checksums is mandatory in IPv6, and thus checksums cannot be fully disabled in IPv6. With UDP Lite packets transmitted by wireless module 101, where the mandatory checksum for IPv6 can cover the packet header, wireless network 102 can forward all packets received, potentially including bit errors, to server 105 over the Internet 107.

Server 105 can receive the multiple copies of the UDP or UDP Lite packets, which could include bit errors received, and server 105 could compare or combine the multiple copies or each individual UDP Lite packet in order to remove bit errors. Note that UDP Lite is not required, and wireless module 101 could send the message 208 using a single UDP packet, or multiple copies of a regular UDP (i.e. non UDP Lite) packet. However, using UDP Lite with multiple packets sent can provide benefits such as if the sensor data is encrypted in the packet, then a single bit error would normally break the receiver's ability to decipher the data using a cryptographic key, unless the

Petitioner Samsung Ex-1038, 0091

encrypted data was channel coded and the channel coding could recover from the bit error in order to present an error-free input of the encrypted data to a deciphering algorithm.

Further, between periods of sleep when a wireless module 101 becomes active and transmits RF signals 201, module 101, which may also comprise a wireless module 101, could send the sensor data in a single UDP Lite packet where the packet includes channel coding, which can also be referred to forward error correction. Forward error correction could also be implemented by sending multiple copies of the same UDP packet. Note that since large segments of message 208 could include encrypted or hashed data, those segments may not be appropriate for compression since the data is often similar to random strings which are not readily compressed. Channel coding techniques for the data in message 208 could include block codes and convolution codes. Block codes could include Reed-Solomon, Golay, BCH, Hamming, and turbo codes. According to a preferred exemplary embodiment, data within message 208 is sent as a UDP Lite packet using a turbo code to correct multiple bit errors within a packet or datagram sent by module 101 and received by server 105.

In system 100 illustrated in Figure 2, server 105 can use IP:port 207 to receive the packet from wireless module 101 and sent from source IP:port 204 to IP:port 207, and the packet could comprise a message 208 that may include the data from a sensor associated with module 101 or monitored unit 119. As contemplated herein, a message 208 illustrated in Figure 2 does not need to include sensor data and other data could be transmitted or sent, such as a server instruction 414 (described in Figure 4 below), or other data pertaining to module 101 or a monitored unit 119. Note that server 105 can use IP:port 207 to receive a plurality of messages 208 from a plurality of wireless modules 101. Server 105 preferably listens for UDP packets on IP:port 207 or monitors IP:port 207, although TCP packets could be supported as well. If server 105 receives multiple copies of the same UDP packet from module 101, server 105 preferably includes a timer. The timer can start when the first packet in the series of packets comprising a message 208 is received, and packets received outside the expiration of the timer would be discarded. In this manner, server 105 would be protected from replay attacks, even though module 101 may send multiple copies of the same packet in order to implement forward error correction. The timer used by a server 105 to drop duplicate packets received outside the timer window could be a relatively short value such as less than 5 seconds.

Petitioner Samsung Ex-1038, 0092

After receiving the message 208 and processing the message according to the techniques described below such as in Figure 4, server 105 can send a response 209. Since module 101 may belong to a wireless network 102 which includes a firewall 104, the source IP:port of the message 208 received by server 105 could be different from the source IP:port 204 utilized by wireless module 101. The source IP:port in message 208 could be changed if firewall 104 performs network address translation (NAT), as one example. Server 105 may not readily know if a NAT translation has been performed on the message 208. Alternatively, firewall 104 may not perform NAT, but could still block data from the Internet 107 which does not properly match the firewall rules. As one example, firewall 104 could be a symmetric firewall (but without NAT functionality), where only packets from IP:port 207 to IP:port 204 are allowed to pass the firewall after message 208 has been sent by module 101.

In either case, where firewall 104 may or may not perform NAT routing, server 105 preferably sends the response 209 from the server IP:port 207 to the source IP:port it receives in message 208. According to a preferred exemplary embodiment, response 209 is a UDP packet sent from server 105 with (i) a source IP:port 207 and (ii) a destination IP:port equal to the source IP:port received in message 208, as illustrated in packet 209a. The example use of source and destination IP:ports in message 208 and response 209 are also illustrated in Figure 6a below. In this manner, the UDP packet can traverse a firewall 104, if firewall 104 is present. If firewall 104 is present and performs NAT routing, then firewall 104 can receive the response 209 and change the destination IP address and port within response 209 to equal IP:port 204.

According to exemplary preferred embodiments, module 101 may also obtain power from a land-line source, such as a traditional 120 volt wall socket, or possibly power over Ethernet, and other non-transient power sources could be utilized as well. In this case, module 101 may remain persistently connected to the Internet through either a wireless network 102 or a wired connection such as Ethernet. In other words, module 101 may omit entering periods of sleep or dormancy where inbound packets from the Internet would not be received due to the sleep state of module 101. Consequently in an exemplary embodiment, module 101 which does not sleep for periods longer than a minute may preferably periodically send a firewall port binding packet 211 from IP:port 204 to IP:port 207 in order to keep ports and addresses within a firewall 104 and/or firewall 124 open to communications between module 101 and server 105. Firewall port binding packet 211

Petitioner Samsung Ex-1038, 0093

can comprise a packet that is sent periodically using a timer interval that is shorter than the port-binding timeout period 117 on a firewall 104 and firewall 124.

Continuing with this exemplary embodiment where module 101 does not sleep for periods longer than approximately one minute, if UDP is utilized for message 208 and response 209, then a small UDP packet comprising firewall port binding packet 211 can be sent periodically such as every 45 seconds. If TCP is utilized for message 208 and response 209, then a small TCP packet comprising firewall port binding packet 211 can be sent periodically such as every 4 minutes. Other possibilities for the timing of sending firewall port binding packet 211 are possible as well. By sending firewall port binding packet 211 periodically, server 105 (i) can send module 101 a response 209, which could include a module instruction 502 as explained in Figure 5a, at (ii) time intervals between message 208 and response 209 that are longer than the firewall port binding timeout values 117 of firewall 104 and/or firewall 124. Without firewall port binding packet 211, if (A) a response 209 sent from server 105 at an exemplary 180 seconds after receiving message 208, such as after a firewall port binding timeout value 117 of firewall 104 of an exemplary 60 seconds, then (B) response 209 would be dropped by firewall 104 and the response 209 would not be received by module 101.

Figure 3

Figure 3 is a flow chart illustrating exemplary steps for a server to receive a message from a module, in accordance with exemplary embodiments. As illustrated in Figure 3, Figure 3 can include steps used by a module controller 105x in a server 105 as illustrated in Figure 1c. The processes and operations, including steps for module controller 105x, described below with respect to all of the logic flow diagrams may include the manipulation of signals by a processor and the maintenance of these signals within data structures resident in one or more memory storage devices. For the purposes of this discussion, a process can be generally conceived to be a sequence of computer-executed steps leading to a desired result.

These steps usually require physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical, magnetic, or optical signals capable of being stored, transferred, combined, compared, or otherwise manipulated. It is

Petitioner Samsung Ex-1038, 0094

convention for those skilled in the art to refer to representations of these signals as bits, bytes, words, information, elements, symbols, characters, numbers, points, data, entries, objects, images, files, or the like. It should be kept in mind, however, that these and similar terms are associated with appropriate physical quantities for computer operations, and that these terms are merely conventional labels applied to physical quantities that exist within and during operation of the computer.

It should also be understood that manipulations within the computer are often referred to in terms such as listing, creating, adding, calculating, comparing, moving, receiving, determining, configuring, identifying, populating, loading, performing, executing, storing etc. that are often associated with manual operations performed by a human operator. The operations described herein can be machine operations performed in conjunction with various input provided by a human operator or user that interacts with the computer.

In addition, it should be understood that the programs, processes, methods, etc. described herein are not related or limited to any particular computer or apparatus. Rather, various types of general purpose machines may be used with the following process in accordance with the teachings described herein.

The present invention may comprise a computer program or hardware or a combination thereof which embodies the functions described herein and illustrated in the appended flow charts. However, it should be apparent that there could be many different ways of implementing the invention in computer programming or hardware design, and the invention should not be construed as limited to any one set of computer program instructions.

Further, a skilled programmer would be able to write such a computer program or identify the appropriate hardware circuits to implement the disclosed invention without difficulty based on the flow charts and associated description in the application text, for example. Therefore, disclosure of a particular set of program code instructions or detailed hardware devices is not considered necessary for an adequate understanding of how to make and use the invention. The inventive functionality of the claimed computer implemented processes will be explained in more detail in the following description in conjunction with the remaining Figures illustrating other process flows.

Petitioner Samsung Ex-1038, 0095

Further, certain steps in the processes or process flow described in all of the logic flow diagrams below must naturally precede others for the present invention to function as described. However, the present invention is not limited to the order of the steps described if such order or sequence does not alter the functionality of the present invention. That is, it is recognized that some steps may be performed before, after, or in parallel other steps without departing from the scope and spirit of the present invention.

The processes, operations, and steps performed by the hardware and software described in this document usually include the manipulation of signals by a CPU or remote server and the maintenance of these signals within data structures resident in one or more of the local or remote memory storage devices. Such data structures impose a physical organization upon the collection of data stored within a memory storage device and represent specific electrical or magnetic elements. These symbolic representations are the means used by those skilled in the art of computer programming and computer construction to most effectively convey teachings and discoveries to others skilled in the art.

At step 311, the server 105 can record a module public key 111, or a plurality of module keys 111 in a module database 105k. The module public key 111 could be received in a message 208 according to steps 516 and 517, including authenticating the message 208, as depicted and described in connection with Figure 5b below. Module public key 111 could also be recorded at step 311 before module 101 connects to the Internet 107 the very first time, and in this case module public key 111 could be recorded in server 105 by M2M service provider 108 or module provider 109. At step 312, the server 105 can open a TCP/UDP socket associated with an IP:port number 207 and listen or monitor for incoming message from modules. At step 313, server 105 can receive a message 208 sent by module 101, using the IP:port number 207. Although not illustrated in Figure 3, upon the first communication from module 101 by server 105 where the communication could include step 313, according to an exemplary embodiment, module 101 can also send a certificate 122 to server 105, where certificate 122 would normally include module public key 111 and module identity 110. Server 105 could utilize a certificate 122 to verify a module identity 110, as described in Figure 4 below at step 412.

An exemplary format of message 208 is depicted and described in connection with Figure 6a below, and other possibilities for a message 208 exist as well. Although not illustrated in Figure 3,

Petitioner Samsung Ex-1038, 0096

after receiving message 208, server 105 may also process any channel coding present in message 208 in order to eliminate any bit errors received. The channel coding could be included in a message 208 that utilizes the UDP Lite protocol. At step 314, server 105 can decrypt a message 208 using a cryptographic algorithm 141 and one of (i) server private key 105c, or (ii) a symmetric key 127. Additional details regarding step 314 are depicted and described in connection with Figure 4 below. At step 315, server 105 can verify that message 208 was sent by module 101 using a module identity 110, module public key 111, and a cryptographic algorithm 141. Additional details regarding step 315 are depicted and described in connection with Figure 4 below. Note that step 315 can take place before step 314 if the module identity 110 and/or a digital signature is not encrypted within message 208 (i.e. a sensor measurement in message 208 could be encrypted but a module identity 110 or digital signature may not be encrypted). Step 315 may optionally be omitted, if a symmetric key 127 is used to cipher data within message 208, such that a module digital signature from module 101 was previously verified when the symmetric key 127 was implemented.

After verifying the identity of module 101 in step 315, at step 316 server 105 can record sensor data or sensor measurements within message 208 in a module database 105k, if message 208 has a sensor measurement. Note that message 208 may not have a sensor measurement, and in this case step 316 can be skipped, or message 208 may also include other data besides a sensor measurement. Sensor data recorded in module database 105k can be made available for subsequent processing by server 105 or other servers or applications associated with an M2M service provider 108 in order to manage the function and operation of module 101 or monitored unit 119. As illustrated in Figure 7 through Figure 9, received sensor data could also be forwarded by server 105 to an application server 171. Although not illustrated in Figure 3, in an exemplary embodiment at step 316 server 105 could alternatively forward the sensor data to application 171i instead of recording the data in module database 105k.

After receiving message 208, server 105 can process a response 209 at step 317a. Step 317a can comprise encrypting an instruction, where the instruction could include an acknowledgement of the message received, a command or setting for an actuator, and/or another control message for module 101. Server 105 can utilize a module public key 111 and cryptographic algorithms 141 in order to encrypt the instruction. Step 317b can comprise creating a digital signature for the response 209 using the server private key 105c and cryptographic algorithms 141.

Petitioner Samsung Ex-1038, 0097

Additional details regarding steps 317a and 317b are depicted and described in connection with Figure 5a below. Note that step 317a and/or step 317b may optionally be omitted, such that response 209 is transmitted without encryption and/or a signature, and security could be obtained through other means, such as through firewalls 104 and 124, or using a secured network link between module 101 and server 105, such as setting up a virtual private network (VPN) or SSH tunnel between the two endpoints. These alternative means for security at the network layer would likely require additional bandwidth and power consumption for a module 101 and thus may not be adequately efficient. As one example, if module 101 is a wireless module that sleeps for relatively long periods such as every hour (and obtains a new IP address for every wake period), setting up a new VPN between module 101 and server 105 in order to receive send a message from module 101 may not be practical due to the extra drain on a battery 101k for re-establishing the VPN. Or, only portions of steps 317a and 317b could be used, such that a response 209 (or a message 208 received in step 313) is not encrypted but a digital signature is used in the response 209 (or message 208).

After completing steps 317a and 317b, at step 209a, server 105 can send response 209 from (a) the source port utilized to receive message 208 to (b) a destination IP:port. The destination IP:port can comprise the source IP:port in message 208 as received by server 105, and the destination IP:port can represent the external interface of a firewall 104. In other words, server 105 may send response 209 from server IP:port 207 to the source IP:port received in message 208, which could represent the source IP:port on a wireless network firewall 104, wherein the source IP:port on the wireless network firewall 104 contains the firewall IP address 210. The wireless network firewall 104 could forward the response 209 to module IP:port 204. As contemplated herein, server 105 can send response 209 as soon as practical after receiving message 208, and in any case response 209 should be sent before the expiration of a firewall port binding timeout value 117 associated with firewall 104. According to a preferred exemplary embodiment, response 209 is sent by server 105 within 1 second of receiving message 208. After completing step 209a as illustrated in Figure 3b, server 105 can return to step 312 and listen for or monitor for additional incoming messages 208 from modules 101.

Petitioner Samsung Ex-1038, 0098

Figure 4

Figure 4 is a flow chart illustrating exemplary steps for a server to process a message, including verifying a module's identity and decrypting data, in accordance with exemplary embodiments. The steps illustrated in Figure 4 may comprise step 315 and step 316 illustrated in Figure 3 above. Server 105 can receive message 208 using IP:port 207, as illustrated in Figure 2. Message 208 can be formatted according to the UDP protocol or UDP Lite protocol, although other possibilities exist as well without departing from the scope of the present invention

At step 407, server 105 can process the packet using the appropriate transport layer protocol, such as UDP. In this step 407, the body of the packet comprising message 208 can be extracted, and a checksum, if any, can be calculated to verify the integrity. Note that if the UDP Lite protocol is utilized, the checksum may optionally only apply to the packet header. At step 408, server 105 can remove channel coding, if present in message 208. Channel coding techniques utilized in step 408 could include block codes and convolution codes, and can use the same channel coding algorithms used in channel coding algorithms implemented by module 101, depicted and described in connection with Figure 5a below. By processing channel coding in step 408, server 105 can correct potential bit errors received in message 208, although channel coding 408 may be optionally omitted. As noted above, the use of channel coding 408 can be preferred in an embodiment, since any bit errors received within module encrypted data 403 in message 208 could break (i) a cryptographic algorithms 141 used by server 105 at subsequent steps 413, and/or (ii) the verification of module digital signature 405 at step 410 below.

At step 409, the server 105 can read and record the module identity 110, if module 110 is included in message 208 as external to module encrypted data 403 as illustrated in an exemplary message 208 in Figure 6a below. Although not illustrated in Figure 4, server 105 can select a module public key 111 for module 101 by querying a module database 105k with module identity 110. Module identity 110 could comprise a string or session identifier, whereby server 105 could derive or track a module identity 110 from one message 208 to the next message 208 using the string or session identifier. By including module identity 110 in a message 208, but external to module encrypted data 403 such as illustrated in Figure 6a below, a server 105 can utilize module identity 110 in order to select a server private key 105c or symmetric key 127 for decrypting module encrypted data 403. According to an exemplary embodiment, a plurality of server private

Petitioner Samsung Ex-1038, 0099

keys 105c could be utilized, where a first private key 105c is used with a first set of modules 101 and a second private key 105c is used with a second set of modules 101. The first and second private keys 105c could use or be associated with different sets of parameters 126. By reading the module identity 110 outside of module encrypted data 403, the module identity 110 can be read before decryption, in order to identify which of the first or second set server private keys 105c that a module 101 sending message 208 is associated with, and thus server 105 can subsequently select the first or second set of server private keys 105c to use when decrypting module encrypted data 403.

Alternatively according to an exemplary embodiment, if server 105 operates in a distributed environment (such as comprising multiple sub-servers 105w as illustrated in Figure 1f), an unencrypted module identity 110, including a possibly a session identifier for module identity 110 within a message 208, can be utilized by a message preprocessor 105y to select the appropriate sub-server 105w to process the message 208. Server 105 using message preprocessor 105y could forward the message 208 to the correct sub-server 105w. At step 410, server 105 can validate and verify the module identity 110 using the module digital signature 405 inserted by module 101 in message 208. As described in Figure 4a above, module digital signature 405 can comprise a secure hash signature or tag, where module 101 generated the hash signature using the module private key 112 and digital signature algorithms 141d. As one example, server 105 can utilize the module public key 111 recorded in memory 105e to securely validate the module digital signature 405 receive in a message 208.

The module digital signature 405 can be verified according to public key infrastructure (PKI) standards such as the National Institute of Standards (NIST) "FIPS 186-4: Digital Signature Standard", or IETF RFC 6979 titled “Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)”. Other PKI standards or proprietary techniques for securely verifying a module digital signature 405 may be utilized as well. If message 208 comprises an initial communication from module 101, at step 412 server 105 can verify that module public key 111 is associated with module identity 110 using a module certificate 122, where certificate 122 includes a signature 123 from a certificate authority 118, as illustrated in Figure 1h. Server 105 could receive certificate 122 before module 101 sends message 208, or server 105 could query module 101 or another server for certificate 122 after receiving message 208. Server 105 could use digital signature algorithms 141d to compare a secure hash calculated

Petitioner Samsung Ex-1038, 0100

using (i) a first certificate 122 and/or public key from module 101 and (ii) a second certificate and/or public key from certificate authority 118 or another server, in order to confirm that module public key 111 is associated with module identity 110, where module identity 110 was read from message 208 in step 409. The secure hash could also be calculated using module public key 111 and a public key from certificate authority 118, and other possibilities using PKI exist as well for server 105 to confirm module public key 111 is associated with module identity 110 at step 412.

Steps 409 and 410 are not required to utilize the efficient techniques described herein, and may optionally be omitted. As one example, security could be maintained at the network layer through the use of wireless network firewall 104 and server network firewall 124, such that only an inbound message 208 to server 105 could be received by server 105 after security methods are applied at the network layer or application layer. Note that if (A) module encrypted data 403 includes module identity 110 and/or module digital signature 405, then (B) steps 409 and/or 410 may also take place after step 413, where server 105 (i) first decrypts module encrypted data 403 and can then (ii) verify module identity 110 by performing steps 409 and 410 after step 413. If module encrypted data 403 utilizes a symmetric cipher 141b, then a module identity 110 can preferably be external to module encrypted data 403 so that server 105 can select the appropriate symmetric key 127 used by module 101 in order to decipher module encrypted data 403 (since a plurality of modules 101 may communicate with server 105 concurrently).

After verifying module digital signature 405 in step 410, server 105 can record an authenticated module encrypted data 403 from module 101 received in message 208. At step 413, server 105 can decrypt module encrypted data 403 using cryptographic algorithms 141 and either (i) server private key 105c as a decryption key with asymmetric ciphering 141a or (ii) symmetric key 127 with symmetric ciphering 141b. A symmetric key 127 may be stored in a module database 105k, as noted in Figure 1f above. If a symmetric key 127 is used at step 413, the symmetric key 127 could be (i) sent by server 105 in a response 209 or (ii) received by server 105 in a prior message 208, before the message 208 illustrated in Figure 4 was received by server 105.

With an asymmetric ciphering 141a scheme used in a module encrypted data 403 and by cryptographic algorithms 141 at step 413, server 105 can decrypt module encrypted data 403 using (i) server private key 105c and (ii) RSA algorithms 153, elliptic curve cryptography (ECC) algorithms 154, or other algorithms for public key cryptography. The use and application of RSA

Petitioner Samsung Ex-1038, 0101

algorithms 153 and cryptography are described within IETF RFC 3447, among other published standards. The use and application of ECC cryptography and algorithms are described within IETF RFC 6637, among other published standards. ECC algorithms 154 may be preferred in order to maintain high security with small key lengths, compared to RSA, in order to minimize the message lengths, radio frequency spectrum utilization, and processing power required by module 101. Thus, the use of ECC algorithms within a decryption algorithm at step 413 may help conserve the life of a battery 101k of module 101 while maintaining the objective of securing system 100. Note that module encrypted data 403 may also include a security token 401 (not shown in Figure 4, but shown in Figure 5a), which could comprise a random string, and thus each module encrypted data 403 received by server 105 in message 208 may be reasonably considered unique and thus robust against replay attacks.

With a symmetric ciphering 141b scheme used in a module encrypted data 403 and by cryptographic algorithms 141 at step 413, server 105 can decrypt module encrypted data 403 using (i) symmetric key 127 and (ii) a symmetric cipher 141b such as AES 155, Triple DES, or similar secure symmetric ciphers. As one example, by using ECC cryptography and ECIES, server 105 could decrypt module encrypted data at step 413 by using the steps outlined in Figure 3, titled "ECIES Encryption Functional Diagram" in "A Survey of the Elliptic Curve Integrated Encryption Scheme" by Martinez et al in the Journal of Computer Science and Engineering, Volume 2, August 2010, page 11, (herein incorporated by reference). Other possibilities exist as well without departing from the scope of the present invention. Server 105 can utilize step 413 illustrated in Figure 4 to extract the plaintext, or decrypted data within module encrypted data 403.

After decrypting module encrypted data 403, server 105 can read the resulting data within message 208, which could comprise a server instruction 414. The server instruction 414 can represent the purpose of the message 208 for server 105. Server instruction 414 could comprise a plurality of different procedures for server 105, such as an "update" with sensor data, a "query" for data or instructions from server 105 or M2M service provide 108, a "notification" of state or condition at module 101 such as an alarm or error, a "configuration request" where module 101 seeks configuration parameters, a "software request" where module 101 request updated software or routines, a "registration" message where module 101 periodically registers with server 105, etc. Thus, server instruction 414 can comprise the purpose module 101 sends message 208. In addition, server instruction 414 could comprise a "confirmation", where module 101 sends a "confirmation"

Petitioner Samsung Ex-1038, 0102

in a second message 208 after receipt of a response 209, where response 209 could include a module instruction 502 (below), and the "confirmation" in this second message 208 could signal server 105 that the module instruction 502 had been properly executed. As contemplated herein, the term "Message (update)" can comprise a message 208 that includes a server instruction 414 of "update", and the term "Message (confirmation)" can comprise a message 208 that includes a server instruction 414 of "confirmation", etc.

As examples for server instruction 414, an "update" could be used to periodically notify server 105 of regular, periodic sensor data 305 acquired by a sensor 101f. An "update" for server instruction 414 may also comprise a periodic report regarding monitored unit 119 or information regarding a state, condition, or level for an actuator 101y. A "query" for server instruction 414 could comprise module 101 querying server 105 for data from a module database 105k, where the data could be associated with monitored unit 119, wireless network 102, an element within module 101 such as an actuator setting. A "notification" for server instruction 414 could comprise module 101 notifying server 105 that an alarm or error condition has occurred, such as a sensor measurement exceeds a threshold value or another error condition such as loss of contact with monitored unit 119. A "configuration request" for server instruction 414 could comprise module 101 requesting server 105 for configuration parameters or a configuration file. Other possibilities for server instruction 414 exist without departing from the scope of the present invention.

At step 415, server 105 can process the server instruction 414. If server instruction 414 comprises an "update", then sensor data, or other data in server instruction 414 including potentially a new symmetric key 127 generated by module 101, could be recorded in module database 105k, Other applications may subsequently access the sensor data for generating reports or making decisions regarding monitored unit 119. If server instruction 414 comprises a "query", then server 105 could execute the query at step 415. If server instruction 414 comprises a "notification" of an alarm, then step 415 could initiate procedures for alarm notification to 3rd parties or alarm resolution. Other possibilities for processing a server instruction 414 at step 415 exist without departing from the scope of the present invention.

Petitioner Samsung Ex-1038, 0103

Figure 5a

Figure 5a is a flow chart illustrating exemplary steps for a server to process a response for a module, including sending and signing a module instruction, in accordance with exemplary embodiments. The steps illustrated in Figure 5a may comprise step 317a and step 317b illustrated in Figure 3 above. Since message 208 and response 209 may traverse the public Internet 107, a module 101 and a server 105 may prefer to take additional steps to sending plaintext in packets in order to maintain security of a system 100. Server 105 can process a response 209 to a message 208 from module 101 using a module public key 111 and a server private key 105c, according to a preferred exemplary embodiment. If a symmetric cipher 141b is utilized within cryptographic algorithms 141, then server 105 may also utilize a symmetric key 127 to encrypt data within a response 209. Note that the security methods described herein are optional, and message 208 and response 208 can be sent without any or all of the additional security steps described herein, but the use of these security steps may be preferred.

After receiving message 208 as illustrated in Figure 2, server 105 can prepare an acknowledgement 501. The acknowledgement 501 can be a simple text, binary, or hexadecimal string to confirm that message 208 has been received and/or processed by server 105. Since message 208 may be transmitted via a UDP or UDP Lite packet, module 101 may preferably utilize a reply message from server 105 containing acknowledgement 501, in order to confirm message 208 has been received by server 105. Alternatively, if TCP is used to transmit message 208, an acknowledgement 501 may be used at the application layer of the Open Systems Interconnection (OSI) model, wherein a simple TCP ACK message may operate at the lower transport layer than the application layer. UDP may be preferred over TCP in order to reduce processing resources for module 101 and server 105, especially considering the relatively small and comparably infrequent messages sent between a module 101 and a server 105 (when compared to web browsing and considering module 101 may have a battery 101k that may preferably last for weeks or longer without recharging). In processing a response 209, server 105 may optionally add a security token 401, which could be a random number 128a, or a randomly generated text, binary, or hexadecimal string. Security token 401 could be a random number 128a or string that is included in response 209 in order to make each response 209 unique and thus avoid any replay attacks when response 209 traverses Internet 107. Note that a message 208 may also preferably include a security token 401.

Petitioner Samsung Ex-1038, 0104

In other words, the use of security token 401 can ensure to a high level of certainty that each response 209 will be different and thus the data within response 209 would not be sent more than once. Note that security token 401 may be generated by module 101 in message 208, and in this case server 105 can use the same security token received in message 208. Security token 401 can alternatively be generated by server 105 and different than any security token 401 received in message 208. As one example, server 105 could use a first security token 401 received in message 208 to process a second security token 401, where the second security token 401 is generated using (i) a pre-agreed algorithm between module 101 and server 105 and (ii) the first security token 401 as input into the pre-agreed algorithm. Security token 401 illustrated in Figure 5a can be derived or processed by using message 208 in accordance with preferred exemplary embodiments.

Server 105 may also optionally add a module instruction 502 when preparing a response 209. The module instruction 502 could be a string that contains instructions or configuration parameters for module 101, such as an order to change state, parameters regarding the monitoring of monitored unit 119, server names or addresses, radio frequency parameters, wireless network 102 authentication parameters or keys, keys for communication with server 105 or M2M service provider 108, etc. Module instruction 502 may also comprise an instruction to change the state of actuator 101y, a timer value, a sensor threshold value, the threshold for an alarm state, and information for display at a user interface 101j, an instruction to sleep, etc. Module instruction 502 may further comprise an updated module private key 112, and updated server public key 114, or the address or name of a new server 105 added to M2M service provider 108. According to an exemplary preferred embodiment, a module instruction 502 could comprise a "key generation" instruction, where module 101 generates a new pair of a module private key 112 and a module public key 111, utilizing the exemplary steps and procedures illustrated in Figures 5b below. The "key generation" 608 module instruction 502 (illustrated in Figure 6a below) could be used to create new keys for a new purpose (such as connecting to a new wireless network 102 or communicating with a new server 105), while the existing keys used to communicate with server 105 could remain operable or be deprecated at a later time. Alternatively, an existing module public key 111 could be deprecated or become invalid once server 105 sends a "key generation" module instruction 502.

In order to control module 101, server 105 would normally need to include module instruction 502 in the response 209 only after receiving message 208, since the server 105 would normally not be able to send messages to a module 101 at arbitrary times, such as before a message

Petitioner Samsung Ex-1038, 0105

208 has been received by the server 105. The reasons include (i) the module may normally be in a sleep or dormant state, in order to conserve battery life or power consumption, where an unsolicited incoming Internet packet from server 105 would not be received by module 101, and (ii) a wireless network 102 (or equivalent wired network that a wired module 101 could connect with) may frequently include a firewall 104. Firewall 104 could prevent packets from the Internet 107 from reaching module 101 unless module 101 had previously first sent a packet to server 105 within a firewall port-binding timeout period 117 of firewall 104. The port-binding timeout period of a firewall 104 may be an exemplary period such as 20 – 60 seconds for UDP packets and several minutes for TCP packets. Note that module instruction 502 may optionally be omitted, such that (b) some response 209 messages may include module instruction 502, and (b) other response 209 messages may omit module instruction 502, but include an acknowledgement 501 to message 208. Also note that according to an exemplary embodiment described herein, the use of optional strings or steps can be depicted in Figures 4 and 5a through the use of dashed lines for the various elements illustrated.

Server 105 may then use as input the acknowledgement 501, security token 401, and module instruction 502, including optional data and parameters 126, into cryptographic algorithms 141 at step 503. The cryptographic algorithms 141 at step 503 can utilize either (i) module public key 111 as an encryption key if asymmetric ciphering 141a is utilized, or (ii) a shared symmetric key 127 if a symmetric cipher 141b is utilized, such as AES 155 ciphering. The output of cryptographic algorithms 141 at step 503, using acknowledgement 501, security token 401, and module instruction 502, plus optional data and parameters 126, as input, can be server encrypted data 504, as illustrated in Figure 5a. Server encrypted data 504 could be a string or number, including a text, binary, or hexadecimal string or series of numbers or bits, and other possibilities for the formal of server encrypted data 504 exist as well, including a file, without departing from the scope of the present invention. By using module public key 111 and/or symmetric key 127 in the cryptographic algorithms 141 at step 503, server encrypted data 504 may only be reasonably decrypted by module 101 using module private key 112 and/or symmetric key 127. Thus the response 209 transmitted across an Internet 107 may be reasonably considered secure and only reasonably decrypted by module 101.

Server 105 can then process server encrypted data 504 by appending or including server identity 206. Note that server identity 206 can be appended or included after the operation of step

Petitioner Samsung Ex-1038, 0106

503, since the server identity 206 may optionally be openly readable within a response 209 transmitted or sent to module 101. As one example, server identity 206 could comprise IP address 106 as a source IP address in response 209, which would be openly readable on the Internet 107 since a valid packet must have a source and destination IP address. Additional details on an exemplary structure of response 209 are illustrated in Figure 6a below. By including server identity 206 after encryption at step 503, the module can read the server identity 206 and verify a digital signature within response 209 without having to first decrypt data within response 209 using the module private key 112 or symmetric key 127. Note that server identity 206 could alternatively be included within server encrypted data 504, such that step 505 takes place before step 504. In other words, including server identity 206 external to a server encrypted data 504 can be used by module 101 to select the proper server public key 114 when verifying a digital signature in response 209.

Server 105 can then process a server digital signature 506 using the server private key 105c. The server digital signature 506 can be processed according to public key infrastructure (PKI) standards such as the National Institute of Standards (NIST) "FIPS 186-4: Digital Signature Standard" (which is hereby incorporated herein by reference), or IETF RFC 6979 titled "Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)" (which is hereby incorporated herein by reference). The use of a server digital signature 506 can be processed according to the description of a digital signature according to the Wikipedia entry for "Digital Signature" as of September 9, 2013, which is incorporated by reference herein in its entirety. Also note that other uses of a digital signature as contemplated within the present invention may refer to the above three references and related standard techniques for processing and creating digital signatures. Other PKI standards or proprietary methods for securely generating a server digital signature 506 may be utilized as well.

According to a preferred exemplary embodiment, ECC algorithms for generating server digital signature 506 may be utilized in order to minimize the key length compared to RSA algorithms. Server digital signature 506 may comprise a secure hash signature using a hash algorithm such as secure hash algorithm 1 (SHA-1), or subsequent standards such as SHA-2 and SHA-3, and other possibilities exist as well. Server digital signature 506 is illustrated in Figure 5a as being processed after server encrypted data 504, but server digital signature 506 may also optionally be included in server encrypted data 504. Step 506 may also take place before step 505.

Petitioner Samsung Ex-1038, 0107

Also note that server digital signature 506 may preferably be included in a response 209 before module 101 begins either (i) utilizing a symmetric key 127 shown in step 413 to encrypt a module encrypted data 403, or (ii) accept or process a module instruction 502. After including server digital signature 506 in a first response 209 that uses asymmetric ciphering 141a, server 105 may omit server digital signature 506 in a second subsequent response. The second subsequent response could be a case where (i) server encrypted data 504 utilizes a symmetric key 127 for ciphering (where server 105 received the symmetric key 127 in a message 208 that utilized asymmetric ciphering 141a as illustrated in Figure 4 above) and (ii) expiration time 133 of symmetric key 127 has not transpired.

Although energy may be conserved for a module 101 utilizing the exemplary steps illustrated in Figure 5a and elsewhere herein, a high level of security is desirable for many "machine-to-machine" applications. A module 101 may be utilized for industrial applications or health monitoring, where the receipt of unauthorized module instructions 502 from 3rd parties could results in damages or losses. Without proper security that can include the steps illustrated in Figure 5a, response 209 could include a module instruction 502, and module 101 could potentially receive commands or instructions from sources other than server 105, such as hackers.

Figure 5b

Figure 5b is a flow chart illustrating exemplary steps for a server to communicate with a module that has derived a public key and private key, in accordance with exemplary embodiments. In order to utilize communications secured with PKI techniques such as private keys, public keys, certificates, and identities, a module 101 may preferably obtain or generate these keys and utilize a module identity 110 and/or a certificate 122 in a secure manner. Given that a plurality of modules 101 may be deployed in potentially remote places, without frequent contact with end users or technicians, the use of secure PKI techniques for a module 101 can create a significant set of challenges for the generation of module public key 111 and module private key 112, as well as properly and securely obtaining a certificate 122 with an module identity 110. Using conventional technology, significant challenges and costs can be incurred when (i) module 101 has already been

Petitioner Samsung Ex-1038, 0108

deployed, such as collecting data from a monitored unit 119, and (ii) module 101 needs to utilize a new set of module private key 112 and module public key 111.

Exemplary embodiments that include derivation or processing of a new module private key 112 and module public key 111 may utilize the particular steps and procedures contemplated herein, in order to minimize any potential human intervention (with related costs) while continuing to maintain or also enhance security, compared either (i) externally generating module private key 112, and/or (ii) continuing to use the same module private key 112 for the lifetime of module 101. Over a long period of operating time for a module 101, such as several years or longer, there may be many reasons module 101 may need a new pair of PKI keys, such as (i) expiration of a certificate 122, or the certificate 122 of a parent signature authority, (ii) the transfer of ownership or control of module 101, where the prior ownership could have direct or indirect access to the module private key 112, (iii) supporting a new server 105 that has different security requirements or a different set of parameters 126 (longer keys, different ECC curves, different cryptographic algorithms 141, etc.), and/or (iv) revocation of a public key in a chain of signatures 123 associated with a certificate 122. In the case of (ii) above, new ownership of module 101 may require a module 101 to utilize a new module private key 112 since the old ownership may have access to an old module private key 122. In the case of (iii) above, a new server 105 may require a pair of public/private keys incompatible with a prior set of public/private keys utilized by module 101 and/or a certificate 122 for module 101.

Other possibilities exist as well for reasons why a module 101 and/or server 105 may prefer for a module 101 to utilize a new module public key 111 and new module private key 112. In an exemplary embodiment, module 101 may generate a new public/private key periodically in order to enhance the security of a system 100. A benefit of a system 100 supporting periodic generation of keys by module 101 is that the key length can be shortened in order to obtain a similar level of security, and the processing power and energy consumption, possibly from a battery 105k, can be reduced through the use of shorter key lengths. In other words, over time such as several months or years, the use of a plurality of different pairs of public/private keys for module 101 with shorter key lengths can be both more secure and energy efficient than using a single pair of public/private keys with a longer key length for the lifetime of module 101. Shorter key lengths may also be more compatible with processing power constraints of a module 101. Thus, in exemplary embodiments,

Petitioner Samsung Ex-1038, 0109

module 101 and/or server 105 may prefer for module 101 to periodically generate new public and private keys.

The general approach adopted by most mobile phone networks over the past two decades has been founded upon the use of a pre-shared secret key recorded in SIM cards, such as the Ki pre-shared secret key in 2G and 3G networks. That approach may work for mobile phones, where the SIMs can often be easily replaced, but the use of a pre-shared secret key in a SIM may not be suitable for a module 101 and M2M service provider 108 for many circumstances. As one example, significant costs may be incurred by swapping out a SIM card for already deployed modules 101, especially if they are in remote locations or continually moving such as a tracking device on a container, pallet, truck, or automobile. In an exemplary embodiment, a module 101 may preferably record multiple pairs of public/private keys 111/112 for various and different functions, such as connecting to different servers 105, connecting to different wireless networks 102, etc. As contemplated herein, recording more than one public/private key 111/112 can comprise module 101 recording a plurality of pairs of module public keys 111 and module private keys 112. In exemplary embodiments, one pair comprising a first module public key 111 and a first module private key 112 can be identified or selected from a different pair comprising a second module public key 111 and a second module private key 112 using a module public key identity 111a.

The number of pairs of public/private keys useful to a module 101 concurrently could be several, such as an exemplary three or more actively used public/private keys, although other possibilities exist as well. Manually trying to change or add a new SIM card each time a new security key is required may not be efficient or feasible. Or in another exemplary embodiment, the multiple pairs of private and public keys could be used in sequence, such that module 101 with server 105 utilizes a single module public key 111 and module private key 112 at any given point in time. In the case where module 101 (i) uses more than one private key 112 and more than one public key 111 and (ii) derives at least one module private key 112 and one public key 111 during the lifetime of module 101, this case may be considered module 101 using a plurality of module private keys 112 and using a plurality of module public keys 111. In the case where module 101 derives or generates more than one module private key 112 and module public key 111 during the lifetime of module 101, this case may be considered module 101 deriving a plurality of module private keys 112 and module public keys 111, or also deriving a plurality of pairs of module public keys 111 and module private keys 112. The various pairs in the plurality may use different sets of

Petitioner Samsung Ex-1038, 0110

parameters 126 or the same set of parameters 126. The plurality of module public keys 111 and module private keys 112 can be processed by a CPU 101b with key pair generation algorithms 141e and a random number generator 128. The random number generator 128 can use input from a sensor 101f, a radio 101z, and/or temporary random seed file.

In exemplary embodiments, module 101 can use a module public key 111 for sending a module encrypted data 403 or receiving a server encrypted data 504 by either (i) sending the module public key 111 to a server 105 in order to allow the module encrypted data 403 to be decrypted (such as using a step 413) or the server encrypted data 504 to be encrypted (such as using a step 503), or (ii) inputting the module public key 111 into a key derivation function 141f in order to derive or process a derived shared secret key 129b, which could be used with a symmetric key 127. Other possibilities exist as well for module 101 to use its own public key 111 with cryptographic algorithms for communicating with a server 105.

Figure 5b illustrates exemplary steps that can be performed with module 101, including using a module program 101i, for generating, deriving, and/or updating a module public key 111 and module private key 112. The steps illustrated in Figure 5b include both (i) an "initial" or "startup" case where module 101 has not previously derived keys (or keys not internally derived may not have been loaded), and (ii) a subsequent or "follow on" time where module 101 can generate or derive keys after keys were initially obtained or derived. Note that efficient and secure methods and systems contemplated herein, including in Figure 5b, may also be utilized with a regular consumer mobile phone, or smartphone, as a module 101. Mobile phones as module 101 can benefit from (i) deriving a module public key 111 and a module private key 112, (ii) sending module encrypted data 403 in a message 208 using the derived keys, and (iii) receiving a server encrypted data 504 in a response 209 also using the derived keys. In the exemplary embodiment where module 101 comprises a mobile phone, then sensor 101f may comprise a microphone and actuator 101y may comprise a speaker, and other possibilities exist as well to those of ordinary skill in the art for module 101 to comprise a mobile phone.

At step 511, during manufacturing of module 101, including manufacturing of sub-components such as a circuit board, assembly of hardware components illustrated in Figure 1b, etc., a module identity 110 could be written into the hardware, and could comprise a serial number, International Mobile Equipment Identity (IMEI) number, Ethernet MAC address, or a similar

Petitioner Samsung Ex-1038, 0111

persistent identification for a module 101. An IEMI number may be used with a mobile phone as module 101, in a preferred embodiment. For security purposes, the module identity 110 may preferably be written into a read-only location, such as a readable location on a system bus 101d, which could also comprise a ROM 101c. Recording and utilizing module identity 110 is also depicted and described in connection with Figure 1e, Figure 2, and elsewhere herein. Alternatively, module identity 110 could be recorded in a non-volatile memory such as a flash memory 101w.

At step 512, module 101 can be distributed to end users and also installed with a monitored unit 119. If module 101 is a mobile phone, then monitored unit 119 could be a person that carries the mobile phone. Also note that a monitored unit 119 could be omitted, and a module 101 could use the techniques contemplated herein. At step 513, a shared secret key 510, parameters 126, and a server address 207 can be recorded in a nonvolatile memory 101w. Parameters 126 may comprise settings for a cryptographic algorithms 141 as illustrated in Figure 1g, including (i) key lengths, (ii) algorithms to utilize for key generation or ciphering, such as selecting RSA algorithms 153 or ECC algorithms 154, (iii) a specific secure hash algorithm 141c to utilize, such as SHA-256 or SHA-3, (iv) an expiration date of the module public key 111, (v) a maximum time value for an expiration time 133 associated with a symmetric key 127, (vi) a ECC parameters 137 or an ECC standard curve 138 as parameters 126 in Figure 1h, (vii) the specification of or values for a padding scheme for use with a digital signature algorithms 141d, and/or similar or related values for using cryptographic algorithms 141d . Although not illustrated in Figure 5b, at step 512 a configuration file could also be loaded into non-volatile memory, where the configuration file includes a plurality of fields specifying the operation of module 101. The shared secret key 510, parameters 126, and server address 207 could be included in a configuration file.

Continuing at step 513, server identity 206 could be utilized in place of or in addition to server address 207, and in this case module 101 can later perform a DNS or DNSSEC lookup using server identity 206 in order to obtain server address 207 for use in a message 208, such as the destination address. Shared secret key 510 and server address 207 (or server identity 206) could also be recorded in a ROM 101c at step 513. Step 513 may also be performed concurrently with step 511 or step 512. According to an exemplary embodiment, a manufacturer may perform step 513 and in this case step 513 could take place concurrently with step 511. In another embodiment, a distributor of module 101 could perform step 513 and in this case step 513 could take place concurrently with step 512. Alternatively, step 513 may be performed by a technician or end user

Petitioner Samsung Ex-1038, 0112

after manufacturing and distribution and before module 101 begins collecting sensor data with a monitored unit. Other possibilities exist as well for the sequence of steps 511 through 513 illustrated in Figure 5b without departing from the scope of the present invention.

Note that step 513 may take place multiple times during the lifetime of a module 101, and in this case (a) the first time step 513 is conducted, step 513 could be conducted concurrent with steps 511 or 512, and (b) a subsequent time step 513 is conducted, step 513 could be conducted after the receipt of a response 209, where the response 209 includes a second shared secret key 510, server address 207, and also potentially a new module identity 110. In other words, although not illustrated in Figure 5b, a module 101 could return to step 513 from later steps upon the equivalent of a "factory reset", or similar command where flash memory 101w and other nonvolatile memory would be cleared. In an exemplary embodiment where step 513 takes place a second time may potentially be the transfer of ownership or control of module 101, or a another embodiment where step 513 takes place a second time could be the upload of new firmware that is incompatible with a previous configuration file. In any case, shared secret key 510 can preferably be uniquely associated with module 101 (i.e. any given shared secret key 510 may belong only to an individual module 101).

Shared secret key 510 may comprise a pre-shared secret key 129a, as described in Figure 1e. If module 101 has already derived a module private key 112 and module public key 111 (such as when step 513 is being conducted at a second or additional time as contemplated in the previous paragraph), then shared secret key 510 may comprise (i) a key received in a server encrypted data 504 including possibly a symmetric key 127, or (ii) a derived shared secret key 129b. Derived shared secret key 129b could be obtained from using a key derivation function 141f and module public key 111 and server public key 114, using a module public key 111 that has already been derived or used by module 101 (such as if at least one module private key 112 and module public key 111 had already been used or derived before step 513).

As contemplated herein in an exemplary embodiment, an first module private key 112 and first module public key 111 could be derived outside module 101 and loaded into a nonvolatile memory such as flash memory 101w at a prior time before step 513, and the shared secret key 510 could be received by module 101 using the first module private key 112 and module public key 111 (such as receiving the shared secret key 510 in a server encrypted data 504 using the first module

Petitioner Samsung Ex-1038, 0113

private key 112 which had been loaded). Step 513 could then comprise a later time after the server encrypted data 504 has been received that includes the shared secret key 510, where module 101 may (i) prefer to begin utilizing keys that module 101 internally derives using cryptographic algorithms 141 instead of (ii) continuing to use the first module public key 111 and module private key 112 that were derived outside of the module 101, such as possibly loaded into a nonvolatile memory from an external source.

In the embodiment where shared secret key 510 has not been received by module 101 in a server encrypted data 504, shared secret key 510 could be obtained and loaded by a distributor, installer, or end user into a nonvolatile memory such as flash memory 101w in the form of a pre-shared secret key 129a, where pre-shared secret key 129a was obtained using a module identity 110 and pre-shared secret key code 134 as depicted and described in connection with Figure 1e above. Module 101 could also utilize a first pre-shared secret key 129a, including a first pre-shared secret key 129a entered by potentially a distributor, installer, or end-user described in Figure 1e, to derive shared secret key 510. Other possibilities exist as well for shared secret key 510, and shared secret key 510 can be useful for the proper identification and/or authentication of module 101 upon module 101's generation of a private key 112 and public key 111, as described below including step 517. If module 101 is a mobile phone, as contemplated herein, shared secret key 510 could be loaded by a distributor or company selling or servicing the mobile phone, or shared secret key 510 could be obtained by the end user or subscriber accessing a web page associated with a mobile operator for a wireless network 102 associated with the mobile phone and/or SIM card.

Also note that as contemplated herein, an initial module private key 112 and initial module public key 111 could be recorded into nonvolatile memory at step 513. For example, a manufacturer, distributor, installer, technician, or end-user could load the initial module private key and initial module public key 111, where the initial module public key 111 would be utilized to authenticate at step 517 a subsequent set of public/private keys derived by module 101 at step 515. In this case, the initial module public key 111 and/or initial module private key 112 described in the previous two sentences could comprise the shared secret key 510. One reason the initial module private key 112 with the initial module public key 111 would comprise a shared secret key 510 may be that (i) the initial module private key 112 and initial module public key 111 together have been "shared" in the sense that the initial module private key 112 has been located outside module 101 and in possession of an entity such as the manufacturer, distributor, installer, technician, or end-user

Petitioner Samsung Ex-1038, 0114

in order to load the initial module private key into a nonvolatile memory such as flash memory 101w (and initial module public key 111 is subsequently shared with server 105), (ii) the initial module private key 112 and initial module public key 111 can be used to authenticate a subsequent message 208 containing a public key internally derived by the module at step 517 below, and (iii) the initial module private key 112 would remain "secret" in the sense that it is not publicly shared (i.e. an initial or "loaded" module private key 112 could preferably kept confidential and thus part of a "shared secret key"). Thus, Figure 5b also contemplates an embodiment where shared secret key 510 at step 513 comprises an initial public/private key pair for module 101 that is not internally derived by module 101, including keys derived at step 515.

Note that the contemplation of the use of shared secret key 510 as a pre-shared secret key 129a within the present invention may be different than the use of a pre-shared secret key within a SIM card as commonly supported by wireless networks 102 with mobile phones in 2013. Specifically, as depicted and described in connection with Figure 1e and elsewhere herein, the shared secret key 510, either (i) comprising a pre-shared secret key 129a or (ii) derived from a pre-shared secret key 129a, may be moved by CPU 101b into a volatile memory such as RAM 101e, with subsequent access by cryptographic algorithms 141. In contrast, the pre-shared secret key within a SIM card for mobile phones is usually designed to prevent movement of the pre-shared secret key within a SIM into RAM 101e.

If a SIM card is present within module 101, and the SIM card contains a pre-shared secret key, such as Ki, then as contemplated herein, shared secret key 510 may be derived using the SIM card and Ki. As one example, module 101 could (i) utilize a RAND message, potentially received from a 3G or 4G mobile network such as wireless network 102, and (ii) input the RAND into the SIM card and receive a response RES (or SRES), and utilize the string in RES to process or derive a shared secret key 510. Response RES could also comprise a shared secret key 510. Server 105 could also submit the same RAND associated with the SIM card and Ki to wireless network 102, and receive the same RES as obtained by module 101. By both module 101 and server 105 having the same RES value, they can follow a pre-agreed series of steps to use the same RES in order to derive a commonly shared secret key 510 (or the shared RES could comprise a shared secret key 510). In one embodiment where module 101 includes a SIM card for a wireless network 102, such as a 4G LTE network, module 101 and server 105 could both utilize a key derivation function 141f, using the same RES as input, in order to derive the same shared secret key 510.

Petitioner Samsung Ex-1038, 0115

At step 514, module 101 can read module identity 110 using a read-only address. Module 101 can read module identity 110 directly from read-only hardware address by using system bus 101d, including from a ROM 101c, or module 101 can read module identity 110 from a nonvolatile memory such as a flash memory 101w. Thus, the read-only address could comprise an address accessible on system bus 101d that is designated read-only for a period of time. The module identity 110 could be recorded into a flash memory 101w by module 110 after a prior read of module identity 110 from a read-only address. In this case (module 101 taking the step described in the previous sentence), reading module identity 110 from the nonvolatile memory at step 514 can also comprise module 101 reading module identity 110 using a read-only address. Thus, although module 101 may read module identity 110 from a flash memory 101w, if (a) module 101 initially utilized a read-only address to record the module identity 110 into the flash memory 101w, then (b) reading module identity 110 from the flash memory 101w could comprise using a read-only address to read module identity 110. Other possibilities exist as well, such as the address that includes module identity 110 in either (i) a nonvolatile memory such as a ROM 101c or (ii) an address accessible on system bus 101d, could be designated for a period of time as available for a read-only operation. Step 514 could also take place after step 515 below.

At Step 515, module 101 can derive module private key 112 and a corresponding module public key 111 using (i) random number generator 128, (ii) parameters 126, (iii) cryptographic algorithms 141, and/or (iv) a key pair generation algorithm 141e. Module 101 at step 515 and elsewhere in the present invention can be a mobile phone such as a smartphone. Private key 112 and corresponding module public key 111 can be derived according to a wide range of parameters 126, and can utilize different algorithms for different pairs of keys, such as RSA 153 or ECC 154. Key derivation at step 515 could generate keys of various lengths, such as 2048 bits with RSA 153 or 283 bits with ECC 154, and other possibilities exist as well. If using ECC 154 to derive a pair of keys for module 101, step 515 could also accommodate the use of different elliptic curves for compatibility with server 105, such as the use of odd-characteristic curves, Koblitz curves, and making sure the derived keys by module 101 use a compatible or identical elliptic curve or defined elliptic curve equation as server 105, etc. Module 101 can use ECC parameters 137 or an ECC standard curve 138 in a parameters 126 to derive module private key 112 and/or module public key 111.

Petitioner Samsung Ex-1038, 0116

Deriving keys in step 515 could also comprise using values such as constants or variables in a parameters 126 to define an elliptic curve equation for use with an ECC algorithm 154. The values or constants to define an equation for an elliptic curve could be input into a key pair generation algorithms 141e in the form of ECC parameters 137 or an ECC standard curve 138. In an exemplary embodiment, where a parameters 126 does not include constants and variables for defining an elliptic curve equation, a key pair generation algorithms 141e could use pre-defined elliptic curves with ECC algorithms 154 such as standardized, named curves in ECC standard curve 138 including exemplary values such as sect283k1, sect283r1, sect409k1, sect409r1, etc. Exemplary, standardized named curves, as opposed to module 101 and server 105 using an internally generated elliptic curve equation using parameters 126, are also identified as example curves in IETF RFC 5480, titled "Elliptic Curve Cryptography Subject Public Key Information". Thus, module 101 could use either standardized elliptic curves, or a separate defined elliptic curve equation as specified in a parameters 126.

The curve for module 101 to utilize in deriving module public key 111 and module private key 112 at step 515 could be specified in parameters 126. Consequently, the parameters of keys generated by module 101 at step 515 (including key length or algorithms utilized) may be selected based upon the requirements of the application and can be included in a parameters 126. When deriving keys at step 515, module 101 may also preferably utilize data from sensor 101f, radio 101z, a bus 101d, a physical interface 101a, memory 101e, and/or a clock in order to generate a seed 129 for random number generator 128, or random number generator 128 could utilize these inputs directly. A random number 128a can be input into key pair generation algorithm 141e in order to derive the module public key 111 and module private key 112. Note that with ECC algorithms 154, a module private key 112 can be a random number 128a in one embodiment, and the module public key 111 can be derived with a key pair generation algorithms 141e using the module private key 112 comprising the random number 128a.

Upon key derivation at step 515, module private key 112 and module public key 111 can be recorded in a nonvolatile memory 101w. Module private key 112 is preferably not transmitted or sent outside module 101. Note that module 101's internal derivation, or processing or creation, of module private key 112 and corresponding module public key 111 can have many benefits. First, module private key 112 does not need to be recorded in any other location than within module 101, and thus may also be considered not shared. Recording module private key 112 only within module

Petitioner Samsung Ex-1038, 0117

101 avoids potential security risks of (i) storing or recording module private key 112 in other locations, such as with module provider 109, M2M service provider 108, or an installer or end user of module 101, and (ii) transferring module private key 112 to and/or from these other locations. One security risk from storage of module private key 112 outside module 101 is that unauthorized 3rd parties may gain access to the module private key 112.

Also note that over a potential lifetime of a decade or more of operation of module 101, each time a new module private key 112 may be required (for various potential reasons outlined above), the external recording and/or transferring of module private key 112 incurs a potential security risk. Security risks can be compounded if the external location records private keys 112 for a plurality of modules 101. Also, by internally generating private key 112 at step 515, module 101 can overcome significant limitations and costs requiring the distribution of a pre-shared secret key Ki in the form of a SIM card or similar physical distribution of a pre-shared secret key, after module 101 begins operations. In comparison, the use of a shared secret key 510 in the present invention does not require physical distribution of a new shared secret key 510 after module 101 begins operations. Module 101's key derivation could be triggered by either (i) a bootloader program 125, where the bootloader program 125 determines that memory within module 101 does not contain a module private key 112, or (ii) via a module instruction 502 such as a "key generation" command in a response 209 from a server, and other possibilities exist as well.

Note that module 101's generation of keys after deployment and installation may create challenges for authentication of a new module public key 111 with module identity 110, since module 101 may be connecting to server 105 or M2M service provider 108 via the Internet 107. After module 101 creates new module public key 111 and module private key 112 at step 515, at step 516 server 105 can receive a message 208 with the module identity 110, the new module public key 111, and parameters 126. Parameters 126 in message 208 at step 516 can represent the parameters 126 used to generate the module public key 111. The sub-steps for a server 105 to receive a message 208 are also depicted and described in connection with Figure 2 above. Parameters 126 within a message 208 can comprise descriptive values for new module public key 111. Note that at step 516, server 105 does not need to receive new module public key 111 in the form of a certificate 122 (although it could be in the form of a certificate 122). New module public key 111 could be received by server 105 within a string or field within a body 602 of a TCP/UDP packet 601a, illustrated in Figure 6b below. As depicted in step 516 shown in Figure 6b below,

Petitioner Samsung Ex-1038, 0118

message 208 can also optionally include a module public key identity 111a, which can be recorded in module database 105k along with module identity 110 and module public key 111a.

According to an exemplary embodiment, a first source (IP:port) number received in a first message 208 at step 516 can be different than a second source IP:port number in a second message 208 at step 518 below, wherein a response 209 send in step 519 below can preferably be sent to the second source IP:port number received in the second message 208 at step 518 in order to traverse a firewall 104 (as depicted and described in connection with packet 209a in Figure 2). In other words, the proper destination IP:port for a response 209 to a module 101 can change over time, such as the proper destination IP:port changing due to the use of sleep states by module 101 and/or function of a firewall 104. Consequently, according to an exemplary embodiment, a response 209 can utilize a destination IP:port number equal to the source IP:port number received in the last message 208 from module 101 received by server 105.

At step 517, server 105 can authenticate the message 208 received in step 516 using the shared secret key 510 described in step 513. Server 105 could record the shared secret key 510. If step 517 occurs for the first time in a lifetime of module 101, then shared secret key 510 could comprise a pre-shared secret key 129a recorded by server 105 in a module database 105k illustrated in Figure 1f. If step 517 occurs at subsequent time, then server 105 could have sent shared secret key 510 in a server encrypted data 504 and recorded shared secret key 510 in a module database 105k for later use (such as at step 517). Server 105 can authenticate the message 208 according to message digest, or using the shared secret key 510 as a symmetric key 127 within a symmetric ciphering algorithm 141b, where the successful encryption and decryption of data within message 208 using the shared secret key 510 on both ends could be confirmation that message 208 is authenticated, since both parties would only be able to mutually encrypt and decrypt by sharing the same shared secret key 510.

Other possibilities exist as well for server 105 to use a shared secret key 510 in order to authenticate a message 208 that contains a new module public key 111 (where module 101 contains a new module private key 112). In one embodiment, message 208 in step 516 could include a module digital signature 405, where the module 101 used the shared secret key 510 as a private key to generate the module digital signature 405. After receiving authenticated new module public key 111 in steps 516 and 517, according to a preferred exemplary embodiment, server 105 can

Petitioner Samsung Ex-1038, 0119

preferably only accept and process (A) either incoming (i) a symmetric keys 127 ciphered with a asymmetric ciphering algorithm 141a, and/or (ii) incoming server instructions 414, when (B) the next or a subsequent incoming message 208 from module 101 using module identity 110 also includes a valid module digital signature 405 verified by using the new module public key 111, received at step 516.

According to an exemplary embodiment, shared secret key 510 can be associated with a module public key identity 111a, and shared secret key 510 can be used to authenticate a particular value for a module public key identity 111a. In this embodiment, (i) a message 208 with module public key 111 and a first module public key identity 111a may be authenticated using a shared secret key 510, but (ii) a second message with module public key 111 and a second module public key identity 111a may not be authenticated using the same shared secret key 510. Thus, in accordance with an exemplary embodiment, shared secret key 510 can be used for both (i) a single time for authenticating a module public key 111, and (ii) authenticating a module public key 111 with a particular value for the module public key identity 111a. Note that module public key identity 111a can be particularly useful with key revocation, such that a key revocation could specify a particular module public key identity 111a (associated with a particular module public key 111) to be revoked, but other module public keys 111 with different module public key identities 111a could remain valid and not revoked.

Although not illustrated in Figure 5b, server 105 could operate with a certificate authority 118 in order to utilize a new module public key 111, as described in this paragraph. At step 516, new module public key 111 could be received by server 105 in the form of a uniform resource locator (URL) or domain name for download of a certificate 122 corresponding to the new module public key 111. If new module public key 111 is included in a certificate 122 in this embodiment of step 517 (or a URL to the certificate 122), then module 101 could send server 105 a URL or address on the Internet 107 where server 105 could download the new module public key 111, such as if module 101 had a certificate authority 118 sign the new module public key 111. In this case, (i) the certificate authority 118 (or a separate server than server 105) could perform the steps of 516 and 516 before server 105 conducts step 518 below, and (ii) certificate authority 118 would need some confirmation module 101 using module identity 110 was the correct owner of new module public key 111. Certificate authority 118 could authenticate module 101 using the shared secret key 510 (instead of server 105 authenticating module 101 directly with the shared secret key 510). Other

Petitioner Samsung Ex-1038, 0120

possibilities exist as well for module 101 to utilize shared secret key 510 to authenticate a module public key 111 that has been derived by module 101.

After steps 516 and 517, server 105 can update a module database 105k using the module identity 110 to insert or update the new module public key 111, and parameters 126 associated with new module public key 111. Server 105 may communicate with a plurality of modules 101, and thus could utilize a module database 105k in order to record the new module public key 111 and parameters 126 with the module identity 110. In one embodiment, the module identity 110 could preferably operate as an index within a table of module database 105k in order to speed reads and writes from the table used with module public key 111, parameters 126, and also selecting a symmetric key 127 for a symmetric ciphering algorithm 141b in later messages. As described in Figure 1g, parameters 126 can include data useful for the operation of cryptographic algorithms 141 and module public key 111. According to a preferred exemplary embodiment, some modules 101 in a system 100 could utilize a first elliptic curve, such as using a first set of ECC parameters 137 or first ECC standard curve 138 within a parameters 126, and other modules 101 could utilize a second and different elliptic curve within a parameters 126, such as a second set of ECC parameters 137 or second ECC standard curve 138.

After updating the new module public key 111, in step 518 of Figure 5b, server 105 could receive a second message 208, and the second message 208 can include a module identity 110 and module encrypted data 403. Although not illustrated in Figure 5b, the second message 208 could also include a module digital signature 405, wherein the module digital signature is created with the new module public key 111 received in step 516. Server 105 could then utilize the steps illustrated in Figure 4 in order to process the incoming message 208 with the new module public key 111, including using the module identity 110 received in the second message 208 to select the new module public key 111 and subsequently verify a module digital signature 405 using the new module public key 111 and digital signature algorithm 141d. Also as discussed in Figure 4 in connection with processing a received message 208, server 105 could decrypt the module encrypted data 403 in the second message 208 by using server private key 105c. In one embodiment, the second message 208 as illustrated in Figure 5b, which could be the next message after authenticating module public key 111 in step 517, could include a symmetric key 127.

Petitioner Samsung Ex-1038, 0121

The module encrypted data 403 in step 518 could include a symmetric key 127 for utilization with a symmetric cipher 141b. Module 101 could also send sensor data in a module encrypted data 403 at step 518. Or, at step 518 the second message 208 could be a signal for server 105 to use a key derivation function 141f with the server public key 114 and the new module public key 111 (received at step 516) to create a new derived shared key 129b for use with symmetric ciphering algorithms 141b in subsequent messages 208. If the second message 208 in step 518 comprises a signal for server 105 to derive a new derived shared key 129b, then this second message 208 could then optionally leave off module encrypted data 403 and/or a module digital signature 405. The successful use of a new derived shared key 129b (using the new module public key 111 and existing server public key 114) with symmetric ciphering algorithms 141b at subsequent steps by both module 101 and server 105 can indicate to each the communications are mutually authenticated. Second message 208 could also include a server instruction 414, and other possibilities exist as well without departing from the scope of the present invention.

At step 519, server 105 can send a response 209 to module 101, where the response 209 includes server encrypted data 504 and a module instruction 502. Server 105 could take the steps to create and send response 209 as depicted and described in connection with Figure 5a. Response 209 could be formatted according to the exemplary response 209 illustrated in Figure 6a. The module instruction 502 could be an acknowledgement 501 that the second message 208 sent in step 518 was received by server 105. At step 520, server 105 can receive a third message 208 with a confirmation 414 to server 105. Confirmation 414 can be used to signal proper execution of module instruction 502, if module instruction 502 comprised an instruction other than an "ACK" or acknowledgement 501. If module instruction 502 in step 519 was an acknowledgement 501 from server 105, then the confirmation 414 may omitted and in this case step 520 could be skipped.

At step 521 server 101 can determine or evaluate if a new module public key 111 and/or certificate 122 are required for continued operation. One reason for the need of new keys could be the expiration of a certificate 122 for module 101, or the desire to utilize a different set of parameters 126 such as a longer key length for increase security or the use of a different ECC parameters 137 or a different ECC standard curve 138 with cryptographic algorithms 141. As described elsewhere herein, many other possibilities exist for reasons why module 101 and/or server 105 can prefer for module 101 to utilize a new module public key 111 and new module private key 112. Either server 105 or module 101 may determine that the use of a new module public key 111

Petitioner Samsung Ex-1038, 0122

and new module private key 112 may be preferred at step 521. If module 101 determines that the use of a new module public key 111 and new module private key 112 is preferred or desirable, module 101 could send server 105 a signal that new keys will be generated either before step 521 or at step 521.

Upon determining new keys are desirable at step 521, then server 105 could instruct module 101 to derive new private and public keys by returning to step 515. Although not illustrated in Figure 5b, upon determining "yes" at step 521, server 105 could send a module instruction 502 of "new key generation" and also a new set of parameters 126 to utilize with the new module private key 112 and module public key 111. In accordance with exemplary embodiments, module instruction 502, including the "new key generation" instruction and set of parameters 126, can be sent in a response 209 both (i) after module 101 wakes from a sleep or dormant state and sends a message 208 after waking from the sleep or dormant state, and (ii) before the expiration of a firewall port binding timeout value 117 after receiving the message 208. If server 105 determines that new keys are not required or desirable at step 521, server 105 can then proceed to step 312 and wait for additional incoming messages 208 from module 101 or other modules. Step 312 is also depicted and described in connection with Figure 3.

Figure 6a

Figure 6a is a simplified message flow diagram illustrating an exemplary message received by a server, and an exemplary response sent from the server, in accordance with exemplary embodiments. Figure 6a illustrates exemplary details within message 208 received by server 105 and also response 209 sent by server 105. Message 208 may comprise a TCP/UDP packet 601a sent from module 101 source IP:port 204 to server 105 destination IP:port 207. According to an exemplary embodiment, UDP or UDP Lite formatting for TCP/UDP packet 601a may be preferred. Source IP:port 204 and destination IP:port 207 in message 208 may be included within a header in TCP/UDP packet 601a. Although a single message 208, response 209, module 101, and server 105 are shown in Figure 6a, system 100 as illustrated in Figure 2 may comprise a plurality of each of these elements. As contemplated herein, the term "datagram" may also refer to a "packet", such that referring to an element as datagram 601a can be equivalent to referring to packet 601a.

Petitioner Samsung Ex-1038, 0123

TCP/UDP packet 601a may include a body 602, which can represent the data payload of TCP/UDP packet 601a. The data payload of message 208 can optionally include channel coding 406 as described in Figure 4 above, if the transport protocol for TCP/UDP packet 601a supports the transmission of bit errors in the body 602 (as opposed to entirely dropping the packet), such as with the UDP Lite protocol. Support for the transmission of bit errors in body 602 by wireless network 102 would be preferred over entirely discarding a packet, since the programs such as module controller 105x could include support for and utilization of channel coding 406. Without UDP Lite formatting, message 208 can alternatively sent by module 101 as a UDP datagram, such as if wireless network 102 (or a wired connection) does not support the UDP Lite protocol. Note that in this case (no support for the transmission of bit errors in a body 602), wireless network 102 and nodes within Internet 107 would preferably include channel coding on the data link layers of the OSI stack in order to maintain robustness to bit errors at the physical layers of various hops along the path between module 101 and server 105.

Note that if (A) message 208 comprises (i) regular UDP or TCP formatting (i.e. not UDP Lite or similar variations) within an IPv6 network, or (ii) a UDP or TCP format within an IPv4 network with a 603 enabled, then (B) channel coding 406 may optionally be omitted. Checksum 603 can comprise a value to for an integrity check of a packet 601a, and the calculation and use of checksum 603 is defined in IETF standards for TCP and UDP packets. In accordance with a preferred exemplary embodiment, including the use of IPv6 for Internet 107 and a UDP datagram for message 208 and response 209, a checksum 603 sent by module 101 in a message 208 does not equal a checksum 603 in the message 208 received by server 105.

The body 602 can include a module identity 110, module encrypted data 403, and channel coding 406. Although not illustrated in Figure 6a, body 602 could also include a module digital signature 405, as illustrated in Figure 6 of U.S. Patent Application Serial No. 14/039,401. Module identity 110 is illustrated in Figure 6a as external to module encrypted data 403, although module identity 110 may optionally only be included in module encrypted data 403, and in this case module identity 110 would not be external to module encrypted data 403 in a body 602. By including module identity 110 as external to module encrypted data 403, server 105 can use the unencrypted module identity 110 in order to select either (i) the appropriate module public key 111 to verify module digital signature 405 if an asymmetric cipher 141a is used within cryptographic algorithms 141, or (ii) the appropriate symmetric key 127 within cryptographic algorithms 141 to decrypt the

Petitioner Samsung Ex-1038, 0124

module encrypted data 403. Module public key 111 and symmetric key 127 may preferably be recorded in a database 105d, such that server 105 can access a plurality of public keys using module identity 110 in body 602 for a plurality of modules 101.

Thus, by including module identity 110 external to module encrypted data 403, server 105 can utilize the module identity 110 to query a database 105d and select the appropriate module public key 111 or symmetric key 127. As noted previously, module identity 110 could comprise a string or number that is uniquely associated with module identity 110, such as a session identity, as opposed to being a module identity 110 that is read from hardware in module 101 such as an IMEI number, Ethernet MAC address, etc. Module identity 110 is illustrated in Figure 6a as a session identity that is a different representation of module identity 110 of a serial number such as in Figure 2, but in both cases the values can comprise a module identity 110 since the values can be uniquely associated with module 101 at any point in time.

According to an exemplary embodiment where asymmetric ciphering 141a of module encrypted data 403 is utilized, such as (i) the first message 208 sent by module 101 and (ii) where a symmetric key 127 had not been previously exchanged, module identity 110 can be (a) within module encrypted data and (b) not external to module encrypted data 403. In this case, server 105 can utilize server private key 105c to, in sequence, decrypt module encrypted data 403, extract module identity 110 from the decrypted module encrypted data 403, and then used the module identity 110 to select module public key 111 from module database 105k in order to verify a module digital signature 405. Note that if a module identity 110 is in body 602 and external to module encrypted data 403, then module identity 110 could be obfuscated or otherwise ciphered according to a pre-agreed algorithm with server 105, such that server 105 can utilize the obfuscated or ciphered module identity 110 to select a module public key 111 from module database 105k. The value of "[Module Identity String]" shown in Figure 6a could comprise an obfuscated module identity 110. According to an exemplary embodiment where (i) symmetric ciphering of module encrypted data 403 is utilized, such as after a first message 208 had already been sent by module 101 and a symmetric key 127 had previously been exchanged, then (ii) module identity 110 can be external to module encrypted data 403 and in body 602 in order for server 105 to utilize module identity 110 and select symmetric key 127 from a module database 105k, thereby enabling server 105 to decrypt the module encrypted data 403 using the selected symmetric key 127.

Petitioner Samsung Ex-1038, 0125

The module digital signature 405 can be calculated using the steps and algorithms described in Figure 4 above. Module digital signature 405 can be a secure hash string or number, and can be calculated using module private key 112 and digital signature algorithms 141d. Server 105 can verify module digital signature 405 using module public key 111 according to the standard techniques for verifying digital signatures using PKI as described at step 410 in Figure 4. Note that module digital signature 405 can be useful for server 105 to maintain security, since server public key 114 may be shared and potentially other nodes besides module 101 could attempt to send in encrypted data using server public key 114.

In addition, the module digital signature 405 may optionally be omitted from body 602 after module 101 has previously sent symmetric key 127 in a previous message 208 to the message 208 illustrated in Figure 6a. In other words, in a series of messages 208, module 101 can preferably change from (i) using asymmetric ciphering 141a with an initial message 208 that includes symmetric key 127 in a module encrypted data 403 (where the initial message 208 also includes module digital signature 405 and module identity 110) to (ii) using symmetric ciphering 141b with subsequent messages 208 without module digital signature 405 in the series (where the subsequent messages 208 can include an obfuscated module identity 110 external to module encrypted data 403 for server 105 to select the appropriate symmetric key 127). The series of messages 208 could begin when the initial message 208 is sent by module 101 and end when expiration time 133 of symmetric key 127 has transpired, and subsequently a new series of messages 208 could begin where the first message 208 in the new series of messages changes back to asymmetric ciphering 141a with initial message 208 that includes symmetric key 127 in a module encrypted data 403 (where the initial message 208 also includes a new module digital signature 405). Other possibilities exist as well without departing from the scope of the present invention.

Using a message 208 with a module digital signature 405 can be both more efficient and overall more secure than digest authentication (such as the digest authentication described in IETF RFC 2069), although using digest-based authentication may be alternatively used. First, the use of a module digital signature 405 requires only a single packet for message 208 and a single packet for response 209 for secure communication between module 101 and server 105. The alternative digest-based authentication would normally require at least 4 packets comprising: (i) message 208, (ii) a challenge to message 208 from server 105 with a security token 401, (iii) a second message from module 101 with a hashed string generated using (i) the challenge, (ii) cryptographic

Petitioner Samsung Ex-1038, 0126

algorithms 141, and (iii) the module private key 112, and then (iv) an acknowledgement from server 105. The additional messages with digest-based authentication would thereby drain battery life faster or utilize more energy compared to using module digital signature 405.

Second, the use of module digital signature 405 allows a system 100 to be more highly secured since (i) server 105 may need to be connected to the Public Internet 107 and receive packets from a wide range of IP addresses that are not known before messages 208 arrive, and (ii) by using module digital signature 405, server 105 can then preferably not respond to incoming packets and messages without first receiving a properly signed module digital signature 405 (where the module identity 110 associated with module digital signature 405 could also be verified using a certificate 122 and a certificate authority public key 131). By server 105 remaining silent to all packets except packets with a properly signed module digital signature 405, system 100 can thereby remain more secure. In other words, according to preferred exemplary embodiments, server 105 does not send a response 209 to a first message 208 in a series of messages 208 that does not include a validated module digital signature 405 (where the validated module digital signature 405 includes a verified module identity 110), thereby increasing security. Once at least one module digital signature 405 has been received by server 105, then server 105 could use a symmetric key 127 to verify a module identity until a timer expiration 133 for the symmetric key 127. Server 105 could receive a symmetric key using the message 208 illustrated in Figure 6 of U.S. Patent Application Serial No. 14/039,401, and other possibilities exist as well for securely sending and receiving a symmetric key 127.

Module encrypted data 403 can be processed using the steps and algorithms described in Figure 4. Note that module encrypted data 403 as illustrated in Figure 6a is shown in a plaintext form for ease of illustration, but actual module encrypted data 403 within body 602 of a packet 601a could be transmitted as binary, hexadecimal, Base64 binary-to-text encoding, or other encoding rules. Note that encryption by module 101 may optionally be omitted, and the server instruction 414 with corresponding data could be included within a message 208 without encryption, such as if security could be maintained at the network level. As one example in this case without encryption, server instruction 414 could be included in body 602 as plaintext. The encryption and/or security could be applied through other means, such as a secure tunnel between module 101 and server 105, although setting up and maintaining a secure tunnel and similar or other means of security may require more processing and bandwidth resources than the efficient techniques described herein.

Petitioner Samsung Ex-1038, 0127

Module encrypted data 403 can include a server instruction 414, a server identity 206, a module identity 110, a security token 401, a timestamp 604a, and a sensor measurement 604b. The server instruction 414 can represent the purpose of the message 208 for server 105, and Figure 6a illustrates an "update" for server instruction 414. An update for server instruction 414 could be used to periodically notify server 105 of regular, periodic sensor measurements 604b acquired by a sensor 101f. An update for server instruction 414 may also comprise a periodic report regarding monitored unit 119, and a server instruction 414 is described in Figure 4. Other server instructions 414 besides an "update" may be included in a module encrypted data 403 within a body 602. The "update" illustrated in message 208 in Figure 6a can also include a new symmetric key 127, and the module encrypted data 403 illustrated in Figure 6a may comprise the use of either an asymmetric ciphering 141a with public/private keys, or (ii) symmetric ciphering 141b with a symmetric key 127.

An initial transmission or negotiation of a symmetric key 127 may preferably utilize asymmetric ciphering 141a and the use of a public key as an encryption key and a private key as a decryption key. Subsequent transmission of a new symmetric key 127 may utilize either (i) a symmetric cipher 141b with a previously negotiated but still valid symmetric key 127 (i.e. expiration time 133 has not transpired), or (ii) asymmetric ciphering 141a. If the data within instruction 414 is longer than the maximum data length supported by a selected asymmetric ciphering algorithm 141a and the public/private key pair, then module encrypted data 403 within message 208 can be broken up into several sections, such that the data within each section is less than the maximum data length supported by the asymmetric ciphering algorithm 141a and key length.

Server identity 206 within module encrypted data 403 can be useful for properly identifying that server 105 is the proper recipient and final destination of message 208. Server identity 206 can be useful if a plurality of servers 105 is utilized by an M2M service provider 108 with potentially hundreds of thousands or millions of modules 101. In this case, with a plurality of servers 105, server private key 105c may represent a private key that is shared among a plurality of servers 105, since otherwise server 105 may not be able to decrypt module encrypted data 403 if each server 105 in the plurality of servers 105 did not share the common server private key 105c. Continuing in this example of a plurality of servers 105, a server identity 206 may represent a server that associated with M2M service provider 108 but not the recipient of message 208. In this case, (i) a first server

Petitioner Samsung Ex-1038, 0128

105 could receive message 208 and decrypt message 208 using a common server private key 105c or symmetric key 127, and (ii) the first server 105 can forward message 208 to the second server 105 (not shown) with server identity 206. In this case, the first server 105 can forward message 208 to the second server (not shown) without the encryption applied to module encrypted data 403, since (i) the second server 105 may not have access to the server private key 105c and/or symmetric key 127, or (ii) the first server 105 could have already decrypted the module encrypted data 403 in order to read server identity 206 within module encrypted data 403.

Module identity 110 within module encrypted data 403 can represent the identity of module 110, and could represent a serial number read by module 101 from a read-only hardware address. Module identity 110 is described in Figure 1c and can represent a unique identifier of module 101. Module identity 110 outside module encrypted data 403 can represent a string or number that is different than a serial number that can be used by module 101 within a module encrypted data 403. Security token 401 within module encrypted data 403 can represent a random string in order to make message 208 reasonably unique and thus system 100 in Figure 2 robust against replay attacks. If module encrypted data 403 includes symmetric key 127, then security token 401 could optionally be omitted since symmetric key 127 can also function as a security token 401. Security token 401 is described in Figure 5a. Timestamp 604a can represent a time value that module 101 sends message 208 or a time value that module 101 acquired sensor data 604b. Sensor data 604b is described with the description of a sensor 101f in Figure 1e, and sensor data 604b can represents data module 101 acquires using sensor 101f. Sensor data 604b within message 208 may be stored by server 105 in a module database 105k, or potentially forwarded to another server (not shown) for additional processing. Sensor data 604b can comprise a wide range of values for a sensor 101f besides the exemplary value of a temperature reading shown in Figure 6a, including raw sensor data, compressed sensor data, and processed or averaged sensor data. The specific sensor data 604b shown in Figure 6a is illustrated to be exemplary and not limiting for sending and receiving sensor data. Sensor data 604b may also be referred to as a sensor measurement 604b.

Although not illustrated in Figure 6a, body 602 or module encrypted data 403 may also include an (i) identity of monitored unit 119, which may be associated with sensor data 604b, and/or (ii) a sensor identity 151 associated with sensor data 604b, such that data from potentially multiple sensors 101f could be properly identified and recorded. As one example, module 101 could collect sensor data for a plurality of monitored units 119, and in this case message 208 would preferably

Petitioner Samsung Ex-1038, 0129

include an identity of monitored unit 119 associated with the sensor data 604b. Or, a sensor 101f could have a sensor identity 151, and message 208 could include the sensor identity 151 with the corresponding sensor data 604b (also illustrated in Figure 7 of U.S. Patent Application Serial No. 14/039,401). As described above, message 208 could also include a symmetric key 127, as illustrated in Figure 6 of U.S. Patent Application Serial No. 14/039,401.

Note that if (A) module encrypted data 403 exceeds an acceptable length for input or output into asymmetric ciphering algorithms 141a, such as data within a module encrypted data 403 comprising an exemplary 3000 bits but only a 2048 bit key length is utilized in an exemplary module private key 112 processed with an RSA algorithm 153, then (B) module encrypted data 403 within body 602 could comprise multiple separate sub-sections for module encrypted data 403. In this case, each sub-section could comprise data less than the maximum acceptable length for encryption, and the sub-sections could be combined in order to form a module encrypted data 403 within body 602.

Figure 6a also illustrates exemplary details within response 209 sent by server 105. Response 209 may comprise a TCP/UDP packet 601b sent from server 105 IP:port 207 the IP address 210 and port number 605, where IP address 210 represents the external IP address of wireless network firewall 104 and port number 605 is the source port in message 208 as received by server 105 (i.e. the source port in message 208 after traversing the firewall 104 illustrated in Figure 6a). Thus, IP:port with IP address 210 and port number 605 may be different than IP:port 204 in response 209, since the presence of a wireless network firewall 104 may perform NAT routing, which could change the source IP address and source port number from IP:port 204 to IP address 210 and port number 605 in message 208, as received by server 105. The use of wireless network firewall 104 in wireless network 102 may require that response 209 be sent from IP:port 207 to IP address 210 and port number 605 in order to be properly processed by firewall 104 and forwarded to module 101 at IP:port 204. Source IP:port 207 and destination IP address 210 and port number 605 in response 209 may be included within a header in TCP/UDP packet 601b. TCP/UDP packet 601b could comprise a regular UDP packet, a UDP Lite packet, or a TCP datagram, or similar protocols supported by an Internet 107. TCP/UDP packet 601a and TCP/UDP packet 601b can preferably utilize the same protocol.

Petitioner Samsung Ex-1038, 0130

As noted previously, the use of checksums may be mandatory in IPv6 networks, and thus a response 209 comprising a packet 601b can include a checksum value 603 (illustrated in message 208 but not response 209) for the header. The use of firewalls such as firewall 104 can change the header values in a packet 601b. In accordance with a preferred exemplary embodiment, a first checksum value 603 within a response 209 sent by server 105 can be different and/or not equal to a second checksum value 603 within the response 209 received by module 101. Likewise, in an exemplary embodiment, a first checksum value 603 within a message 208 sent by a module 101 can be different and/or not equal to a second checksum value 603 within the message 208 received by server 105.

A UDP, TCP, or UDP Lite datagram as a TCP/UDP packet 601b within response 209 may include a body 606. Body 606 may comprise the payload or data within a UDP, TCP, or UDP Lite packet. Body 606 can include a server identity 206, a server digital signature 506, server encrypted data 504, and channel coding 406. Server identity 206 is illustrated in Figure 6a as external to server encrypted data 504 within body 606, but server identity 206 may optionally be included in server encrypted data 504 instead. Module 101 may communicate with a plurality of servers 105, and server identity 206 as external to server encrypted data 504 can allow module 101 to select the appropriate symmetric key 127 to utilize for decrypting server encrypted data 504 (since each of the multiple servers 105 that module 101 communicates with may utilize a different symmetric key 127).

Also note that the server identity 206 can be similar to module identity 110, such that multiple different values for server identity 206 could be utilized in a system 100, but each of the different values could preferably be uniquely associated with server 105. As one example, server identity 206, outside server encrypted data 504 as illustrated in Figure 6a, may comprise a session identity or session identifier, as opposed to a different server identity 206 that could comprise a hardware serial number or domain name for server 105. Thus, server identity 206 outside a server encrypted data 504 may be a different string or representation than server identity 206 within server encrypted data 504, but both strings/numbers used for server identity 206 in response 209 could be associated with server 105.

Server digital signature 506 in body 606 can comprise a secure hash signature of a subset of body 606, where the subset of body 606 can comprise server encrypted data 504, and/or server

Petitioner Samsung Ex-1038, 0131

identity 206 as illustrated in Figure 6a. In other words, processing the secure hash signature can omit (i) server digital signature 506 itself and (ii) channel coding 406 as input into the cryptographic algorithms 141 used to process or verify server digital signature 506. In this manner, module 101 can utilize server digital signature 506 to authenticate that response 209 was sent by server 105. Channel coding 406 in body 606 is also depicted and described in connection with Figure 5a above.

Body 606 may include server encrypted data 504. Server encrypted data 504 is depicted and described in connection with Figure 5a above. Server encrypted data 504 may include an acknowledgement 501, wherein acknowledgement 501 can notify module 101 that message 208 has been received by server 105. As illustrated in Figure 6a, server encrypted data 504 may optionally also include a module instruction 502 for module 101. The module instruction 502 could be a string that contains instructions or configuration parameters for module 101, such as an order to change state, parameters regarding the monitoring of monitored unit 119, server names or addresses, radio frequency parameters, timer values, settings for actuator 101y, etc. A module instruction 502 is depicted and described in connection with Figure 5a above. The exemplary module instruction 502 illustrated in Figure 6a comprises a "key generation" 608 instruction for module 101 derive a new set of keys. The use of a "key generation" 608 instruction was also depicted and described in connection with Figure 5b above. Other possibilities for a module instruction 502 within a response 209 are possible as well without departing from the scope of the present invention. Although not depicted in Figure 6a or Figure 2, if response 209 includes a module instruction 502, according to an exemplary embodiment, module 101 can preferably send a second message 208 to server 105, where the second message 208 includes a confirmation that module instruction 502 was successfully executed or implemented by module 101. This confirmation could be included in a server instruction 414 for server 105 within a second message 208.

Also, although a server encrypted data 504 may preferably be included within a body 606, body 606 may optionally omit server encrypted data 504 and include data from server 105 that is not encrypted, such as plaintext. As one example in this case, acknowledgement 501 could be included in body 606 as plaintext. In addition, although a server digital signature 506 is not illustrated in Figure 6a, a server digital signature 506 could be included in body 606 and external to server encrypted data 504. In an exemplary embodiment, the inclusion of a server digital signature 506 in a response 209 is illustrated in Figure 6 of U.S. Patent Application Serial No. 14/039,401.

Petitioner Samsung Ex-1038, 0132

The server digital signature 506 may (i) optionally be omitted as well, or (ii) included within server encrypted data 504.

Also, although not illustrated in Figure 6a, server encrypted data 504 could include a symmetric key 127 for module 101 to utilize with symmetric ciphering 141b in cryptographic algorithms 141 for processing a module encrypted data 403 in subsequent messages 208 and/or responses 209. If server encrypted data 504 includes a symmetric key 127, then server 105 preferably can utilize an asymmetric ciphering 141a with cryptographic algorithms 141 to process the server encrypted data 504 containing the symmetric key 127. An example for the previous sentence could be if message 208 was received without a symmetric key 127 and server 105 can issue the symmetric key 127. As contemplated herein, more than one symmetric key 127 may be used concurrently in a system 100, such as a first symmetric key 127 utilized in symmetric ciphering 141b for a message 208, and a second symmetric key 127 utilized in symmetric ciphering 141b for a response 209. Other possibilities exist as well without departing from the scope of the present invention.

Server encrypted data 504 in a response 209 may include a security token 401. Security token 401 may be a random string and may also be generated by either server 105 or module 101. If security token 401 is generated by module 101, then security token 401 may be included in message 208 and also utilized by server 105 in response 209, as illustrated in Figure 6. By including security token 401 in acknowledgement 501, system 100 can be made robust to replay attacks since each response 209 can be reasonably unique for each response 209 sent by server 105.

Figure 6b

Figure 6b is a simplified message flow diagram illustrating an exemplary message received by a server, wherein the message includes a derived module public key, in accordance with exemplary embodiments. As discussed in Figure 5b, there can be cases where module 101 derives a new module public key 111 and new module private key 112. On example would be the initial creation of the key pairs by module 101, and many other examples could exist as well. Figure 6b can illustrate an exemplary format and contents of a message 208 for steps 516 and 517 of Figure 5b. This exemplary message 208 can also help to illustrate the significant differences from

Petitioner Samsung Ex-1038, 0133

conventional technology and improvements for efficient and secure communications by utilizing embodiments contemplated herein.

A message 208 illustrated in Figure 6b using steps 516 and 517 can include (i) sending new module public key 111, a module public key identity 111a, a module identity 110, a server instruction 414, and a set of parameters 126 associated with the new module public key 111 and/or cryptographic algorithms 141 for using the new module public key 111. Exemplary parameters 126 illustrated in Figure 11 include (i) a secure hash algorithm 141c to utilize in signatures, which could comprise the SHA 256 algorithm as shown (which may also be known as the SHA-2 algorithm), (ii) a selected elliptic curve for use with ECC algorithms 154 or a modulus to use with RSA algorithms 153, and (iii) a time-to-live value for the public key, such as the illustrated "time to live" value of 1 year shown in Figure 6b. The time value for the validity of new module public key 111 could alternatively be specified in a set expiration date. Other values associated with cryptographic algorithms 141 could be included in parameters 126 as well, and the illustrated values are intended to be exemplary instead of limiting. Other possibilities for data with a message 208 illustrated in Figure 6b include a parameters 126 including a set of ECC parameters 126, or a specified secure hash algorithm 141c comprising SHA-3 or SHA-512.

Additional values or fields within a message 208 associated with communicating a new module public key 111 with server 105 could include a server instruction 414 of "new public key". This server instruction 414 could inform server 105 to utilize the new module public key 111 within the message 208. Module public key identity 111a can include a sequence number or identity for the new module public key 111, such that module 101 or server 105 can properly reference and/or select the key from a plurality of module public keys 111 that could be associated with module identity 110. Although module public key identity 111a is illustrated as a separate field in server instruction 414, module public key sequence number 111a could optionally be included in parameters 126, such that the value within parameters 126 specifies the current sequence number or module public key identity 111a for the new module public key 111 included in a message 208.

Other fields and features within a message 208 as illustrated in a Figure 11 can be similar to the fields presented in Figures 6a. Since (a) Figure 6a can also illustrate a first message 208 sent by a module 101 to a server 105, such as after keys are derived in a step 515, then (b) module 101 can read multiple values from RAM 101e or a nonvolatile memory 101w or 101c in order properly

Petitioner Samsung Ex-1038, 0134

construct or format message 208. Each of (i) destination IP:port number 207, (ii) parameters 126, and (iii) shared secret key 510 can preferably be written into nonvolatile memory at step 512 of Figure 5b, if message 208 in Figure 6b represents the first message 208 sent by module 101. The source IP:port number 204 can represent a number assigned by an operating system 101h.

If message 208 in Figure 6b comprises a subsequent time message 208 is received by server 105 (i.e. not a first time module 101 sends a module public key 111), such as after step 521 illustrated in Figure 5b, then each of (i) destination IP:port number, (ii) parameters 126, and (iii) shared secret key 510 could be updated by server 105 using a module instruction 502 within a server encrypted data 504 before message 208 illustrated in Figure 6a is received by server 105. In this manner, shared secret key 510 could change from (i) comprising a pre-shared secret key 129a (for a first message 208 after module key derivation) to (ii) comprising a shared secret key that is sent by server 105 within a server encrypted data 504 (for a subsequent message 208 after module key derivation).

After receiving message 208, server 105 can use the unencrypted module identity 110 illustrated in a body 602 of Figure 6b to select the shared secret key 510 in order authenticate message 208. As described in step 517 of Figure 5b, server 105 may preferably authenticate message 208 that includes module public key 111 in order to confirm that module public key 111 originated from physical module 101 with a hardware module identity 110 (as opposed to being an imposter submitting the module public key 111). The use of a channel coding 406 is described in connection with Figures 4 and 5a, and channel coding may optionally be omitted. If message 208 comprises a UDP Lite packet, then channel coding may optionally be applied within the body 602. If message 208 comprises a UDP packet, then channel coding may comprise sending the exact same UDP packet 601a multiple times, such as an exemplary 3 packets 601a sent at the same time.

Although not illustrated in Figure 6b, in an exemplary embodiment module public key 111 could also be received in a message 208, where the module public key 111 and parameters 126 can be included in an encrypted format within a module encrypted data 403. As depicted and described in connection with steps 1001 and 1002 of Figure 10, and also Figure 11 of U.S. Patent Application Serial No. 14/039,401, the security of a system 100 can be further increased by both (i) ciphering module public key 111 and parameters 126, and (ii) only sharing the module public key 111 in a confidential manner with server 105. If module 101 needed a module public key 111 for other

Petitioner Samsung Ex-1038, 0135

purposes, such as obtaining a certificate, then a second, publicly disclosed module public key 111 could be utilized, where the second module public key 111 is different than a module public key 111 using parameters 126 that is sent to a server 105 in a module encrypted data 403.

Figure 6b also illustrates an exemplary embodiment, where module public key 111 can be authenticated with server 105 using a module digital signature 405. If message 208 comprises a first time module 101 utilizes a step 516 and step 517, such that a module public key 111 has not previously been sent to server 105, then message 208 could include a module digital signature 405 using the shared secret key 510, which could comprise the pre-shared secret key 129a. If message 208 comprises a subsequent time module 101 utilizes a step 516 and step 517, such that a module public key 111 has previously been sent to server 105, then message 208 could include a module digital signature 405 using the previous module private key 112 (i.e. not the new module private key associated with the new module public key 111 in the message 208 shown in Figure 6b). As noted in Figure 5b, module digital signature 405 could be omitted, and message 208 with module public key 111 could be authenticated using a message digest algorithm and the shared secret key 129a.

Figure 7

Figure 7 is a simplified message flow diagram illustrating exemplary data transferred between a module and an application using a server, in accordance with exemplary embodiments. Figure 7 includes a system 700 and illustrates an exemplary message 208 from a module 101 to a server 105 and also an exemplary application message 701 between an application 171i and server 105. Note that application message 701 could also be considered as transferred between, sent to, or received from server 105 and application server 171. System 700 can comprise a module 101, a server 105, and an application 171i operating on an application server 171, and these elements may communicate over a network such as the Internet 107. For example, application server 171 may utilize an IP:port number 702 for sending and receiving messages with server 105. The IP address within IP:port number 702 is illustrated as an IPv4 address, but an IPv6 address could be utilized as well, or other addressing schemes are possible. Message flows within a module 101 from a sensor 101f and to an actuator 101y are also included in a system 700 as illustrated in Figure 7. Message flows within a module 101 could utilize a system bus 101d.

Petitioner Samsung Ex-1038, 0136

Although not illustrated in Figure 7, before module 101 sends a module public key 111 to server 105, possibly by using step 516 as illustrated in Figure 7, module 101 can derive the public and private keys using step 515 and a set of parameters 126. Alternatively, module 101 may have the module public key 111 and module private key 112 generated outside module 101 and loaded into a non-volatile memory 101w. Server 105 can utilize step 516 to receive a module public key 111 from module 101. Server 105 can utilize a step 517 and a shared secret key 510 to authenticate a message 208 that contains the module public key 111 from step 516. Authentication of module public key 111 may be preferred in order to ensure that the module public key 111 is properly associated with the correct physical module 101, and prevent an imposter, hacker, etc. from sending in a fake module public key 111 for module 101. After using step 517 to authenticate module public key 111, server 105 can record module public key 111 and associated module identity 110 (plus optionally a module public key identity 110a) in a module database 105k. Although not illustrated in Figure 7, server 105 can also send an application message 701 to application 171i after successfully recording module public key 111.

Application 171i operating within an application server 171 can send an application message 701 to server 105, and server 105 can receive the application message 701. Application message 701 could include a module instruction 502, where the module instruction 502 could comprise an actuator setting 706. Although not illustrated in Figure 7, module instruction 502 as transmitted or sent by application 171i or application server 171 could include a module identity 110 and/or an actuator identity 152. Actuator setting 706 could include a setting value and an actuator identity 152. As one exemplary embodiment, module 101 may have a plurality of actuators 101y that comprise thermostats. Actuator setting 706, where one actuator 101y had an actuator identity 152 of "Left", could comprise an exemplary string like "Left, 25.5", where module 101 would set the "left" thermostat/actuator 101y to 25.5 degrees C. The value "left" could also comprise the actuator identity 152. Other possibilities exist as well without departing from the scope of the present invention, and a thermostat, temperature settings, or actuator identities are not required to use the methods and systems contemplated herein. As discussed below in connection with Figure 8, actuator setting 706 within an application message 701 could be received within a secure connection data transfer 802 from application server 171. Thus, in an exemplary embodiment, the actuator setting 706 may preferably not be plaintext as transmitted across a network such as the Internet 107 between server 105 and application server 171 in an application message 701.

Petitioner Samsung Ex-1038, 0137

A module instruction 502 (i) from an application 171i or application server 171, and (ii) within an application message 701 could include other exemplary values or instructions for a module 101, besides the exemplary actuator setting. According to exemplary embodiments, a module instruction 502 could comprise information for module 101 such as (i) sleep timers or instructions or values for a CPU wake controller 101u, (ii) server address 106 or server identity 206 for communicating with a server 105 (such as sending a different server address 106 for module 101 to utilize in future communications), (iii) a new or updated values for set of data reporting steps 101x, (iv) a new or updated module program 101i, (v) software or firmware for operating system 101h and device driver 101g, (vi) a calibration value for sensor 101f or actuator 101y, (vii) values for a set of parameters 126, (viii) software or settings for radio 101z, (ix) updated cryptographic algorithms 141, (x) a new module private key 112, (xi) a symmetric key 127, (xii) a pre-shared secret key value 129a for use in communicating with a wireless network 102 (where the pre-shared secret key value 129a can be the equivalent of a Ki value in a network supporting ETSI/3GPP standards), (xii) a value for a module identity 101, (xiii) a value to use in a channel coding 406, or (xiv) a security token 401 or settings for using security tokens. Other possibilities exist as well for a module instruction 502 without departing from the scope of the present invention. After receiving module instruction 502 in a response 209 from server 105, module 101 could record the data in module instruction 502 within a nonvolatile memory 101w or RAM 101e.

After receiving application message 701, server 105 can wait for wait interval 703. As depicted and described in connection with Figures 2 and 6a, firewall 104 may be present in a system 700 and/or system 100, which could block the transmission or sending of packets from server 105 to module 101 at arbitrary times. In addition, according to exemplary preferred embodiments, module 101 can enter periods of sleep or dormancy using a CPU wake controller 101u in order to conserve energy or the life of a battery 101k, if present. During periods of sleep or dormancy, module 101 may not be able to receive packets from server 105. Consequently, server 105 can preferably wait for the wait interval 703 as illustrated in Figure 7, before sending response 209 which could include the module instruction 502. As illustrated in Figure 7, the module instruction 502 could include an actuator setting 706, but module instruction 502 could include other data as well such as the exemplary module instructions 502 described in the previous paragraph.

According to exemplary embodiments, wait interval 703 can vary depending upon module 101 and monitored unit 119, and wait interval 703 could comprise a wide range of values. Module

Petitioner Samsung Ex-1038, 0138

101 could send a sensor data 604b or a report or a message 208 at exemplary reporting intervals such as every minute, 10 minutes, hour, 6 hours, daily, or longer. Wait interval 703 could be associated with the reporting interval, and the wait interval 703 would end when the next message 208 from module 101 is received. If server 105 supports a plurality of modules 101, wait interval 703 can be associated with the specific module 101 associated with the module instruction 502, possibly by using a module identity 110 in both a message 208 and an application message 701. In other words, server 105 can preferably wait for a message 208 from the specific module 101 associated with the module instruction 502 before sending the response 209 which could include the module instruction 502. Response 209 could be sent using the source and destination IP:port numbers depicted and described in connection with Figure 2.

Upon the receipt of message 208 from module 101 with module identity 110, the wait interval 703 can end. As illustrated in Figure 7, message 208 could include a server instruction 414. The server instruction 414 in the exemplary embodiment illustrated in Figure 7 comprises an "update" server instruction 414, and could include a sensor measurement 604b. Sensor measurement 604b could be obtained by module 101 from sensor 101f before sending message 208, and possibly after module 101 wakes from a dormant state using a CPU wake controller 101u. Sensor measurement 604b could be collected by a module program 101i using a system bus 101d. As illustrated in Figure 6a, a server instruction 414 with sensor data 604b could be within a module encrypted data 403 and received by server 105. Server 105 could utilize the steps illustrated in Figure 4 to process the received message 208 at the end of wait interval 703. Sensor measurement 604b as used by module program 101i, server 105, application 171i, and/or application server 171 could represent a different string or number at each element, depending upon encoding rules or encoding schemes utilized by each element, but sensor measurement 604b at each location can represent data or a value collected by a sensor 101f.

After processing the received message 208 that could include sensor data 604b, server 105 can send application 171i operating on application server 171 an application message 701 that includes an update instruction 704, where update instruction 704 could include sensor data 604b, module identity 110, and sensor identity 151, if present. Update instruction 704 could include data other than sensor data 604, such as data pertaining to the state of module 101, including subcomponents illustrated in Figures 1b and 1e. Using update instruction 704 or a plurality of update instructions 704, application 171i can aggregate data to generate reports for presentation to

Petitioner Samsung Ex-1038, 0139

user 183 or make decisions using service controller 171x. Based on data input in update instruction 704, application 171i could output module instruction 502 in an application message 701. Application 171i could record data received in update instruction 704 within an application database 171k.

After receiving message 208 with server instruction 414, server 105 can send a response 209 to module 101. Note that response 209 is illustrated in Figure 7 as being sent after sending update instruction 704 to application server 171, but response 209 could also be sent to module 101 before sending update instruction 704 to application server 171. Response 209 can include module instruction 502, where module instruction 502 could comprise actuator setting 706, according to an exemplary embodiment. Module instruction 502 could also comprise other data for module 101 in other exemplary embodiments, as outlined above. Although not illustrated in Figure 7, response 209 could include module instruction 502 within a server encrypted data 503 using the steps depicted and described in connection with Figure 5a. Module instruction 502 could also include actuator identity 152 associated with actuator setting 706. Response 209 can be formatted as depicted and described in Figures 2 and 6a, such that response 209 can traverse a firewall 104 and be received by module 101 using IP address 204. Network firewall 104 is illustrated as a dashed line in Figure 7, and may be optionally not be present. But, the use of network firewall 104 may be included in a system 100 and/or system 700 and network firewall 104 may be beyond the control of a module 101, server 105, module provider 109, M2M service provider 108, etc.

After receiving response 209 with the module instruction 502 and actuator setting 706, module 101 can process the response 209, which could also include server encrypted data 503. Module 101 could extract actuator setting 706 from the module instruction 502. Module instruction 502 could include an actuator identity 152. Module 101 can use a module program 101i to send the actuator setting 706 to the actuator 101y with actuator identity 152. Actuator setting 706 as sent by module program 101i may be in a different format or data structure than actuator setting 706 as sent by application 171i, but both sets of data can achieve the same objective of having an actuator 101y apply a setting. According to one exemplary embodiment, actuator setting 706 as sent by module program 101i could be an analog voltage along a system bus 101d, while actuator setting 706 as sent by application 171i could be a string or number. Or, actuator setting 706 as sent by module program 101i to actuator 101y could be a number in a different format than a number in actuator

Petitioner Samsung Ex-1038, 0140

setting 706 sent by application 171i, application server 171, and/or server 105. Note that as contemplated herein, the term "actuator data" can include or comprise "actuator setting".

After applying actuator setting 706, actuator 101y can send an acknowledgement to module program 101i. Module program 101i can then send a second message 208 to server 105, where message 208 includes a server instruction 414 of "confirmation". The server instruction 414 of "confirmation" could be included in a module encrypted data 403 according to a preferred exemplary embodiment. Server 105 can receive the second message 208 with the module encrypted data 403 and decrypt the module encrypted data 403 using a step 413 to extract the server instruction 414 of "confirmation". The second message 208 may include the actuator identity 152 and/or also the module identity 110. Server 105 can send an application message 701 that includes a confirmation 705, where the confirmation can (i) inform application 171i that the actuator setting 706 sent to server 105 has been properly and/or successfully applied by module 101 and/or actuator 101y. Confirmation 705 could also include module identity 110 and/or actuator identity 152. Application 171i could then send an acknowledgement back to server 105 after receiving the confirmation 705.

According to preferred exemplary embodiments, actuator identity 152 is preferably globally unique, such that that including an actuator identity 152 in any packet would allow a server 105 or application 171i to lookup a module identity 110 and/or module 101 using the actuator identity 152 and a database such as module database 105k. Similarly, a sensor identity 151 may be globally unique, according to preferred exemplary embodiments such that a sensor identity 151 in any packet would allow a server 105 or application 171i to lookup a module identity 110 and/or module 101 using the sensor identity 151 and a database such as application database 171k.

Figure 8

Figure 8 is a simplified message flow diagram illustrating exemplary data transferred between a module and an application using a server, in accordance with exemplary embodiments. System 800 can include an application server 171, a server 105, and a module 101 in connected via a network. The network could comprise the Internet 107. Application server 171 could include an application 171i, where application 171i can include logic, algorithms, databases, user interfaces,

Petitioner Samsung Ex-1038, 0141

and programs for managing a plurality of modules 101 with a plurality of users 183. Application server 171 and application 171i may be associated with an M2M service provider 108, and M2M service provider 108 could use application 171i to provide and manage a service with distributed modules 101 associated with a plurality of monitored units 119.

Module 101 can derive a public key 111 and a private key 112 using step 515. Module 101 can derive the public and private keys using step 515 and a set of parameters 126. Alternatively, module 101 may have the module public key 111 and module private key 112 generated outside module 101 and loaded into a non-volatile memory 101w. Server 105 can utilize step 516 to receive a module public key 111 from module 101. Server 105 can utilize a step 517 to authenticate a message 208 that contains the module public key 111 in step 516. Authentication of module public key 111 may be preferred in order to ensure that the module public key 111 is properly associated with the correct physical module 101 with a module identity 110, and prevent an imposter, hacker, etc. from sending in a fake module public key 111 for module 101. After using step 517 to authenticate module public key 111, server 105 can record module public key 111 in a module database 105k. Although not illustrated in Figure 8, server 105 can also send an application message 701 to application 171i after successfully recording an authenticated module public key 111. Although not illustrated in Figure 8, a module public key 111 received in step 516 may also include a module public key identity 111a in order to track which of a plurality of potential module public keys 111 for a module 101 may be used.

Also, server 105 is not required to receive module public key 111 from module 101 in order to utilize the methods and systems contemplated herein. Instead of receiving module public key 111 in a message 208 from module 101, server 105 could alternatively query another server such as application server 171 or a server associated with certificate authority 118 for either module public key 112 or a certificate 122 associated with module 101 using a module identity 110. In addition, server 105 could have a list or database table of module identities 110 and module public keys 111 loaded into a module database 105k.

After recording module public key 111 and module identity 110, possibly including a module public key identity 111a, server 105 can wait for wait interval 703. Wait interval 703 could represent the time between reports or messages 208 submitted by module 101, and wait interval 703 for an individual module 101 could comprise a wide range of values from several times a second to

Petitioner Samsung Ex-1038, 0142

several days or longer, depending upon the application and/or monitored unit 119. The wait interval 703 can end when server 105 receives a message 208 from module 101 with a module identity 110.

Module controller 105x within server 105 can receive a message 208 that includes a server instruction 414 with sensor data 604b. The sensor data 604b and/or server instruction 414 could be included in a module encrypted data 403, where the module encrypted data 403 can use the module public key 111 submitted in step 516 above and derived by module 101 in step 515. According to one exemplary embodiment, module encrypted data 403 could be ciphered with a symmetric key 127 that is derived shared key 129b from a key derivation function 141f and module public key 111 received in step 516 (and also server public key 114). Module controller 105x can process message 208 using the steps depicted and described in connection with Figure 4 in order to decrypt the module encrypted data 403 and obtain the plaintext server instruction 414 and plaintext sensor data 604b. Although sensor data 604b is illustrated as the server instruction 414 in Figure 8, server instruction 414 could have other values such data associated with any of the components for module 101 illustrated in Figure 1b and Figure 1e. Server instruction 414 could be a "query" where module 101 queries for information from server 105 or application 171i, or server instruction 414 could be an alarm or error notification outside a regular reporting interval. Other possibilities for server instruction 414 exist without departing from the scope of the present invention. Server instruction 414 could also be a periodic "registration" message with no subsystem data for module 101, and a "registration" could be a message for server 105 indicating module 101 is awake and online with Internet 107.

Server 105 can establish a secure connection with application server 171 and application 171i using a secure connection setup 801 and a secure connection data transfer 802. Server 105 can utilize a server program 101i to manage the communication with application 171i and/or application server 171, while a module controller 105x can manage communication with a module 101. Alternatively, server program 101i and module controller 105x can be optionally combined or omitted, such that server 105 performs the actions illustrated in Figure 8 for server programs 101i and module controller 105x. Likewise, server 105 and application 171 could be combined or operate on the same local area network (LAN) and thus not be connected via the Internet 107. If server 105 and application 171 are nodes within the same LAN or virtual private network (VPN), then the network connection can also be considered a secure connection (without using encryption between the nodes), since packets routed between the nodes may not need to traverse the Internet

Petitioner Samsung Ex-1038, 0143

107 and thus the network layer could provide security. Although secure connection setup 801 is illustrated in Figure 8 as occurring after message 208 is received by server 105, secure connection setup 801 could take place before message 208 is received by server 105. Secure connection setup 801 could utilize a secure protocol such as TLS, IPSec, or VPN to establish a secure connection between server 105 and application 171i and/or application server 171, such that data transferred between the two nodes is encrypted and also not subject to replay attacks. As contemplated herein, a secure connection can comprise any of a TLS connection, an IPSec connection, a VPN connection, or a LAN connection between server 105 and application server 171 and/or application 171i, and other possibilities exist as well without departing from the scope of the present invention.

Other secure connections may be utilized as well, including a secure shell (SSH) tunnel, future versions of standard secure connections, or also a proprietary protocol for a secure connection. Secure connection setup 801 as illustrated in Figure 8 may utilize a TLS protocol, such as TLS version 1.2. Secure connection setup 801 can include the transfer of a certificate 122 for application server 171, and also the transfer of an application public key 171w. Server 105 can utilize application public key 171w to encrypt data received from module 101 in a message 208, such as sensor data 604b. According to one exemplary embodiment, application message 701 could be ciphered with a symmetric key 127 that comprises a derived shared key 129b from (i) a key derivation function 141f (ii) application public key171w and server public key 114.

The message flow in a secure connection setup 801 also illustrates one benefit of the present invention, where a message 208 can be securely transferred between module 101 and server 105 using a single UDP datagram, while secure connection setup 801 may require a plurality of TCP messages in both directions. In other words, using a secure connection setup 801 between module 101 and server 105 may not be energy efficient for module 101, while using secure connection setup 801 between server 105 and application server 171 can be efficient, since the data from a plurality of modules 101 can be shared over the secure connection setup 801. Also note that since module 101 may sleep for relatively long periods such as 30 minutes or longer, a new secure connection setup 801 would likely be required to support a firewall 104 after each period of sleep, and completing the process of a secure connection setup 801 each time module 101 wakes may not be energy or bandwidth efficient for a module 101.

Petitioner Samsung Ex-1038, 0144

After completing server connection setup 801, server 105 can use a secure connection data transfer 802 to send a first application message 701, where the first application message 701 could include update instruction 704 that includes sensor data 604b that server 105 received in a message 208. Data within the first application message 701 containing update instruction 704 could be ciphered according to the specifications of the secure connection, such as TLS or IPSec, and other possibilities exist as well. Note that server 105 can decrypt a module encrypted data 403 that includes sensor data 604b and subsequently encrypt the sensor data 604b according to the format required by secure connection setup 801 for transfer to application 171i using secure connection data transfer 802. Server 105 can use two different server public keys 114, recorded in the form of a certificate 122 in one embodiment, to with a first server public key 114 used decrypt module encrypted data 403 and a second server public key 114 used encrypt update instruction 704. Server public keys 114 can be used by server 105 in a key derivation function 141f to derive a shared public keys 129b used in a symmetric ciphering algorithm 141b for both secure connection data transfer 802 and module encrypted data 403 (with a different derived shared public key 129b with module 101 and application server 171, respectively).

In another embodiment, server 105 can use the same server public key 114 to both decrypt module encrypted data 403 and encrypt update instruction 704. Other possibilities exist as well for server 105 to use a server public key 114 to (i) encrypt update instruction 704, such as using an asymmetric ciphering algorithm 141a, and (ii) decrypt module encrypted data 403 without departing from the scope of the present invention. As illustrated in Figure 8, server 105 can receive an acknowledgement 804 after sending the first application message 701, with update instruction 704 that includes sensor data 604b, where acknowledgement 804 can signal that application message 701 with update instruction 704 has been received by application 171i and/or application server 171. Although not illustrated in Figure 8, the acknowledgement 804 could optionally include a module instruction 502 for module 101.

After receiving message 208, server 105 can then send a response 209. Response 209 could be sent before or after server 105 sends update instruction 704 to application 171i using secure connection data transfer 802. Response 209 can include a server encrypted data 504 that includes a module instruction 502. Module instruction 502 could be processed by server 105, or could be obtained by server 105 from application 171i in an application instruction 701. In other words, a secure connection data transfer 802 may be utilized by a server 105 and an application server 171 to

Petitioner Samsung Ex-1038, 0145

send a second application message 701 to server 105, and be received by server 105, in addition to the sending the first application message 701 from server 105 to application server 171 that is illustrated in Figure 8.

According to an exemplary preferred embodiment, server 105 waits for a response or acknowledgement 804 from application 171i to application message 701 before sending response 209 to module 101. One reason for waiting for a response or acknowledgement 804 from application 171i is that response or acknowledgement 804 from application 171i could include a module instruction 502, and the module instruction 502 may preferably be included in a response 209. Other possibilities exist as well without departing from the scope of the present invention.

Figure 8 can also illustrate a benefit of an exemplary embodiment contemplated herein. According to an exemplary embodiment, (i) server 105 and application server 171 can utilize a first set of cryptographic algorithms 141 for sending and receiving data between server 105 and application server 171, such as with a secure connection data transfer 802, and (ii) server 105 and module 101 can utilize a second set of cryptographic algorithms 141 for sending and receiving data between server 105 and module 101, such as using the second set of cryptographic algorithms 141 for a module encrypted data 403 and/or server encrypted data 504. In an exemplary embodiment, server 105 and application server 171 can use RSA algorithms 153 in the first set of cryptographic algorithms 141, while server 105 and module 101 can use ECC algorithms 154 in the second set of cryptographic algorithms 141. As one example, server 105 can use an (i) RSA-based asymmetric ciphering algorithm 141b and first server public key 114 with the application server 171 to securely transfer a first symmetric key 127 with application server 171, and (ii) an ECC-based asymmetric ciphering algorithm 141b and second server public key 114 with the module 101 to securely transfer a second symmetric key 127 with a module 101.

Other possibilities exist as well for a server 105 to use a different cryptographic algorithms 141 or parameters 126 for each of application server 171 and module 101. (A) Server 105 and application server 171 could use a first set of parameters 126 for use with cryptographic algorithms 141 for an application message 701 with related server digital signatures, while (B) server 105 and module 101 could use a second set of parameters 126 for use with cryptographic algorithms 141 for a module encrypted data 403 and/or server encrypted data 504 and related digital signatures. In order to maximize security between servers such as server 105 and application server 171, the first

Petitioner Samsung Ex-1038, 0146

set of parameters 126 could specify (i) a longer public and private key length, (ii) a shorter key expiration time 133, (iii) a longer secure hash algorithm (such as an exemplary 512 bits), (iv) a longer symmetric ciphering key 127 length (such as an exemplary 192 or 256 bits), (v) the use of or values for RSA algorithm 153 and a modulus, (vi) the use of Diffie Hellman key exchange or a first key exchange algorithm for a key derivation function 141f and key exchange, (vii) the use of or values for a second symmetric ciphering algorithm 141b for symmetric ciphering, (viii) the use of or values for an RSA digital signature algorithm or a second digital signature algorithm, and similar settings.

In accordance with a preferred exemplary embodiment, in order to minimize processing power and/or energy usage required for a module 101, the second set of parameters 126 could specify (i) a shorter public and private key length, (ii) a longer key expiration time 133, (iii) a shorter secure hash algorithm (such as an exemplary 256 bits), (iv) a shorter symmetric ciphering key 127 length (such as an exemplary 128 bits), and (v) the use of an ECC algorithm 154, (vi) the use of or values for an ECC standard curve 138 and/or ECC parameters 137, (vii) the use of or values for ECDH 159 or a second key exchange algorithm for key derivation and exchange, (vii) the use of or values for of a second symmetric ciphering algorithm 141b for symmetric ciphering, (viii) the use of or values for of ECDSA 158 or a second digital signature algorithm for digital signatures, and similar settings. In an embodiment, the first set of parameters 126 (which can be used by server 105 and application server 171) and the second set of parameters 126 (which can be used by server 105 and module 101) can both specify the use of elliptic curve cryptographic algorithms 141, but with different sets of parameters 126 such that the first set of parameters 126 is selected for server to server communications, and the second set of parameters 126 is selected for communications between a server 105 and a module 101. In another embodiment, the first set of parameters 126 and the second set of parameters 126 can both specify the use of RSA based cryptographic algorithms 141, but with different sets of parameters 126 such that the first set of parameters 126 is selected for server to server communications, and the second set of parameters 126 is selected for communications between a server 105 and a module 101.

In this manner, the use of cryptographic algorithms 141 between (i) server 105 and application server 171 and (ii) server 105 and module 101 can be optimized given different constraints for processing power and energy consumption for server 105, application server 171, and a module 101. In addition, an application server 171 may use cryptographic algorithms 141 and

Petitioner Samsung Ex-1038, 0147

parameters 126 that may not be compatible with cryptographic algorithms 141 and parameters 126 used by a module 101, and server 105 can use cryptographic algorithms 141 and parameters 126 to enable a translation or conversion of encrypted data and digital signatures between a module 101 and an application server 171, thereby establishing connectivity between a module 101 and an application server 171 through a server 105. According to an exemplary embodiment, server 105 can function as a gateway between application server 171 and/or application 171i and a plurality of modules 101.

Figure 9

Figure 9 is a simplified message flow diagram illustrating exemplary data transferred between (i) a server and an application and between (ii) a server and a module, in accordance with exemplary embodiments. An application server 171, a server 105, and a module 101 can send and receive data illustrated in Figure 9. Application server 171 can include application 171i and use an Internet Protocol address and port (IP:port) number 903 for sending and receiving data with server 105. Server 105 can include a server program 101i and a module controller 105x, where server program 101i can access a first server IP:port number 901 for communicating with application server 171, and module controller 105x can access a second server IP:port number 207 for communication with module 101. In accordance with a preferred exemplary embodiment, multiple modules 101 can send data to server IP:port number 207, and thus server 105 and/or a module controller 105x can use a single IP:port number 207 to communicate with a plurality of modules 101. In addition, server 105 could specify that one subset of modules 101 communicate with a first IP:port number 207, and a second subset of modules 101 communicate with a second IP:port number 207, etc. In another embodiment, server 105 could use multiple Internet Protocol addresses for sending and receiving data with a module 101, although a given module 101 can preferably send a message 208 to IP:port number 207 and receive a response 209 from the IP:port number 207, and a different module 101 could use a different value for IP:port number 207, including potentially a different IP address 106. Module 101 can utilize an IP:port number 204 for sending and receiving data with server 105.

As illustrated in Figure 9, a symmetric firewall 104 could be included between module 101 and server 105, and the of IP addresses and port numbers in packets between server 105 and module

Petitioner Samsung Ex-1038, 0148

101 illustrated in Figure 9 could also represent routing if a firewall 104 is present and functions as a symmetric firewall without NAT routing. In this case, firewall 104 may not perform network address translation on source and destination IP addresses, but rather filter packets based on pre-determined rules. For example, a firewall 104 that is a symmetric firewall could drop inbound packets from IP:port number 207 to module 101 unless module 101 had previously sent a packet to IP:port number 207 within a firewall port binding timeout value 117. Alternatively, a firewall 104 may be optionally omitted, and in this case the destination address in packets sent from server 105 to module 101 could include the IP address 202 of module 101, which is also the case illustrated in Figure 9. In other words, Figure 9 illustrates an exemplary routing of packets in the cases that (i) firewall 104 is a symmetric firewall, and (ii) firewall 104 is optionally not present.

Server 105 can receive a message 208 from a module 101. Server 105 can use a module controller 105x to receive the message, and module controller 105x could also be identified as a process operating on server 105 that binds to the port number in IP:port 207, which could include a port number 205. Message 208 could include module identity string 904, which could represent a temporary or transient string or number used by module 101 and server 105 to associate and identify message 208 with module identity 110. Module identity string 904 could also comprise a module identity 110. Server 105 can use module identity string 904 to select a symmetric key 127 in order to decrypt module encrypted data 403, since module identity string 904 may preferably be not encrypted. Server 105 and module 101 could use an algorithm within cryptographic algorithms 141 in order to process a module identity string 904, whereby the module identity string 904 can be converted between (i) a module identity 110 in a form such as a serial number or IMEI within module 101 and/or server 102, and (ii) a module identity string 904 in a message 208 that can traverse the Internet 107.

Message 208 as received by server 105 can also include a server instruction 414 within a module encrypted data 403, where the module encrypted data 403 could be ciphered using a symmetric key 127. The server instruction 414 illustrated in Figure 9 can be an exemplary "update" instruction, where the "update" instruction can include a security token 401 and sensor data 604b. Sensor data 604b can include a sensor identity 151 and a sensor measurement. Server instruction 414 within a message 208 could include many other values besides an update, including a registration, a query, an alarm or error notification, configuration request, software request, confirmation, or other values also depicted and described in connection with a server instruction

Petitioner Samsung Ex-1038, 0149

414 in Figure 4. Although message 208 is illustrated as a UDP datagram 601a in Figure 9, message 208 could also be transmitted as a TCP datagram or other Internet transport protocols including Datagram Congestion Control Protocol (DCCP) and Stream Control Transmission Protocol (SCTP). A security token 401 can comprise a random number 128a processed by a random number generator 128 and can be preferably not reused and therefore can keep message 208 unique and not subject to replay attacks. Since a UDP protocol may be implemented for message 208, and the connectionless UDP protocol may require a module 101 to send retransmissions of a UDP datagram 601a for message 208, if module 101 does not receive a response 209 within a specified timer period.

According to an exemplary preferred embodiment, server 105 can include a timer 905, such that multiple UDP datagrams 601a received within the timer 905 period may be processed, but datagrams received outside the expiration of the timer 905 would be dropped. Note timer 905 can be particularly useful for security of a system 100 when module 101 may transmit multiple copies of UDP datagram 601a. Module 101 may transmit multiple copies of a UDP datagram 601a in order to implement forward error correction and compensate for any packet loss on the Internet 107 or possibly with wireless network 102. The UDP datagram 601a may also be sent as a UDP Lite datagram with channel coding 406. Server 105 can start timer 905 when the first UDP datagram 601a in message 208 is received, and discard UDP datagrams 601a for message 208 after the timer 905 expires, such as after an exemplary 2 seconds although other possibilities exist as well. In this manner (i) module 101 can securely send multiple copies of the same UDP datagram 601a in message 208, and (ii) server 105 can remain robust against replay attacks. Server 105 can also reset the timer 905 to a zero value upon sending response 209, and the timer value 905 could start again upon the receipt of a first UPD datagram 601a in the next message 208.

If the UDP Lite protocol is utilized for message 208 with multiple copies of UDP Lite datagram 601a received, then each UDP Lite datagram 601a could be different, depending on the presence of bit errors in the datagram, and thus server 105 can use timer 905 to collect the multiple copies of UDP Lite datagram 601a within the timer 905 period and process the multiple packets received, including combining the data across multiple packets, in order to eliminate bit errors within the datagrams and collect an error-free message 208.

After receiving message 208, server 105 use the steps outlined in Figure 5a to process message 208 and read the plaintext server instruction 414, such as the sensor data 604b illustrated in

Petitioner Samsung Ex-1038, 0150

Figure 9. Other possibilities exist as well for sensor data 604b or values or information inside a server instruction 414. Server 105 can then send or transmit a first application message 701 to application server 171 that includes data received from the server instruction 414 from module 101 in message 208. The data received in the server instruction 414 from module 101 could be included by server 105 in an update instruction 704. An application 171i operating within application server 171 or associated with application server 171 could receive the first application message 701. The first application message 701 could be formatted according to a TCP datagram 902, although other possibilities exist as well including UDP.

In accordance with an exemplary preferred embodiment, the first application message 701 may include an update instruction 704 with sensor data 604b, although update instruction 704 could also contain or include other data pertaining to module 101 besides sensor data 604b, such as a state of a component with module 101, a state of a software routine, variable, or parameter associated with module 101. The first application message 701 sent from server 105 to application server 171 could be a datagram within a secure connection data transfer 802 as illustrated in Figure 8. Sensor data 604b could be sent by server 105 using application server public key 171w, such as either (i) mutually deriving a common shared key 129b between server 105 and application 171i using a key derivation function 141f, where the shared key 129b could function as a symmetric key 127 with a symmetric ciphering algorithm 141b, or (ii) server 105 sending a symmetric key 127 to application server 171 using an asymmetric ciphering algorithm 141a and the application server public key 171w. Message 805 in Figure 8 with the label of "Client Key Exchange" can comprise server 105 sending a symmetric key 127 (or value or parameter 126 for deriving symmetric key 127) to application server 171, where the symmetric key 127 can be used by server 105 to encrypt update instruction 704 illustrated in Figure 9.

In accordance with an exemplary preferred embodiment, application message 701 may include (i) module identity 110 encrypted within secure connection data transfer 802 and also a server identity 206 that is not encrypted. In this manner, application server 171 can use server identity 206 to select a symmetric key 127 (possibly sent in message 805 as described in the paragraph above) in order to decrypt the encrypted data in update instruction 704. Although not illustrated in Figure 9, in accordance with another exemplary embodiment, both a message 208 and the first application message 701 may also include a module digital signature 405. Server 105 can forward the module digital signature 405 received in a message 208 with sensor data 604b to the

Petitioner Samsung Ex-1038, 0151

application server 171 in the first application message 701 illustrated in Figure 9. The module digital signature 405 in a first application message 701 does not need to be encrypted. The application server 171 can verify the module digital signature 405 using step 411 of Figure 4 (using a module public key 111). In this manner, application 171 can verify that module 101 originated the sensor data 604b, even though application server 171 received the application message 701 from server 105.

Application server 171 can receive the first application message 701 sent by server 105 and process the message. The message processing by application server 171 could use steps similar or equivalent to the steps utilized by server 105 illustrated in Figure 4, in order to extract a plaintext application instruction 704. Although not illustrated in Figure 9, application 171i could record data received within application instruction 704 and record the data in an application database 171k. Application 171i could use the data received in application instruction 704 or a plurality of application instructions 704 to generate reports, graphs, emails, or other user information for a user 183.

Upon processing the information within application instruction 704, application 171i or application server 171 could send a second application message 701 to server 105, as illustrated in Figure 9. The second application message 701 could be sent using a secure connection data transfer 802, and could include a module instruction 502 and a module identity 110. The second application message 701 can use the IP:port number 903 as a source IP:port number for the second application message 701, where IP:port number 903 also represented a destination IP:port number for the first application message 701. The second application message 701 can use the IP:port number 901 as the destination IP:port number, where IP:port number 901 was the source port number in the first application message 701. The module instruction 502 within the second application message 701 can comprise could include an actuator setting 706. The module instruction 502 within the second application message 701 can comprise other data or module instructions 502 for a module 101 that do not include an actuator setting 706, such as the exemplary data depicted and described in connection with Figure 5a.

Either server 105 or application server 171 could use the application server public key 171w to process the second application message 701. As one example, server 105 and/or application server 171 could use a key derivation function 141f to derive a key, where key derivation function

Petitioner Samsung Ex-1038, 0152

141f used application server public key 171w. The derived key could be used to encrypt and/or decrypt the module instruction 502 in the second application message 701. Other possibilities exists as well for the second application message 701 to use the application server public key 171w, such as server 105 sending a symmetric key 127 (used to encrypt and/or decrypt module instruction 502 in the second application message 701), where they symmetric key 127 was ciphered using the application server public key 171w.

Server 105 can received the second application message 701, and the message could be received using an IP:port number 901. Although an IPv4 address is shown in Figure 9, and IPv6 address could be utilized as well. Server 105 could decrypt a body 602, that contains module identity 110 and a module instruction 502, using algorithms specified according to a secure connection data transfer 802. According to an exemplary embodiment, a secure connection data transfer 802 between a server 105 and an application server 171 could also comprise the steps for encrypting/decrypting and signing/verifying that are depicted and described in connection with Figure 4 and Figure 5a, and thus secure connection data transfer 802 could also optionally use the same steps and procedures between server 105 and application server 171 that are contemplated between server 105 and module 101. As one example, the application message 701 packets illustrated in Figure 9 sent between server 105 and application 171 could be formatted to UDP and include a server encrypted data 504. As depicted and described in Figure 8, a first set of parameters with cryptographic algorithms 141 could be used with an application message 701 and a second set of parameters 126 with cryptographic algorithms 141 could be used with server encrypted data 504 and/or module encrypted data 403.

After extracting a plaintext module instruction 502 and module identity 110 from a body 602 in the the second application message 701, server 105 can take steps to process the data within a response 209 for module 101. Server 105 can record or query for information pertaining to module 101 using module identity 110 in a module database 105k. In accordance with exemplary embodiments, server 105 can use module identity 110 received in the second application message 701 to select (i) a symmetric key 127 used by module 101 for encrypting and/or decrypting a server encrypted data 504 that can include the module instruction 502, (ii) a destination IP:port number 204 for sending a response 209, (iii) a source IP:port number 207 for sending a response 209, (iv) a determination if a wait interval 703 is required before sending response 209, (v) a security token 401, and (vi) a set of parameters 126 for use with a cryptographic algorithms 141 in

Petitioner Samsung Ex-1038, 0153

communications with module 101. In one embodiment, different modules 101 connected to server 105 may use different parameters 126, and server 105 can select the parameters 126 using (i) the module identity 110 received in the second application message and (ii) a module database 105k. Server 105 can also use module identity 110 received in the second application message 701 to select (vii) a transport protocol for a response 209, such as TCP, UDP, or UDP Light, and (viii) a channel coding 406 parameter such as a block code, turbo code, or forward error correction coding scheme. Server 105 can use module identity 110 received in application message 701 to format and/or send a response 209 to module 101.

According to a preferred exemplary embodiment, server 105 may receive an application message 701 with data for a module 101 at arbitrary times. Server 105 could also receive an application message 701 at a time when a first application message 701 with module identity 110 has not (i) previously been sent by server 105, (ii) or sent in a comparably long time such as a day or a week. As noted previously, server 105 may not be able to send a module instruction 502 to module 101 at arbitrary times, because of either (i) a sleep or dormant period for module 101, and/or (ii) the presence of a firewall 104. Thus, server 105 may need to (i) receive a message 208 from module 101 (such as upon waking after a sleep period after a firewall port binding timeout value 117 period since the last message 208) before (ii) sending a module instruction 502. Consequently, according to a preferred exemplary embodiment, server 105 can use module identity 110 received within an application message 701 to determine (i) if server 105 should wait until a wait interval 703 expires before sending response 209 (where the wait interval 703 can end upon receipt of a message 208 from a module 101 with the module identity 110 received in the application message 701) or (ii) if server 105 can send response 209 right away (such as a firewall port binding timeout period 117 has not expired), where response 209 includes the module instruction 502 received in the application message 701.

After (A) using module identity 110 received within application message 701 to select values within a response 209 and timing for sending a response 209, then (B) server 105 can send response 209 as illustrated in Figure 9, where the specific response 209 in Figure 9 is exemplary. Response 209 can include a server encrypted data 504. Server encrypted data 504 can include module instruction 502. The exemplary response 209 illustrated in Figure 9 includes an actuator setting 706 within module instruction 502, but other possibilities exist as well. Note that the use of server encrypted data 504 is optional within a response 209, and server 105 could send module

Petitioner Samsung Ex-1038, 0154

instruction 502 as plaintext. However, in this case of module instruction 502 being sent as plaintext, server 105 can preferably include a server digital signature 506 such that module 101 can verify the server digital signature 506 using the server public key 114 and confirm the module instruction 502 was transmitted by server 105. In accordance with exemplary preferred embodiments, (i) a message from module 101 to server 105 that does not include a module encrypted data 403 preferably includes a module digital signature 405, and (ii) a response 209, message sent back, datagram, or packet from server 105 to module 101 that does not include a server encrypted data 504 preferably includes a server digital signature 506. If data is not encrypted within a packet and the packet includes plaintext instructions such as a module instruction 502 or a server instruction 414, then, in accordance with preferred exemplary embodiments, the receiving node can preferably verify the identity of a sender using a digital signature included in the packet.

Response 209 sent from server 105 to module 101 could include a checksum 603. Since firewall 104 may comprise a symmetric firewall 104 (that may not perform network address translation routing), the destination address within IP:port 204 in response 209 illustrated in Figure 9 may match the IP address 202 used by module 101. In this case, where the destination IP:port in response 209 includes IP address 202, a checksum 603 sent by server 105 can be equal to a checksum 603 received by module 101. In accordance with exemplary embodiments, response 209 is transmitted or sent by server 105 within a firewall port binding timeout value 117 after message 208 was received by server 105. In other words, if a firewall port binding timeout value 117 was equal to an exemplary 20 seconds for UDP packets, the response 209 illustrated in Figure 9 would preferably be sent in less than 20 seconds after receiving the last message 208.

Figure 10

Figure 10 is a flow chart illustrating exemplary steps for a server to receive a module instruction within an application message, and for the server to send the module instruction to a module, in accordance with exemplary embodiments. Since an application 171i operating with an application server 171 may utilize a different set of protocols for communications than a module 101, server 105 can provide connectivity between module 101 and application 171i. As illustrated

Petitioner Samsung Ex-1038, 0155

in Figure 8 and Figure 9 above, a server 105 can receive an application message 701 from an application server 171. The application server 171 and/or application 171i could be identified by the source IP address in an application message 701 received by server 105. Application message 701 could include encrypted data using a secure connection data transfer 802, where a body 602 within a packet could include a module instruction 502 and a module identity 110. As illustrated in system 199 in Figure 1i, server 105 can support a network with a plurality of modules 101, and thus a module identity 110 within an application message 701 can be useful to (i) select the proper destination of module instruction 502, and (ii) other values for sending a response 209 to module 101 as depicted and described in connection with Figure 9 above.

At step 1001, server 105 can preferably utilize the protocol for the secure connection data transfer 802 (such as TLS illustrated in Figure 8) to extract the plaintext module instruction 502 and module identity 110. Server 105 could use a first symmetric key 127 with application server 171, such as (i) a first symmetric key 127 derived or transmitted with message 805 and (ii) a symmetric ciphering algorithm 141b. After extracting plaintext from application message 701, server 105 can record the data in a module database 105k, or simply store the data for further processing in a memory 101e. Although not depicted in Figure 10, server 105 could use a message pre-processor 105y to send and receive data with application server 171, where the message pre-processor could comprise a program or library such as a TLS library, and IPSec library, an SSH library, etc.

Server 105 can then wait for a wait interval 703, where server 105 waits for an incoming message from module 101. Server 105 may need to wait for the wait interval 703 because the module may sleep or be dormant, and also a firewall 104 may block inbound packets or datagrams from server 105 to module 101 if module 101 had not previously sent a packet within a firewall port binding timeout value 117. After the wait interval 703, server 105 can use step 503 to encrypt module instruction 502 using a second symmetric key 127 and a security token 401, where the second symmetric key 127 is different than the first symmetric key 127. As illustrated in Figure 5a, the output of step 503 can be a server encrypted data 504. Although step 503 is illustrated as after wait interval 703 in Figure 10, step 503 could also take place either (i) before wait interval 503 or (ii) concurrently with wait interval 703.

According to exemplary embodiments, a first symmetric key 127 used by server 105 and application server 171 is different than a second symmetric key 127 used by module 101 and server

Petitioner Samsung Ex-1038, 0156

105. In addition, according to an exemplary embodiment, server 105 may use an RSA algorithm 153 for asymmetric ciphering 141a in packets with application server 171 and an ECC algorithm 154 for asymmetric ciphering 141a in packets with a module 101. Thus, according to an exemplary preferred embodiment, server 105 can utilize (i) a first certificate 122 with an RSA-based server public key 114 for use in communication with application server 171i and (ii) a second certificate 122 with an ECC-based server public key 114 for use in communication with a module 101. In an exemplary embodiment, the first symmetric key 127 is associated with a first symmetric ciphering algorithm 141b between server 105 and application server 171, and the second symmetric key 127 is associated with a second symmetric ciphering algorithm 141b between server 105 and module 101, and the first and second symmetric ciphering algorithms 141b are different. As depicted and described in connection with Figure 8, the first and second symmetric ciphering algorithms 141b may use different parameters 126, such as a first set of parameters 126 with the first symmetric ciphering algorithms 141b and a second set of parameters 126 with the second symmetric ciphering algorithms 141b.

Server 105 can receive a message 208 from module 101, where the module identity 110 or module identity string 904 in message 208 could represent a number or string associated with the module identity 110 in application message 701. Note that the exact string, number, or digits in module identity 110 or module identity string 904 in message 208 does not need to match the exact string, number, or digits for module identity 110 in application message 701, and the two messages could use different encoding schemes or values for module identity 110. As one example, module identity 110 in application message 701 could represent a serial number for module 101, while module identity 110 in message 208 could represent a session identity. Other possibilities exist as well for a string or number within a module identity 110. Server 105 can preferably uniquely associate module identity 110 in an application message 701 with module identity 110 in a message 208.

After receiving message 208, server 105 can send the server encrypted data 504 processed in step 503 above within a response 209. A server encrypted data 504 within response 209 could include the module instruction 502, where module instruction 502 was received in the application message 701. Note that module instruction 502 within response 209 does not need to be the exact same string, number, or binary digits as module instruction 502 received by server 105 in application message 701. As one example, application message 701 and response 209 could use

Petitioner Samsung Ex-1038, 0157

different coding schemes (such as ASN.1 for response 209, and plaintext for application message 701, although other possibilities exist as well). As illustrated in Figure 10, module instruction 502 within an application message 701 can preferably represent an equivalent action for module 101 as a module instruction 502 within response 209. For example, module instruction 502 in both application message 701 and response 209 could instruct module 101 to (i) throw a switch, (ii) sleep for an interval, (iii) adjust a power level, and other possibilities exist as well. As described above in Figure 9, the use of encryption within response 209 could optionally be omitted, but in this case response 209 may include a server digital signature 506 with module instruction 502.

After sending response 209, at step 1002 the server 105 may preferably receive a confirmation from module 101 that the module instruction 502 had been successfully received and/or successfully applied. The confirmation could be received in the format of a second message 208 from module 101 with a server instruction 414, where the server instruction 414 is a "confirmation". Other data regarding the execution of module instruction 502 by module 101 could be included in the confirmation at step 1002, such as a timestamp 604a when the module instruction 502 was executed. After receiving the confirmation from the module 101, server 105 can preferably send a second application message 701 to an application server 171 and/or application 171i with a confirmation 705. The confirmation 705 could be sent using a secure connection data transfer 802. In accordance with exemplary embodiments, the application message 701 sent from server 105 to application server 171 in the form of a confirmation 705 can include the timestamp 604a.

In an exemplary embodiment, the reliable and secure transmission of timestamp 604a from module 101 to application server 171 through server 105 may be useful for proper management of a monitored unit 119. Due to any sleep or dormant states of module 101, plus periodic outages and recovery of wireless network 102, a first time value that module 101 executes module instruction 502 may be significantly different than a second time value that application server 171 sent the module instruction 502. Consequently, application server 171 may preferably receive a timestamp 604a sent by module 101 in an application message 701 from server 105, and the application message 701 could comprise a confirmation 705.

Although not illustrated in Figure 10, server 105 could then continue listening on or monitoring (i) IP:port 901 for additional incoming application messages 901 from application server 171, and (ii) IP:port 207 for additional incoming messages 208 from a module 101. Although not

Petitioner Samsung Ex-1038, 0158

illustrated in Figure 10, module instruction 502 may optionally be encrypted such that server 105 may not be able to read plaintext within module instruction 502, and in this case step 1001 illustrated in Figure 10 would be bypassed. For example, module instruction 502 may be encrypted with the module public key 111, and thus module instruction 502 may only reasonably be read by module 101. Even if module instruction 502 cannot be read in plaintext form by server 105 upon receiving application message 701, module identity 110 within application message 701 would preferably be in a form where server 105 can (i) process the module identity 110 into plaintext (as a minimum in order to route the message to module 101 among a plurality of modules 101), or (ii) simply read the module identity 110 from a body 602 in the application message 701.

In this embodiment where step 1001 is omitted in Figure 10, the application server 171 can use a module public key 111 and an asymmetric ciphering algorithm 141a to encrypt the module instruction 502 shown in the body 602 of the application message 701 illustrated in Figure 9. The application server 171 can also include a digital signature of the module instruction 502 using the application server private key 171t and a digital signature algorithms 141d. The encrypted module instruction 502, module identity 110, and digital signature can be sent to the server 105 in an application message 701 using the first step shown in Figure 10. The application message 701 can also include an identity of the application server.

Continuing in this embodiment where step 1001 is omitted in Figure 10, the server 105 can then use the waiting interval 703 until a message 208 is received from a module 101. In this case where step 1001 is omitted in Figure 10, then step 503 can also be omitted since the module instruction 502 is already encrypted with the module public key 111 (by the application server 171). After skipping step 503 and receiving the message 208, the server 105 can then send the encrypted module instruction 502 and digital signature (signed by the application server 171) to the module 101 in a response 209, as shown in Figure 10. The module 101 can read receive the response 209, read the identity of the application server, select a public key 171w of the application server 171, verify the digital signature of the module instruction 502, and decrypt the module instruction 502 using the module private key 112 and an asymmetric ciphering algorithms 141a. The module 101 can then apply the module instruction 502 and send a message 208 with a confirmation at step 1002. The confirmation at step 1002 can include a timestamp 604b, which the server 105 can send to the application server 171. In this manner, the module 101 may receive instructions from the application server 171i that are not encrypted by the server 105.

Petitioner Samsung Ex-1038, 0159

Figure 11

Figure 11 is a flow chart illustrating exemplary steps for a server to communicate with an application and a module, in accordance with exemplary embodiments. Figure 11 includes a combination of different exemplary embodiments contemplated in the present invention, including (i) receiving a first module encrypted data 403 with a first sensor data 604b from a module 101 using a first public key 111, (ii) sending the first sensor data 604b in a first application message 701, (iii) sending a module instruction 502 for a module 101 to derive a new public and private key pair using a set of parameters 126, (iv) receiving a second module encrypted data 403 with a second sensor data 604b from module 101 using the second public key, and (iv) sending the second sensor data 604b in a second application message 701.

Server 105 can receive a first module public key 111 at step 516. The first module public key 111 can be in a message 208 that includes a module identity 110 and first parameters 126, where the parameters can provide values associated with the first module public key 111 such as an elliptic curve name or defining equation, a modulus for an RSA key, a time-to-live value, a certificate authority 118 name, etc. According to an exemplary embodiment, a set of parameters 126 can include a module public key identity 111a, in addition to other values. Server 105 can receive the first module public key 111 at step 516 in the form of a certificate 122, although a certificate 122 is not required. Although not illustrated in Figure 11, module public key 111 could optionally be encrypted in a module encrypted data 403, as depicted and described in connection with Step 1001 of Figure 10 in U.S. Patent Application Serial No. 14/039,401. In addition, the submission of the first module public key 111 at step 516 could be authenticated using step 517 of Figure 5b of the present invention. In this manner, server 105 can ensure that the first module public key 111 is properly associated with module identity 110 and/or module 101 (i.e. prevent an incorrect submission of the first module public key 111 or even the potential malicious submission of the first module public key 111). In accordance with a preferred exemplary embodiment, the first message 208 received at step 516 can also include a module public key identity 111a, so that server 105 can properly keep track of multiple different module public keys 111 used by a module 101 over time, such as module 101 periodically rotating public/private key pairs in order to enhance security.

Petitioner Samsung Ex-1038, 0160

At step 1101, server 105 can receive a second message 208 that includes a first module encrypted data 403, where the first module encrypted data 403 was processed by server 105 using the first module public key 111 and first set of parameters 126 received in step 516. In accordance with an exemplary preferred embodiment, server 105 can use the first module public key 111 to process the first module encrypted data 403 by (i) mutually deriving a common shared secret key 129b as a symmetric key 127 for use between server 105 and module 101 using a key derivation function 141f with the first module public key 111 as an input into the key derivation function 141f, and (ii) server 105 sending a symmetric key 127 to module 101 where (ii.a) the symmetric key 127 was ciphered using an asymmetric ciphering algorithm 141a and the first module public key 111 and (ii.b) the first module encrypted data 403 was ciphered using the symmetric key 127. Note that the second message 208 could be optionally sent without ciphering or encryption, and in this case the second message 208 could use the first module public key 111 to include a module digital signature 405 in the second message 208. The second message 208 can include a sensor data 604b or other server instruction 414. According to an exemplary embodiment, the second message 208 may also preferably include a module identity 110 or a module identity string 904 outside of the module encrypted data 403, so that server 105 can select the proper key in order to decrypt the module encrypted data 403.

At step 1102, server 105 can use an application message 701 to send the sensor data 604b from a sensor 101f with module 101 to an application server 171 and/or an application 171i. As illustrated in Figures 8 and Figure 9, the application message 701 can use a secure connection data transfer 802, and could comprise an update instruction 704. The application message 701 can include both a module identity 101 and a server identity 206, and the server identity 206 can be useful for application server 171 since the application server 171 could receive a plurality of application messages 701 from a plurality of servers 105, each using a different key for ciphering. Although not illustrated in Figure 11, steps 1101 and 1102 could be completed in series multiple times before proceeding to step 1103, such as module 101 sending multiple messages 208 with sensor data 604b over several days or longer, and server 105 can correspondingly send the data to an application server 171.

At step 1103, server 105 can process a module instruction 502 for module 101 to derive a second module public key 111 and a second private key 112. Potential reasons for the use of a new public and private key by module 101 are described in connection with Figure 5b and elsewhere

Petitioner Samsung Ex-1038, 0161

herein, and could include the expiration the validity of a certificate 122 with the first module public key 111 among many possible reasons. Although server 105 is illustrated as processing the module instruction 502 at steps 1103, an application server 171 or another server associated with M2M service provider 108 or module provider 109 could send a signal to server 105 for module 101 to derive new keys, and server 105 could then send module 101 a module instruction 502 to derive new keys at step 1103. In an exemplary embodiment, any module instructions 502 originated outside server 105 in a system 100 illustrated in Figure 1 may preferably be sent to server 105 before sending to module 101, since other servers besides server 105 in a system 100 illustrated in Figure 1 would not normally be able to send a packet to module 101 due to the presence of firewall 104. In accordance with an exemplary preferred embodiment, (i) module 101 may only receive a module instruction 502 from a server 105, where server 105 had previously received a message 208, (ii) before module 101 receives the module instruction 502. Further, module 101 may only receive a module instruction 502 both (i) after sending a message 208 and (ii) before the expiration of a firewall port binding timeout value 117 after sending the message 208.

Server 105 can then use step 503 illustrated in Figure 5a to encrypt (i) the module instruction 502 and (ii) the second parameters 126 in a server encrypted data 504, where the module instruction 502 comprises an instruction for module 101 to derive a new pair of keys. Server 105 can use a symmetric key 127 and a symmetric ciphering algorithm 141b to encrypt the module instruction 502 and second parameters 126. The symmetric key 127 used in step 503 illustrated in Figure 11 could be processed using the first module public key 111, where server 105 had (i) verified the identity of module 101 using a module digital signature 405 using the first module public key 111, and then (ii) subsequently sent or received the symmetric key 127 with module 101 after the module digital signature 405 was verified using the first module public key 111. Alternatively, server 105 could have sent the symmetric key 127 to module 101 in a response 209 using an asymmetric ciphering algorithm 141a and the first module public key 111. Although not illustrated in Figure 11, in a different but related embodiment to Figure 11, step 506 can be substituted for step 503, such that module instruction 502 and/or second parameters 126 are not encrypted but rather a server digital signature 506 processed for inclusion in a response at step 1104 below.

At step 1104, server 105 can then send a response 209 that includes the module instruction 502 and second parameters 126, where the module instruction 502 could be included in a server

Petitioner Samsung Ex-1038, 0162

encrypted data 504. The response 209 could be formatted according to the exemplary response 209 illustrated in Figure 6a, where the response 209 can include a module instruction 502 for the module 101 to derive a new key pair. The response 209 could be to (i) the second message 208 received at step 1101, or (ii) a subsequent message 208 received by server 105 after the second message 208 received in step 1101 and not shown in Figure 11. The response 209 at step 1104 can also include a second set of parameters 126 and a security token 401. As contemplated herein, the terms "parameters" and "set of parameters" may be considered equivalent. If response 209 at step 1104 does not include a server encrypted data 504, then response 209 at step 1104 may preferably include a server digital signature 506.

The second set of parameters 126 at step 1104 could be related to the first set of parameters 126 at step 516 illustrated in Figure 11, or may be different. As one example, a second set of parameters 126 could include a different expiration date or time-to-live value for a new module public key 111. The second set of parameters 126 could include a new elliptic curve name or values for a defining equation, including a new elliptic curve for a cryptographic algorithms 141 to be utilized by module 101. Thus, according to a preferred exemplary embodiment, a set of parameters 126 sent to a module in a response 209 can include values for an elliptic curve defining equation. In this manner, module 101 and server 105 can utilize an elliptic curve for an ECC algorithms 154 that is different than an ECC standard curve 138. For example, module 101 and server 105 may prefer to use an elliptic curve for ECC algorithms 154 that is different than defined curves in standards such the list of curve names in section 5.1.1 of IETF RFC 4492 entitled "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)", and other related curves such as defined curves published by NIST.

One benefit of utilizing a non-standard elliptic curve (where the curve can be defined using a ECC parameters 137 in a parameters 126) is that security can be increased, since attempts to break encryption with standard elliptic curves could not be readily applied to non-standard elliptic curves used in an ECC algorithm 154 (i.e. rainbow tables and the like generated for one elliptic curve would not normally be applicable for a sufficiently different elliptic curve). In accordance with a preferred exemplary embodiment, at step 1104 the second set of parameters 126, which can include values for a defining equation and/or ECC parameters 137, can be sent to a module 101 in a response 209, where the parameters 126 are within a server encrypted data 504. The security of a system 100 can be increased by keeping confidential the elliptic curve used in an ECC algorithm

Petitioner Samsung Ex-1038, 0163

154. By sending ECC parameters 137 (possibly within the second set of parameters 126) in a server encrypted data 504 in a response 209, where ECC parameters 137 include values for a different elliptic curve for module 101 to utilize in a cryptographic algorithms, the security of a system 100 can be further increased since the underlying elliptic curves used with public and private keys can change over time.

Module 101 can receive the response 209 sent in step 1104 with the module instruction 502 instructing module 101 to derive a new key pair using the second set of parameters 126. Note the second set of parameters 126 could be omitted in the response 209 sent in step 1104 and in this case module 101 can use the first set of parameters from step 516 illustrated in Figure 11. Module 101 can decrypt the server encrypted data 504 in a response 209 using a symmetric key 127 and/or the first module public key 111 sent in the first message at step 516 shown in Figure 11. At step 515, module 101 can derive the new key pair using the second set of parameters 126. As depicted and described in connection with Figure 5b, module 101 can use the second set of parameters 126, cryptographic algorithms 141, a key pair generation algorithms 141e, and a random number generator 128 to derive a second module public key 111 and a second module private key 112. The random number generator 128 could use input from a sensor 101f, radio 101z, and other hardware in order to input "noisy" data into a seed 129 used by random number generator 128, including using a module random seed file 139.

At step 1105, server 105 can receive the second module public key 111 from module 101 in a third message 208. The third message 208 could include a module identity 110, and the second module public key 112 could be authenticated by server 105 using step 517 depicted and described in connection with Figure 5b above. Note that the third message 208 may also preferably include a module public key identity 111a, so that server 105 can properly track and identify which of a plurality of module public keys 111 may be used. Module public key identity 111a and module public key 111 could be received by server 105 in the form of a certificate 122, although the use of a certificate 122 is not required. Server 105 can authenticate the second module public key 111 at step 1105 using the first module public key 111 received in step 516 in Figure 11. In one embodiment, the second module public key 111 could be authenticated by server 105, where the third message included a module digital signature 405 that module 101 processed using the first module private key 112. Server 105 could use the first module public key 111 and the first set of parameters 126 received in (or used with) step 516 of Figure 11 to verify the module digital

Petitioner Samsung Ex-1038, 0164

signature 405. In this manner, the second module public key 111 could be authenticated with or after step 1105 by server 105.

Upon receiving and authenticating the second module public key 111, server 105 can record the second module public key 111 in a module database 105k or store the key in other memory. After recording the second module public key 111, at step 1106 server 105 can receive a fourth message 208 that includes (i) a module identity, and (ii) a second module encrypted data 403, where the second module encrypted data 403 may be encrypted using the second module public key 111 received at step 1105. The second module encrypted data 403 could include second sensor data 604b or other data as well. Server 105 can decrypt the second module encrypted data 403 in order to extract the plaintext sensor data 604b, or other data for a server 105 or application 171i, including a server instruction 414 different than an "update" message.

At step 1107, server 105 can then send a second application message 701 to an application server 171 and/or application 171i, were the second application message could include the sensor data 604 received in step 1105 and the module identity 110. Server 105 can utilize a secure connection data transfer 802 to send the sensor data 604b and the module identity 110 received in step 1106. In an exemplary embodiment, the keys used for a secure connection data transfer 802 at step 1107 could be the same as used in the secure connection data transfer 802 at step 1102. In this manner, server 105 can support a change in public and private keys for module 101, while no change in public and private keys are required for application server 171 and/or application 171i. Further, application 171i may require a valid certificate 122 for server 105, while server 105 may not require a certificate 122 for each module 101. Although not illustrated in Figure 11, steps 1106 and 1107 could repeat in sequence as server 105 continues to receive additional messages 208 from module 101 over time, and server 105 could continue to update application server 171 and/or application 171i by sending additional application messages 701. Application 171i can use the plurality of sensor data 604b received in Figure 11 to update an application database 171k and information presented to a user 183 though a web portal 171j.

Petitioner Samsung Ex-1038, 0165

Conclusion

Various exemplary embodiments have been described above. Those skilled in the art will understand, however, that changes and modifications may be made to those examples without departing from the scope of the claims.

Petitioner Samsung Ex-1038, 0166

CLAIMS

What is claimed is:

1. A mobile device comprising:

(a) at least one processor; and

(b) at least one computer-readable medium operatively connected to the at least one processor and having stored thereon instructions that, when executed by the at least one processor, cause the mobile device to perform a method of authentication with a wireless network, the method comprising:

(1) storing a server public key, a module identity, cryptographic algorithms, and a pre-shared secret key, wherein the module identity comprises a permanent identifier for the mobile device and the cryptographic algorithms includes a symmetric ciphering algorithm;

(2) deriving a module private key and a corresponding module public key using the cryptographic algorithms;

(3) deriving a symmetric ciphering key using (i) an elliptic curve integrated encryption scheme with the server public key and the module private key and (ii) an American National Standards Institute standard X-9.63 key derivation function;

(4) generating a module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm, wherein the module encrypted data includes the module identity;

(5) sending a message to a server for the wireless network, the message comprising the module encrypted data and the module public key, wherein the server mutually derives the symmetric ciphering key using at least the module public key, and wherein the wireless network selects the pre-shared secret key for the mobile device using the module identity; and

(6) authenticating with the wireless network using a message digest with the pre-shared secret key.

Petitioner Samsung Ex-1038, 0167

2. The mobile device of claim 1, wherein the message further comprises a module identity string, the module identity string comprising a temporary identification for the mobile device.

3. The mobile device of claim 1, wherein the pre-shared secret key comprises a key K, wherein the mobile device and the wireless network mutually derive a response from (i) a random value and (ii) the key K, and wherein the mobile device receives the random value from the wireless network.

4. The mobile device of claim 1, wherein, in step (1), the pre-shared secret key is stored within a subscriber identity module card, the pre-shared secret key comprising a key K.

5. The mobile device of claim 1, wherein, in step (1), the pre-shared secret key is stored before the mobile device communicates with the wireless network.

6. The mobile device of claim 1, further comprising, in step (1), storing parameters for the cryptographic algorithms, the parameters comprising a standard curve for elliptic curve cryptography, and wherein, in step (2), the module public key and the module private key are derived using the standard curve.

7. The mobile device of claim 6, wherein, in step (5), the message further comprises the parameters for the cryptographic algorithms, and wherein the server mutually derives the symmetric ciphering key using at least the module public key and the parameters for the cryptographic algorithms.

8. The mobile device of claim 1, wherein the mobile device receives the pre-shared secret key via a wireless 802.11 connection to a web portal after a user for the mobile device submits a pre-shared secret key code for the mobile device to the web portal.

9. The mobile device of claim 1, further comprising, in step (2), deriving (i) the module private key from a random number generator and (ii) the module public key from a key pair generation algorithm, wherein the module private key comprises a random number.

Petitioner Samsung Ex-1038, 0168

10. The mobile device of claim 9, wherein the random number generator is configured to generate the random number from a seed value, and wherein the seed value comprises data from at least one of a sensor and a radio for the mobile device.

11. The mobile device of claim 1, wherein, in step (1), the server public key is stored in a nonvolatile memory of the mobile device.

12. The mobile device of claim 1, wherein the server comprises a plurality of computers, wherein the plurality includes at least one sub-server and at least one database.

13. The mobile device of claim 1, wherein the server comprises at least one virtualized server operating on at least one computer.

14. The mobile device of claim 1, wherein the wireless network includes the server.

15. The mobile device of claim 1, wherein, in step (1), the module identity is stored in a read-only nonvolatile memory address, wherein the mobile device designates the read-only nonvolatile memory address as read-only for a time interval.

16. The mobile device of claim 1, wherein the wireless network comprises at least one base station communicating with a 3GPP wireless technology.

17. The mobile device of claim 1, wherein the message comprises a single user datagram protocol packet.

18. The mobile device of claim 1, wherein the symmetric ciphering algorithm comprises an Advanced Encryption Standard algorithm and has a length of 128 bits.

19. The mobile device of claim 1, wherein the module identity comprises a number for an international mobile subscriber identity number.

Petitioner Samsung Ex-1038, 0169

20. The mobile device of claim 1, wherein the mobile device comprises a smartphone.

Petitioner Samsung Ex-1038, 0170

ABSTRACT

Methods and systems are provided for supporting efficient and secure "Machine-to-Machine" (M2M) communications using a module, a server, and an application. A module can communicate with the server by accessing the Internet, and the module can include a sensor and/or an actuator. The module, server, and application can utilize public key infrastructure (PKI) such as public keys and private keys. The module can internally derive pairs of private/public keys using cryptographic algorithms and a first set of parameters. A server can authenticate the submission of derived public keys and an associated module identity. The server can use a first server private key and a second set of parameters to (i) send module data to the application and (ii) receive module instructions from the application. The server can use a second server private key and the first set of parameters to communicate with the module.

Petitioner Samsung Ex-1038, 0171

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/647,812	**01/12/2022 05:01:02 PM ET**	**63121/0213**

Title of Invention

Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	6784	FILED BY	Victoria Gilmore
PATENT CENTER #	60484501	FILING DATE	-
CUSTOMER #	1912	FIRST NAMED INVENTOR	John A. Nix
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Albert Boardman

Documents

TOTAL DOCUMENTS: 8

DOCUMENT		PAGES	DESCRIPTION	SIZE (KB)
generatedADS60484501.pdf		6	Application Data Sheet	141 KB
1-424-TrkOneRequest.pdf		2	TrackOne Request	112 KB
2-PowerofAtty.pdf		2	Power of Attorney	256 KB
3-ParentDeclaration.pdf		1	Oath or Declaration filed	122 KB
4-Specification.pdf		146	-	692 KB
4-Specification-SPEC.pdf	(1-141)	141	Specification	704 KB
4-Specification-CLM.pdf	(142-	4	Claims	118 KB

	145)			
4-Specification-ABST.pdf	(146-146)	1	Abstract	112 KB
5-Figures.pdf		17	Drawings-only black and white line drawings	464 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
generatedADS60484501.pdf	3142E2C77232C0B51C7FFF6EAE38FBDE1EC450BF6357A245C CAAD7E4530DCA2A0AA05EEBBE0013D2A542537C8F294D503 FFA1D629BDF0933A5765E1F78C6C36E
1-424-TrkOneRequest.pdf	3365434E01FE8B62D0AE2EBB5848B70496C8AE382EEED5946 8F1A8D6AA0AEC23CE828F7455B5B81A151445E7D64B7A1CF8 A308C8BC86EE1961663E6CEEAE0951
2-PowerofAtty.pdf	15D101CDA7B2B347C5FC0D9E996F3C5B38009E718526316E4 FB8D668043D027E72BD54115DDBE236C7ACCE2F2F7CEC810 A338FACAE6C439E0D62F6EBD0D23085
3-ParentDeclaration.pdf	6FA2B42FF82CCF122D892A93EFB8D1C4557B0C3F4938FD913 CAE55F582C9F432C856ECE0526339AF33D5241CE41A741B70 1B7913653998C4251D73692FE5F17C
4-Specification.pdf	AA6D6E3AC6EB369A60F703C047CD6E8896BACFC44C3E7AD BABF02A446DC5B71DECEAC402713770E315802E9A859DDC1 E8EA587DAE415594535C33FE609D8176C
4-Specification-SPEC.pdf	7DA6B655375ACE6727567A7CDE8904CC5CCC70CA10096DFE E6624B944F664BE1814764C39F93D8C1466C17D302E3B9D315 6B7346827855C6E6E12B60EAD03EE0
4-Specification-CLM.pdf	C95EA43AEE01D7F4A4F1C4CB3A9A1CB4B96EC9822A97F1D0 CD8EB078CEB15601A768642A201115D9F3D6857E2B000ED2A

	3F249428897C46EB8839046C18573AB
4-Specification-ABST.pdf	3D20D969F360F4B5A89E26101396ED6561B9C53F50C6EAA2400556F6F32B3BF00D08B1BC4484F00BE8D203BB0544348E365173DCA5C0559AD6415DFB38DE2118
5-Figures.pdf	3FF85B376669451FC792F888F51F1E7DFAB51996920DE24F03288B680034F6C15F43C7D745C18486B5805DAB6F2ED1F90C531477A0D3C7F6BCA357AA28980ED

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 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.

Application Data Sheet 37 CFR 1.76

The Application Data Sheet is part of the provisional or non-provisional 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.

Inventor Information

of inventors: 1

1. **John A. Nix**

Residence Information
US Residency
Evanston, IL
UNITED STATES

Mailing Address
807 Davis Street, Unit 409
Evanston, IL 60201
UNITED STATES

Application Information

Customer number	**1912 -**
Correspondence address	----
Title of invention	**Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)**
Attorney docket number	**63121/0213**
Entity status	Small
Application type	Nonprovisional Application under 35 USC 111(a)

Petitioner Samsung Ex-1038, 0175

Subject matter	Utility
Total number of drawing sheets	17
Suggested figure for publication	---
Filing by reference	No
Publication request	Normal eighteen-month publication

Representative Information

of representatives: 1

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).

Customer number 1912

Domestic Benefit/National Stage Information

of benefit claims: 5

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c), 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(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior app status	Pending
Application number	---
Continuity type	**Continuation of**
Prior app number	**16593561**
Filing Date	10/04/2019

Prior app status	Patented
Application number	**16593561**
Continuity type	**Continuation of**

Petitioner Samsung Ex-1038, 0176

Prior app number	**16036506**
Filing Date	07/16/2018
Patent number	10530575
Issue date	01/07/2020

Prior app status	Patented
Application number	**16036506**
Continuity type	**Continuation of**
Prior app number	**15583968**
Filing Date	05/01/2017
Patent number	10057059
Issue date	08/21/2018

Prior app status	Patented
Application number	**15583968**
Continuity type	**Continuation of**
Prior app number	**15010905**
Filing Date	01/29/2016
Patent number	9641327
Issue date	05/02/2017

Prior app status	Patented
Application number	**15010905**
Continuity type	**Continuation of**
Prior app number	**14055606**
Filing Date	10/16/2013
Patent number	9276740
Issue date	03/01/2016

Foreign Priority Information

of foreign priority claims: 0

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. 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) 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).

Data was not provided for this section.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

Checking this box will cause the application to be examined under the first inventor to file provisions of the AIA.

☐ 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 2016, 2013, will be examined under the first inventor to file provisions of the AIA.

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.

Petitioner Samsung Ex-1038, 0178

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 the 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.

Applicant Information

of applicants: 1

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.

1. **Network-1 Technologies, Inc.**
   445 Park Avenue, Suite 912
   New York, NY 10022
   UNITED STATES

   Phone: ---
   Fax: ---
   Email: ---

Applicant: Organization
Applicant type: Assignee

Assignee Information including Non-Applicant Assignee Information

of assignees: 0

An assignee-applicant identified in the "Applicant" section will appear on the patent application as an applicant.

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.

Data was not provided for this section.

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 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	First name	Last name	Registration #	Date
/Albert J. Boardman/	Albert J.	Boardman	70601	01/12/2022

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

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

Title of Invention	Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [■] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

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

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

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

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 the 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.

LEGAL NAME OF INVENTOR

Inventor: John A. Nix Date (Optional): October 15, 2013

Signature: John A. Nix

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. 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 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
17/647,812	01/12/2022 05:01:02 PM ET	63121/0213

Title of Invention

Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	6784	FILED BY	Victoria Gilmore
PATENT CENTER #	60484501	AUTHORIZED BY	Albert Boardman
CUSTOMER #	1912	FILING DATE	-
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	John A. Nix

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 1077	E20221BH02202377	Victoria Gilmore

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
2830	PROCESSING FEE, EXCEPT IN PROVISIONAL APPLICATIONS	70.00	1	70.00
2817	REQUEST FOR PRIORITIZED EXAMINATION	2100.00	1	2100.00
2111	UTILITY PATENT APPL. SEARCH FEE	350.00	1	350.00
4011	BASIC FILING FEE- UTILITY	80.00	1	80.00
2311	EXAMINATION OF ORIGINAL PATENT APPLICATION	400.00	1	400.00

TOTAL AMOUNT:	$3,000.00

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 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.

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
17/647,812	01/12/2022	2642	1040	63121/0213	20	1

CONFIRMATION NO. 6784

1912
AMSTER, ROTHSTEIN & EBENSTEIN LLP
90 PARK AVENUE
NEW YORK, NY 10016

FILING RECEIPT

OC000000131303718

Date Mailed: 01/24/2022

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, 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 corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction 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 provided that the request is grantable.

Inventor(s)

John A. Nix, Evanston, IL;

Applicant(s)

Network-1 Technologies, Inc., New York, NY;

Power of Attorney: The patent practitioners associated with Customer Number 1912

Domestic Priority data as claimed by applicant

This application is a CON of 16/593,561 10/04/2019
which is a CON of 16/036,506 07/16/2018 PAT 10530575
which is a CON of 15/583,968 05/01/2017 PAT 10057059
which is a CON of 15/010,905 01/29/2016 PAT 9641327
which is a CON of 14/055,606 10/16/2013 PAT 9276740

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Petitioner Samsung Ex-1038, 0184

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: 01/24/2022
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/647,812**
Projected Publication Date: 05/05/2022
Non-Publication Request: No
Early Publication Request: No
** **SMALL ENTITY** **
Title

Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)

Preliminary Class

455

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

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

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

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

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

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

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

Petitioner Samsung Ex-1038, 0187

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 17/647,812

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	80		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	350		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	400		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*	x 50 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*	x 240 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			210			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	1040		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/647,812	01/12/2022	John A. Nix	63121/0213	6784

1912 7590 03/08/2022

AMSTER, ROTHSTEIN & EBENSTEIN LLP
90 PARK AVENUE
NEW YORK, NY 10016

EXAMINER	
CENTRAL, DOCKET	

ART UNIT	PAPER NUMBER
OPAP	

MAIL DATE	DELIVERY MODE
03/08/2022	PAPER

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

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

Decision Granting Request for Prioritized Examination (Track I)	**Application No.** 17/647,812	**Applicant(s)** Nix, John A.	
	Examiner ANGELA E WALKER	**Art Unit** OPET	**AIA (FITF) Status** Yes

1. THE REQUEST FILED 12 January 2022 IS **GRANTED** .

The above-identified application has met the requirements for prioritized examination

A. ☑ for an original nonprovisional application (Track I).
B. ☐ for an application undergoing continued examination (RCE).

2. **The above-identified application will undergo prioritized examination**. The application will be accorded special status throughout its entire course of prosecution until one of the following occurs:

A. filing a **petition for extension of time** to extend the time period for filing a reply;

B. filing an **amendment to amend the application to contain more than four independent claims, more than thirty total claims** , or a multiple dependent claim;

C. filing a **request for continued examination** ;

D. filing a notice of appeal;

E. filing a request for suspension of action;

F. mailing of a notice of allowance;

G. mailing of a final Office action;

H. completion of examination as defined in 37 CFR 41.102; or

I. abandonment of the application.

Telephone inquiries with regard to this decision should be directed to ANGELA WALKER at (571) 272-1058. In his/her absence, calls may be directed to Petition Help Desk at (571) 272-3282.

/ANGELA E WALKER/ Paralegal Specialist, OPET	

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8127142	B2	2012-02-28	Cuppett	
	2	8522013	B2	2013-08-27	Zhang et al.	
	3	8843179	B2	2014-09-23	Li et al.	
	4	9408012	B2	2016-08-02	Li et al.	
	5	8924715	B2	2014-12-30	Schell et al.	
	6	9698981	B2	2017-07-04	Nix	
	7	9596078	B2	2017-03-14	Nix	
	8	8434139	B1	2013-04-30	Ortiz, Jr.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	9	8965366	B1	2015-02-24	Somayajula et al.	
	10	9020479	B1	2015-04-28	Somayajula et al.	
	11	9253643	B2	2016-02-02	Pattar et al.	
	12	6038322		2000-03-14	Harkins	
	13	7921292	B1	2011-04-05	Pauker et al.	
	14	8526606	B2	2013-09-03	Muthaiah	
	15	8555067	B2	2013-10-08	Schell et al.	
	16	8590028	B2	2013-11-19	Saxena et al.	
	17	8782774	B1	2014-07-15	Pahl et al.	
	18	8948386	B2	2015-02-03	Campagna et al.	
	19	9002018	B2	2015-04-07	Wilkins et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	20	9253643	B2	2016-02-02	Pattar et al.	
	21	8434139	B1	2013-04-30	Ortiz, Jr.	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20140281483	A1	2014-09-18	Vigliaturo et al.	
	2	20130179962	A1	2013-07-11	Arial et al.	
	3	20080031204	A1	2008-02-07	Sood	
	4	20090041110	A1	2009-02-12	Malladi	
	5	20090282246	A1	2009-11-12	Gunther	
	6	20090274306	A1	2009-11-05	Nolte	
	7	20140140509	A1	2014-05-22	Chastain et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	8	20140143534	A1	2014-05-22	Chastain et al.	
	9	20140237101	A1	2014-08-21	Park	
	10	20140235210	A1	2014-08-21	Park et al.	
	11	20060095771	A1	2006-05-04	Appenzeller et al.	
	12	20100223461	A1	2010-09-02	Drader et al.	
	13	20100199334	A1	2010-08-05	Ehrensvard et al.	
	14	20140040628	A1	2014-02-06	Fort et al.	
	15	20070101400	A1	2007-05-03	Freeman et al.	
	16	20160014112	A1	2016-01-14	Gunning et al.	
	17	20150222619	A1	2015-08-06	Hughes et al.	
	18	20010029581	A1	2001-10-11	Knauft	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	19	20140049653	A1	2014-02-20	Leonard et al.	
	20	20120214444	A1	2012-08-23	McBride et al.	
	21	20050050323	A1	2005-03-03	Mizrah	
	22	20090183541	A1	2009-07-23	Sadighi et al.	
	23	20100195833	A1	2010-08-05	Priestley et al.	
	24	20150222604	A1	2015-08-06	Ylonen	
	25	20110268022	A1	2011-11-03	Xu	
	26	20140357229	A1	2014-12-04	Lee et al.	
	27	20110167272	A1	2011-07-07	Kolesnikov	
	28	20160127132	A1	2016-05-05	Lee et al.	
	29	20170206532	A1	2017-07-20	Choi	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	30	20160294829	A1	2016-10-06	Angus	
	31	20150215126	A1	2015-07-30	Ashdown	
	32	20040162472	A1	2004-08-19	Berson et al.	
	33	20110269422	A1	2011-11-03	Xu et al.	
	34	20110269461	A1	2011-11-03	Xu et al.	
	35	20110269472	A1	2011-11-03	Xu et al.	
	36	20110270747	A1	2011-11-03	Xu	
	37	20130294602	A1	2013-11-07	Huxham et al.	
	38	20130340040	A1	2013-12-19	Park et al.	
	39	20140308991	A1	2014-10-16	Lee et al.	
	40	20140329502	A1	2014-10-06	Lee et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	41	20150281964	A1	2015-10-01	Seo et al.	
	42	20070158439	A1	2007-07-12	Conner et al.	
	43	20130183932	A1	2013-07-18	Lemilainen et al.	
	44	20120033613	A1	2012-02-09	Lin et al.	
	45	20130028184	A1	2013-01-31	Lee et al.	
	46	20130182586	A1	2013-07-18	Paladugu et al.	
	47	20020018569	A1	2002-02-14	Panjwani et al.	
	48	20030003895	A1	2003-01-02	Wallentin et al.	
	49	20030211842	A1	2003-11-13	Kempf et al.	
	50	20040179684	A1	2004-09-16	Appenzeller et al.	
	51	20050008159	A1	2005-01-13	Grilli et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	52	20050021875	A1	2005-01-27	Bouthemy et al.	
	53	20050120202	A1	2005-06-02	Cuellar et al.	
	54	20050138353	A1	2005-06-23	Spies et al.	
	55	20050193199	A1	2005-09-01	Asokan et al.	
	56	20050246282	A1	2005-11-03	Naslund et al.	
	57	20050278787	A1	2005-12-15	Naslund et al.	
	58	20060021063	A1	2006-01-26	Hori	
	59	20060056355	A1	2006-03-16	Love et al.	
	60	20060059344	A1	2006-03-16	Mononen	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	1							

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	Cakulev et al., "An EAP Authentication Method Based on Identity-Based Authenticated Key Exchange," August 2012, pp. 1-32.	
	2	Gollmann, "Authentication - Myths and Misconceptions," Progress in Computer Science and Applied Logic, Vol. 20, 2001, pp. 203-225.	
	3	Tin et al., "Provably Secure Mobile Key Exchange: Applying the Canetti-Krawczyk Approach," Information Security Research Centre, Queensland University of Technology, Australia, 2003, pp. 166-179.	
	4	Hegland et al., "A Framework for Authentication in NBD Tactical Ad Hoc Networks," IEEE Communications Magazine, October 2011, pp. 64-71.	
	5	Nicholson et al., "Mobile Device Security Using Transient Authentication," IEEE Transactions on Mobile Computing, Vol. 5, No.II, November 2006, pp.1489-1502.	
	6	Schwaiger et al., "Smart Card Security for Fieldbus Systems," 2003, pp. 398-406.	
	7	CSMG, Reprogrammable SIMs: Technology, Evolution and Implications, 25 SEP 2012, pp. 1-95.	
	8	GlobalPlatform Inc., GlobalPlatform Card Specification, Version 2.2.1, JAN 2011, pp. 1-303.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	9	GlobalPlatform Inc., GlobalPlatform Card Security Upgrade for Card Content Management, Card Specification v 2.2. - Amendment E, Version 1.0, NOV 2011, pp. 1-35.
	10	GSM Association, Embedded SIM Task Force Requirements and Use Cases, Version 1.0, 21 FEB 2011, pp. 1-38.
	11	Kirk H.M. Wong et al., A Dynamic User Authentication Scheme for Wireless Sensor Networks, Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), pp. 1-8.
	12	Pierre E. ABI-CHAR, et al., A Fast and Secure Elliptic Curve Based Authenticated Key Agreement Protocol For Low Power Mobile Communications, The 2007 International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST 2007), pp. 1-6.
	13	Jun Shao, et al., An Improved Deniable Authentication Protocol, Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200030, People's Republic of China, pp. 1-3.
	14	Chris Foresman, Embedded SIM could cause carrier conflict for Apple, November 19, 2010, pp. 1-2.
	15	Embedded UICC Remote Provisioning Discussion, Source: Rogers Wireless, 3GPP/SA3-LI#46, Quebec City, Canada, July 17-19, 2012, p. 1-39.
	16	GSMA LAUNCHES EMBEDDED SIM INITIATIVE TO SUPPORT THE CONNECTED FUTURE, November 18, 2010, p. 1-4.
	17	Chang-Seop Park, On Certificate-Based Security Protocols for Wireless Mobile Communication Systems, Dankook University, IEEE Network September/October 1997, pp. 50-55.
	18	M. Prasad, et al., Secure Authentication Key Agreement Protocol for Long Term Evolution - Advanced, Research Scholar, Associate Professor, Department of Computer Science & Engineering, Pondicherry Engineering College, Puducherry, India, Elsevier, 2012, pp. 158-162.
	19	Eun-Jun Yoon, et al., Secure Deniable Authentication Protocol Based on ElGamal Cryptography, 2008 International Conference on Information Security and Assurance, pp. 36-39.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	20	PIETRE-CAMBACEDES et al., Cryptographic key management for SCADA systems - issues and perspectives, 2008 International Conference on Information Security and Assurance, IEEE, pp. 156-161.
	21	BENDER et al., Evolution of SIM provisioning towards a flexible MCIM provisioning in M2M vertical industries, 16th International Conference on Intelligence in Next Generation Networks, IEEE, 2012, pp. 57-64.
	22	PARK et al., Secure Profile Provisioning Architecture for Embedded UICC, 2013 International Conference on Availability, Reliability and Security, IEEE, 2013, pp. 297-303.
	23	Appenzeller et al., Identity-Based Encryption Architecture and Supporting Data Structures RFC 5408, 2009, pp. 1-30.
	24	Baugher et al., Group Key Management Architecture, RFC Draft, 2001, pp. 1-20.
	25	Ben Saied, Yosra; Olivereau, Alexis; Laurent, Maryline; "A Distributed Approach for Secure M2M Communications", 6th International Conference on New Technologies, Mobility and Security (NTMS), 7-10 May 2012, pgs. 1-7.
	26	Boyen et al., Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles), 2006.
	27	Boyen et al., Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BBI Cryptosystems, RFC 5091, 2007, pp. 1-63.
	28	Harney et al., Group Key Management Protocol (GKMP) Architecture, 1994, pp. 1-19.
	29	Kiltz et al., CCA2 Secure IBE: Standard Model Efficiency through Authenticated Symmetric Encryption, 2008.
	30	Krylov, What is Kerberos Authtentication?, 2003, pp. 1-4.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	31	Martin, Introduction to Identity-Based Encryption, ISBN-13 978-1-59693-238-8, 2008.
	32	Merrian-Webster, Network, 2014.
	33	Park et al., A New Practical Identity-Based Encryption System, 2003, pp_ 1-27.
	34	Park et al., Secure Profile Provisioning Architecture for Embedded UICC, 2013 IEEE, pp_ 297-303.
	35	Shih, Jie-Ren; Hu, Yongbo; Hsiao, Ming-Chun; Chen, Ming-Shing; Shen, Wen-Chng; Yang, Bo-Yin; Wu, An-Yeu; Cheng, Chen-Mou; "Securing M2M with Post-Quantum Public-Key Cryptography", IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 7 March 2013, pgs_ 106-116.
	36	Voltage Security, The Identity-Based Encryption Advantage, 2015.
	37	Yang et al., Identity-Based Key Agreement and Encryption for Wireless Sensor Networks, IJCSNS International Journal of Computer Science and Network Security, Vol. 6, No. 5B, May 2006, pp_ 182-189.
	38	Youngblood, An Introduction to Identity-based Cryptography, 2005.

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Albert J. Boardman/	Date (YYYY-MM-DD)	2022-04-05
Name/Print	Albert J. Boardman	Registration Number	70,601

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

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060206710	A1	2006-09-14	Gehrmann	
	2	20060281442	A1	2006-12-14	Lee et al.	
	3	20070206799	A1	2007-09-06	Wingert et al.	
	4	20080016230	A1	2008-01-17	Hollmanns et al.	
	5	20080022089	A1	2008-01-24	Leedom	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	6	20080114978	A1	2008-05-15	Lehtoviorta et al.	
	7	20080165698	A1	2008-07-10	Dalsgard et al.	
	8	20090116642	A1	2009-05-07	Yang et al.	
	9	20090028341	A1	2009-01-29	Hamachi	
	10	20090077643	A1	2009-03-19	Schmidt et al.	
	11	20090125996	A1	2009-05-14	Guccione et al.	
	12	20090132806	A1	2009-05-21	Blommaert et al.	
	13	20090191857	A1	2009-07-30	Horn et al.	
	14	20090209232	A1	2009-08-20	Cha et al.	
	15	20090268909	A1	2009-10-29	Girao et al.	
	16	20090282246	A1	2009-11-12	Gunther	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	17	20090313472	A1	2009-12-17	Guccione et al.	
	18	20100166167	A1	2010-07-01	Karimi-Cherkandi et al.	
	19	20100031042	A1	2010-02-04	Di Crescenzo et al.	
	20	20100062808	A1	2010-03-11	Cha et al.	
	21	20100098253	A1	2010-04-22	Delerablee	
	22	20100275028	A1	2010-10-28	Takashima	
	23	20110016321	A1	2011-01-20	Sundaram et al.	
	24	20110055553	A1	2011-03-03	Lee et al.	
	25	20110237281	A1	2011-09-20	Busropan et al.	
	26	20110291803	A1	2011-12-01	Bajic et al.	
	27	20110314287	A1	2011-12-22	Escott et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	28	20120011360	A1	2012-01-12	Engels et al.	
	29	20120023336	A1	2012-01-26	Natarajan	
	30	20120072732	A1	2012-03-22	Canard et al.	
	31	20120089568	A1	2012-04-12	Manley et al.	
	32	20120108205	A1	2012-05-03	Schell et al.	
	33	20120117635	A1	2012-05-10	Schell et al.	
	34	20120159153	A1	2012-06-21	Shim et al.	
	35	20120260086	A1	2012-10-11	Haggerty et al.	
	36	20120260090	A1	2012-10-11	Hauck et al.	
	37	20120260095	A1	2012-10-11	Von Hauck et al.	
	38	20120278490	A1	2012-11-01	Sennett et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	39	20120300932	A1	2012-11-29	Cambridge et al.	
	40	20120331292	A1	2012-12-27	Haggerty et al.	
	41	20130091556	A1	2013-04-11	Horn et al.	
	42	20130114810	A1	2013-05-09	Kobayashi et al.	
	43	20130117824	A1	2013-05-09	Naslund et al.	
	44	20130149996	A1	2013-06-13	King et al.	
	45	20130166915	A1	2013-06-27	desai et al.	
	46	20130173747	A1	2013-07-04	Kim et al.	
	47	20130212637	A1	2013-08-15	Guccione et al.	
	48	20130227646	A1	2013-08-29	Haggerty et al.	
	49	20130305345	A1	2013-11-14	Bugenhagen	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	50	20130322621	A1	2013-12-05	Yoon et al.	
	51	20130331063	A1	2013-12-12	Cormier et al.	
	52	20140003604	A1	2014-01-02	Campagna et al.	
	53	20140053241	A1	2014-02-20	Norman et al.	
	54	20140073375	A1	2014-03-13	Li et al.	
	55	20140082358	A1	2014-03-20	Nakhjiri et al.	
	56	20140082359	A1	2014-03-20	Nakhjiri et al.	
	57	20140087790	A1	2014-03-27	Babbage et al.	
	58	20140101444	A1	2014-04-10	Lee et al.	
	59	20140108801	A1	2014-04-17	McBride et al.	
	60	20140140507	A1	2014-05-22	Park et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Albert J. Boardman/	Date (YYYY-MM-DD)	2022-04-05
Name/Print	Albert J. Boardman	Registration Number	70,601

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

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20140143826	A1	2014-05-22	Sharp et al.	
	2	20140161113	A1	2014-06-12	Cui et al.	
	3	20140165155	A1	2014-06-12	Zhang	
	4	20140192976	A1	2014-07-10	Yoon et al.	
	5	20140219447	A1	2014-08-07	Park et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	6	20140219448	A1	2014-08-07	Froels et al.	
	7	20140244994	A1	2014-08-28	Yu	
	8	20140273913	A1	2014-09-18	Michel et al.	
	9	20140287725	A1	2014-09-25	Lee	
	10	20140337937	A1	2014-11-13	Truskovsky et al.	
	11	20140351403	A1	2014-11-27	Lein et al.	
	12	20150012743	A1	2015-01-08	Holtmanns et al.	
	13	20150017910	A1	2015-01-15	Li et al.	
	14	20150071139	A1	2015-03-12	Nix	
	15	20150092590	A1	2015-04-02	Zhu et al.	
	16	20150095514	A1	2015-04-02	Yu	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	17	20150095648	A1	2015-04-02	Nix	
	18	20150113275	A1	2015-04-23	Kim et al.	
	19	20150121495	A1	2015-04-03	Gao et al.	
	20	20130231087	A1	2013-09-05	O'Leary	
	21	20130165073	A1	2013-06-27	Madsen	
	22	20130007442	A1	2013-01-03	Mao et aL	
	23	20120170451	A1	2012-07-05	Viswanathan et aL	
	24	20120084568	A1	2012-08-05	Sarikaya et al.	
	25	20120030461	A1	2012-02-02	Willey et al.	
	26	20080307218	A1	2008-12-11	Logvinov	
	27	20110035584	A1	2011-02-10	Meyerstein et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	28	20090060197	A1	2009-03-05	Taylor et al.	
	29	20150089214	A1	2015-03-26	Dupre	
	30	20140122878	A1	2014-05-01	Cho et al.	
	31	20140115335	A1	2014-04-24	Jorden et al.	
	32	20130173926	A1	2013-07-04	Morese et al.	
	33	20130012168	A1	2013-01-10	Rajadurai et al.	
	34	20120331298	A1	2012-12-27	Xu et al.	
	35	20120190354	A1	2012-07-26	Merrien et al.	
	36	20040221163	A1	2004-11-04	Jorgensen et al.	
	37	20090113203	A1	2009-04-30	Tsuge et al.	
	38	20150163056	A1	2015-06-11	Nix	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	39	20090217348	A1	2009-08-27	Salmela et al.	
	40	20080130879	A1	2008-06-05	Heinonen et al.	
	41	20130122864	A1	2013-05-16	Haggerty et al.	
	42	20150071139	A1	2015-03-12	Nix	
	43	20150095648	A1	2015-04-02	Nix	
	44	20150106616	A1	2015-04-16	Nix	
	45	20150121066	A1	2015-04-30	Nix	
	46	20150143125	A1	2015-05-21	Nix	
	47	20040162472	A1	2004-08-19	Berson et al.	
	48	20150215126	A1	2015-07-30	Ashdown	
	49	20160294829	A1	2016-10-06	Angus	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	50	20110269422	A1	2011-11-03	Xu et al.	
	51	20110269461	A1	2011-11-03	Xu et al.	
	52	20110269472	A1	2011-11-03	Xu et al.	
	53	20110270747	A1	2011-11-03	Xu et al.	
	54	20130294602	A1	2013-11-07	Huxham et al.	
	55	20130340040	A1	2013-12-19	Park et al.	
	56	20140308991	A1	2014-10-16	Lee et al.	
	57	20140329502	A1	2014-11-06	Lee et al.	
	58	20150281964	A1	2015-10-01	Seo et al.	
	59	20070158439	A1	2007-07-12	Conner et al.	
	60	20130183932	A1	2013-07-18	Lemilainen et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Albert J. Boardman/	Date (YYYY-MM-DD)	2022-04-05
Name/Print	Albert J. Boardman	Registration Number	70,601

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

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20120033613	A1	2012-02-09	Lin et al.	
	2	20130028184	A1	2013-01-31	Lee et al.	
	3	20130182586	A1	2013-07-18	Paladugu et al.	
	4	20020018569	A1	2002-02-14	Panjwani et al.	
	5	20030003895	A1	2003-01-02	Wallentin et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	6	20030211842	A1	2003-11-13	Kempf et al.	
	7	20040179684	A1	2004-09-16	Appenzeller et al.	
	8	20050008159	A1	2005-01-13	Grilli et al.	
	9	20050021875	A1	2005-01-27	Bouthemy et al.	
	10	20050120202	A1	2005-06-02	Cuellar et al.	
	11	20050138353	A1	2005-06-23	Spies et al.	
	12	20050193199	A1	2005-09-01	Asokan et al.	
	13	20050246282	A1	2005-11-03	Naslund et al.	
	14	20050278787	A1	2005-12-15	Naslund et al.	
	15	20060021063	A1	2006-01-26	Hori	
	16	20060056355	A1	2006-03-16	Love et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	17	20060059344	A1	2006-03-16	Mononen	
	18	20060206710	A1	2006-09-14	Gehrmann	
	19	20060281442	A1	2006-12-14	Lee et al.	
	20	20070206799	A1	2007-09-06	Wingert et al.	
	21	20080016230	A1	2008-01-17	Holtmanns et al.	
	22	20080022089	A1	2008-01-24	Leedom	
	23	20080114978	A1	2008-05-15	Lehtovirta et al.	
	24	20080165698	A1	2008-07-10	Dalsgaard et al.	
	25	20090116642	A1	2009-05-07	Yang et al.	
	26	20090028341	A1	2009-01-29	Hamachi	
	27	20090077643	A1	2009-03-19	Schmidt et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	28	20090125996	A1	2009-05-14	Guccione et al.	
	29	20090132806	A1	2009-05-21	Blommaert et al.	
	30	20090191857	A1	2009-07-30	Horn et al.	
	31	20090209232	A1	2009-08-20	Cha et al.	
	32	20090268909	A1	2009-10-29	Girao et al.	
	33	20090282246	A1	2009-11-12	Gunther	
	34	20090313472	A1	2009-12-17	Guccione et al.	
	35	20100166167	A1	2010-07-01	Karimi-Cherkandi et al.	
	36	20100031042	A1	2010-02-04	Di Crescenzo et al.	
	37	20100062808	A1	2010-03-11	Cha et al.	
	38	20100098253	A1	2010-04-22	Delerablee	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	39	20100275028	A1	2010-10-28	Takashima	
	40	20110016321	A1	2011-01-20	Sundaram et al.	
	41	20110055553	A1	2011-03-03	Lee et al.	
	42	20110237281	A1	2011-09-29	Busropan et al.	
	43	20110291803	A1	2011-12-01	Bajic et al.	
	44	20110314287	A1	2011-12-22	Escott et al.	
	45	20120011360	A1	2012-01-12	Engels et al.	
	46	20120023336	A1	2012-01-26	Natarajan	
	47	20120072732	A1	2012-03-22	Canard et al.	
	48	20120089568	A1	2012-04-12	Manley et al.	
	49	20120108205	A1	2012-05-03	Schell et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	50	20120117635	A1	2012-05-10	Schell et al.	
	51	20120159153	A1	2012-06-21	Shim et al.	
	52	20120260086	A1	2012-10-11	Haggerty et al.	
	53	20120260090	A1	2012-10-11	Hauck et al.	
	54	20120260095	A1	2012-10-11	Von Hauck et al.	
	55	20120278490	A1	2012-11-01	Sennett et al.	
	56	20120300932	A1	2012-11-29	Cambridge et al.	
	57	20120331292	A1	2012-12-27	Haggerty et al.	
	58	20130091556	A1	2013-04-11	Horn et al.	
	59	20130114810	A1	2013-05-09	Kobayashi et al.	
	60	20130117824	A1	2013-05-09	Naslund et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Albert J. Boardman/	Date (YYYY-MM-DD)	2022-04-05
Name/Print	Albert J. Boardman	Registration Number	70,601

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

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20150106616	A1	2015-04-16	Nix	
	2	20150121066	A1	2015-04-30	Nix	
	3	20150143125	A1	2015-05-21	Nix	
	4	20040162472	A1	2004-08-19	Berson et al.	
	5	20150215126	A1	2015-07-30	Ashdown	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	6	20160294829	A1	2016-10-06	Angus	
	7	20120108205	A1	2012-05-03	Schell et al.	
	8	20130012168	A1	2013-01-10	Rajadurai et al.	
	9	20140219447	A1	2014-08-07	Park et al.	
	10	20140161113	A1	2014-06-12	Cui et al.	
	11	20150113275	A1	2015-04-23	Kim et al.	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	10-2013-0026352	KR	A	2013-03-13	KT CORPORATION		
	2	10-2013-0026958	KR	A	2013-03-14	KT CORPORATION		
	3	19 81 224	EP	A1	2008-10-15	Samsung Electronics Co., Ltd.		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	4	2013027085	WO	A1	2013-02-28	Nokia Corporation et al.		
	5	2013066077	WO	A1	2013-05-10	KT CORPORATION		
	6	2775853	CA	A1	2012-12-01	BlackBerry Ltd.		
	7	2011138238	WO	A1	2011-11-10	Alcatel Lucent		

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	International Search Report for PCT/US2014/068544 dated February 13, 2015.	
	2	T. Pornin, Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm ECDSA), Internet Engineering Task Force RFC 6979, August 2013, pp.I-79.	
	3	GSMA, Fast Dormancy Best Practices Version 1.0,27 July 2011, TS.18, pp. 1-23.	
	4	N. CHU et al, EXALTED: Expanding LTE for Devices, European Commission for Information Society and Media, 31 October 2012, pp. 1-141.	
	5	J. HUANG et al, A Close Examination of Performance and Power Characteristics of 4G LTE Networks, Mobisys' 12, 25-29 June 2012, pp. 1-14.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	6	F. QIAN et al, TOP: Tail Optimization Protocol for Cellular Resource Allocation, 18th IEEE International Conference on Network Protocols (ICNP), 2010, 5-8 Oct. 2010, pp. 285-298.
	7	ETSI, Machine-to-Machine communications (M2M), mia, dla, and mid interfaces, TS 102.921 v1.1.1, Feb 2012, pp. 1-538.
	8	C. DOWNEY, Migrating Legacy M2M Systems to the Cloud, http://www.ecnmag.com/articles/2013/02/migrating-legacy-m2m-systems-cloud, Feb 2013, pp. 1-2.
	9	A. Wander et al, Energy Analysis of Public-Key Cryptography on Small Wireless Devices, Sun Microsystems Laboratories, pp.1-16.
	10	V. Martinez et al, A Survey of the Elliptic Curve Integrated Encryption Scheme, Journal of Computer Science and Engineering, Volume 2, August 2010, pp.7-13.
	11	ETSI, UMTS;LTE; SIM/USIM Internal and External Interworking Aspects, TR 131900 v.10.0.0, May 2011, pp.1-41.
	12	International Search Report and Written Opinion for PCT/US2014/062435 mailed February 6, 2015.
	13	Wikipedia, RSA (algorithm), http://en.wikipedia.org/wiki/RSA_(algorithm), 9 Sept. 2013, pp. 1-12.
	14	Wikipedia, Elliptic Curve Cryptography, http://en.wikipedia.org/wiki/Elliptic_curve_cryptography, 9 Sept. 2013, pp. 1-8 .
	15	L. LARZON, The Lightweight User Datagram Protocol (UDP-Lite), Internet Engineering Task Force RFC 3828, July 2004, pp. 1-12.
	16	Wikipedia, Digital Signature, http://en.wikipedia.orglwiki/Digital_signature, 9 Sept. 2013, pp. 1-10.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	17	D. Cooper, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Internet Engineering Task Force RFC 5280, pp. 1-133.
	18	J. Jonsson et al, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, Internet Engineering Task Force RFC 3447, February 2003, pp.1-72.
	19	D. McGrew et al, Fundamental Elliptic Curve Cryptography Algorithms, Internet Engineering Task Force RFC 6090, February 2011, pp. 1-34.
	20	Wikipedia, Elliptic Curve Diffie-Hellman, http://en.wikipedia.org/wiki/Elliptic_curve_Diffie%E2%80%93Hellman, 24 Sept. 2013, pp. 1-2.
	21	ETSI, Smart Cards; Embedded UICC; Requirements Specification, TS 103 383 v12.1.0, June 2013, pp. 1-20.
	22	3GPP, 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture, 3GPP TS 33.401 V12.9.0 (2013-09) pp. 1-75.
	23	3GPP, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3, 3GPP TS 24.301 v12.2.0, Sept. 2013 pp. 1-6, 63-100.
	24	ETSI, Smart Cards; UICC-Terminal Interfaces; Physical and Logical Characteristics, TS 102 221 v11.0.0, June 2012, pp. 1-181.

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Albert J. Boardman/	Date (YYYY-MM-DD)	2022-04-05
Name/Print	Albert J. Boardman	Registration Number	70,601

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

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	9807605	B2	2017-10-31	Gao et al.	
	2	8577337	B2	2013-11-05	O'Leary	
	3	9800993	B2	2013-11-05	Lee et al.	
	4	9794775	B2	2017-10-17	Huber et al.	
	5	9674690	B2	2017-06-06	Lee et al.	
	6	9628981	B2	2017-04-18	Park et al.	
	7	9572016	B2	2017-02-14	Cormier et al.	
	8	9332129	B2	2016-05-03	Li et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	9	9270653	B2	2016-02-23	Maria	
	10	6804357	B1	2004-10-12	Ikonen et al.	
	11	9923724	B2	2018-03-20	Lee et al.	
	12	6842628	B1	2005-01-11	Arnold et al.	
	13	8352739	B2	2013-01-08	Park et al.	
	14	6721886	B1	2004-04-13	Uskela	
	15	5995625	A	1999-11-30	Sudia et al.	
	16	5852665	A	1998-12-22	Gressel et al.	
	17	5664017	A	1997-09-02	Gressel et al.	
	18	5642420	A	1997-06-24	Kuroda et al.	
	19	5216715	A	1993-06-01	Markwitz	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	20	6256733	B1	2001-07-03	Thakkar et al.	
	21	9020479	B1	2015-04-28	Somayajula et al.	
	22	8965366	B1	2015-02-24	Somayajula et al.	
	23	8452017	B2	2013-05-28	Sherkin	
	24	7957532	B2	2011-06-07	Chen et al.	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20110213959	A1	2011-09-01	Bodi et al.	
	2	20130344864	A1	2013-12-26	Park et al.	
	3	20140082359	A1	2014-03-20	Nakhjiri et al.	
	4	20140120874	A1	2014-05-01	Kang et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	5	20140329502	A1	2014-11-06	Lee et al.	
	6	20150350881	A1	2015-12-03	Weiss et al.	
	7	20130283047	A1	2013-10-24	Merrien et al.	
	8	20120263298	A1	2012-10-18	Suh et al.	
	9	20080044032	A1	2008-02-21	Lou et al.	
	10	20050058294	A1	2005-03-17	Chen et al.	
	11	20160088096	A1	2016-03-24	Quiriconi et al.	
	12	20120190354	A1	2012-07-23	Merrien et al.	
	13	20110035604	A1	2011-02-10	Habraken	
	14	20140237101	A1	2014-08-21	Park	
	15	20140235210	A1	2014-08-21	Park et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	16	20140219447	A1	2014-08-07	Park et al.	
	17	20140140507	A1	2014-05-22	Park et al.	
	18	20140082358	A1	2014-03-20	Nakhjiri et al.	
	19	20150281964	A1	2015-10-01	Seo et al.	
	20	20150121495	A1	2015-04-30	Gao et al.	
	21	20140308991	A1	2014-10-16	LEE et al.	
	22	20130340040	A1	2013-12-19	Park et al.	
	23	20130122864	A1	2013-05-16	Haggerty et al.	
	24	20110270747	A1	2011-11-03	Xu	
	25	20160057725	A1	2016-02-25	Suh	
	26	20160149903	A1	2016-05-26	Suh	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	27	20130157673	A1	2013-06-20	Brusilovsky	
	28	20110268022	A1	2011-11-03	Xu	
	29	20160127132	A1	2016-05-05	Lee et al.	
	30	20140357229	A1	2014-12-04	Lee et al.	
	31	20130227646	A1	2013-08-29	Haggerty et al.	
	32	20130012168	A1	2013-01-10	Rajadurai et al.	
	33	20130294602	A1	2013-11-07	Huxham et al.	
	34	20140003604	A1	2014-01-02	Campagna et al.	
	35	20110269461	A1	2011-11-03	Xu et al.	
	36	20110269472	A1	2011-11-03	Xu et al.	
	37	20110269422	A1	2011-11-03	Xu et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	38	20120011362	A1	2012-01-12	Lambert	
	39	20060129848	A1	2006-06-15	Paksoy et al.	
	40	20120087493	A1	2012-04-12	Chidambaram et al.	
	41	20080107083	A1	2008-05-08	Shirota et al.	
	42	20130165075	A1	2013-06-27	Rishy-Maharaj et al.	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	ANSI X9.63 Overview, Key Agreement and Key Transport Using Elliptic Curve Cryptography, Simon Blake-Wilson, Certicom (2000)	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

EXAMINER SIGNATURE			
Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Albert J. Boardman/	Date (YYYY-MM-DD)	2022-04-05
Name/Print	Albert J. Boardman	Registration Number	70,601

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

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	10169587	B1	2019-01-01	Nix	
	2	10621352	B2	2020-04-14	Nix	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060021063	A1	2006-01-26	Hori	
	2	20100093347	A1	2010-04-15	Hahn et al.	
	3	20110158411	A1	2011-06-30	Medvinsky et al.	
	4	20210126801	A1	2021-04-29	Nix	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	5	20200280436	A1	2020-09-03	Nix	
	6	20210218560	A1	2021-07-15	Nix	
	7	20210184842	A1	2021-06-17	Nix	
	8	20210194681	A1	2021-06-24	Nix	
	9	20190356482	A1	2019-11-21	Nix	
	10	20200226258	A1	2020-07-16	Nix	
	11	20190313246	A1	2019-10-10	Nix	
	12	20210211279	A1	2021-07-08	Nix	
	13	20200162269	A1	2020-05-21	Nix	
	14	20200162247	A1	2020-05-21	Nix	
	15	20190332774	A1	2019-10-31	Nix	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	16	20100291907	A1	2010-11-18	Malcolm David MacNaughtan et al.	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2518976	GB	A	2015-04-08	Vodafone IP Licensing Ltd		
	2	2021007235	WO	A1	2021-01-14	Nix		
	3	2021007235	WO	A1	2021-01-14	Nix		
	4	2021087221	WO	A1	2021-05-06	Nix		
	5	2020223319	WO	A1	2020-11-05	Nix		
	6	2020006162	WO	A1	2020-01-02	Nix		
	7	2019246206	WO	A1	2019-12-26	Nix		
	8	2019222319	WO	A1	2019-11-21	Nix		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	9	2019209598	WO	A1	2019-10-31	Nix		
	10	2019178312	WO	A1	2019-09-19	Nix		
	11	2020123959	WO	A1	2020-06-18	Nix		
	12	2020061023	WO	A1	2020-03-26	Nix		
	13	3110641	CA	A1	2019-10-31	Nix		
	14	3110468	CA	A1	2019-11-21	Nix		
	15	19803936	DE	A1	1999-08-05	Osram GmbH Siemens AG		
	16	3766222	EP	A1	2021-01-20	Nix		
	17	20130026351	KR	A	2013-03-13	KT CORPORATION		☒
	18	2013/048084	WO	A2	2013-04-04	KT CORPORATION		☒

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

NON-PATENT LITERATURE DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Search Report issued in UK Application No. GB2108534.5 dated July 7, 2021.	
	2	ANSI X9.63 Overview, Key Agreement and Key Transport Using Elliptic Curve Cryptography, Simon Blake-Wilson, Certicom (2000)	
	3	TLS 1.3 Wish List Presentation, IETF 87 (Eric Rescorla), dated August 1, 2013.	
	4	European Patent Office Communication with European Search Report and European Search Opinion issued in EP 21182424.8 dated October 12, 2021.	
	5	European Patent Office Communication with European Search Report and European Search Opinion issued in EP 21182451.1 dated October 12, 2021.	
	6	European Patent Office Communication with European Search Report and European Search Opinion issued in EP 21182432.1 dated October 12, 2021.	
	7	Harald Bender et al., "Business transformation of the provisioning process for Machine-to-Machine," 2011 15th International Conference on Intelligence in Next Generation Networks, IEEE, 2011. (Year: 2011).	

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Albert J. Boardman/	Date (YYYY-MM-DD)	2022-04-05
Name/Print	Albert J. Boardman	Registration Number	70,601

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

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Espacenet

KR20130026351A METHOD AND APPARATUS FOR MANAGING PROFILE OF EMBEDDED UICC, PROVISIONING METHOD AND MNO-CHANGING METHOD USING THE SAME

Applicants: KT CORP [KR]

Inventors: PARK JAE MIN [KR],LEE JIN HYOUNG [KR]

Classifications:
IPC ***H04L29/06; H04L9/14; H04W8/18;***

CPC **H04L29/06 (KR); H04L9/14 (KR); H04W12/08 (EP,US); H04W12/35 (EP,US); H04W8/18 (KR);** H04W12/04 (EP,US);

Priorities: KR20110089638A 2011-09-05; KR20110096210A 2011-09-23

Application: KR20110097900A·2011-09-28

Publication: KR20130026351A·2013-03-13

Published as: **KR102001869B1;** KR20130026351A;**US2014219447A1; US9414233B2**

METHOD AND APPARATUS FOR MANAGING PROFILE OF EMBEDDED UICC, PROVISIONING METHOD AND MNO-CHANGING METHOD USING THE SAME

Abstract

PURPOSE: An e-UICC(embedded Universal Integrated Circuit Card), a profile management method of the e-UICC, a terminal with the e-UICC, a provisioning method, and an MNO(Mobile Network Operator) change method are provided to prevent a profile or profile management data which is transmitted and received from an end point connected to an MNO system from access of the terminal or an external entity. CONSTITUTION: An e-UICC transmits an activation request including device identification information and e-UICC identification information to an MNO(S310). An e-UICC state request and technical ability control request/confirmation are performed(S320). The MNO obtains an encoding key, which is a public key from SM(Subscription Manager)-SR(Secure Routing), for the e-UICC(S330). The MNO generates a new e-UICC profile suitable for the MNO through SM-DP(Data Preparation) and transfers the file to the MNO by encoding the file with the public key(S340). [Reference numerals] (S310) Requesting activation(IMEI, eICCId); (S320) Requesting eUICC state, and controlling and responding technology ability; (S330) Authenticating eUICC ID, and collecting device information; (S340) Generating and encoding a new eUICC profile; (S350) Transmitting the encoded eUICC profile; (S360) Transmitting a double encoded profile; (S370) Requesting state, and updating DB

Petitioner Samsung Ex-1038, 0256

KR20130026351A METHOD AND APPARATUS FOR MANAGING PROFILE OF EMBEDDED UICC, PROVISIONING METHOD AND MNO-CHANGING METHOD USING THE SAME

Data originating from sources other than the EPO may not be accurate, complete, or up to date.

The wording below is an initial machine translation of the original publication. To generate a version using the latest translation technology, go to the original language text and use Patent Translate.

A profile management method using an embedded UICC (eUICC) interworking with a MNO system and a subscription management system SM, the eUICC receiving an encrypted profile from the MNO or SM, And decrypting the profile using the profile access credential information that is provided to the eUICC.

The method of claim 1, wherein the encrypted profile is encrypted with the public key of the eUICC, and the profile access credential is a secret key or a private key corresponding to the eUICC public key.

3. The method of claim 2, wherein the SM includes a data preparation (SM-DP) and a secure routing (SM) device, wherein the SM-DP encrypts the profile using the eUICC public key, SR encrypts the primary encrypted profile with the eUICC public key, and the encrypted profile is a double ciphered profile.

5. The method of claim 4, wherein the profile includes at least one of a provisioning profile for provisioning, an operation profile, package information including MNO cryptographic information or MNO cryptographic information, an International Mobile Subscriber Identity (IMSI), a UICC OTA Key, Key, etc.), supplementary service application, and supplementary service data.

3. The method according to claim 2, wherein the encrypted profile is a double ciphered profile, and in the decrypting step, the eUICC performs a primary decryption of the profile with a separate management key and a secondary decryption using the eUICC public key EUICC & lt; / RTI &)

A method of managing a profile using an embedded UICC (eUICC) interworking with a MNO system and a subscription management system (SM), the SM performing a function of managing the eUICC, Wherein the profile-profile refers to a combination of file structure, data and application to be provided to the eUICC, the eUICC is data existing within the profile access credential profile or within the eUICC, Processing or managing the received profile using data that allows secure communication between the eUICC and an external entity to be set up to protect or manage the data; And managing the processed profile information using the received profile information or the profile access credential so that the terminal or terminal including the eUICC can not access the eUICC. How to Manage Profiles.

7. The eUICC of claim 6, wherein the received profile is a Double Ciphered profile and the profile access credential is a public key unique to the eUICC or a corresponding private or private key. How to Manage Profiles.

8. The method of claim 7, wherein the SM comprises a SM-DP (Data Preparation) and an SM-SR (Secure Routing) device.

The eUICC is a built-in UICC (eUICC) interworking with a MNO system and a subscription management system (SM), wherein the eUICC is a profile- A profile that is a combination of a file structure, data, and an application to be provided to the eUICC; profile access credential information to manage the profile structure and its data; And means for enabling the secure communication between the eUICC and the external entity to be established.

10. The eUICC of claim 9, wherein the profile access credential information is a public key or a corresponding private key uniquely assigned to the eUICC.

11. The eUICC of claim 10, wherein the eUICC is capable of ensuring authenticity using the profile access credential information.

(EUICC) equipped with a built-in UICC (eUICC) interworking with an MNO system and a subscription management system (SM), the eUICC terminal having a profile access credential for managing a profile received from the MNO or SM Wherein the issuance processing module generates a public key which is profile access credential information for the eUICC using a self internal security module or a separate internal security

module according to a request from the SM And receives the profile information encrypted with the eUICC public key from the MNO or the SM, and decrypts the encrypted profile key using a secret key (or a private key) corresponding to the public key.

The system of claim 12, wherein the SM comprises a SM-DP (Data Preparation) and an SM-SR (Secure Routing) device, and the issuance processing module installs the security module in response to a request from the SM- Features eUICC equipped terminal.

14. The system of claim 13, wherein the issuance processing module conveys an e-UICC public key together with the SM-SR together with an encryption information-key generation algorithm and key length information of the public key eUICC equipped terminal.

The eUICC-equipped terminal according to claim 13, wherein the encrypted profile information is double ciphered with the eUICC public key and the eUICC management key.

16. The terminal of claim 15, wherein the double-encrypted profile information includes digital signature information generated by the SM-DP or MNO's private key that generated the profile.

16. The terminal of claim 15, wherein the eUICC management key is at least one of an eUICC OTA key and a GP ISD key.

A built-in UICC (eUICC) interworking with a subscriber management system (SM), a security module for decrypting an encrypted profile in response to a request from an issuance processing module in a terminal equipped with the eUICC, Wherein the security module further has a function of generating a public key corresponding to the eUICC according to a request of the issuing process module and transmitting the generated public key to an external SM.

The eUICC of claim 18, wherein the security module decrypts the profile using a secret key corresponding to the public key of the eUICC.

(SIM) and a SIM service management platform, wherein the SIM service management platform includes one or more of the following: a mobile communication network (MNO) system and an embedded UICC (eUICC) The security module includes an operating profile for the MNO and a security module. The security module generates and outputs the public key of the eUICC according to the request of the SIM service management platform, and decrypts the encrypted data with a secret key corresponding to the eUICC public key.

(EUICC) interworking with SM-SR (Secure Routing) and SM-DP (Data Preparation) devices constituting a subscriber management system (MNO) -SR receives the eUICC public key from the eUICC and transmits the eUICC public key to the MNO, and after the SM-DP first encrypts the profile with the eUICC public key received via the MNO, Requesting the MNO to request a profile of the secondary encrypted with a separate security key for the primary encrypted profile by requesting from the MN to the SM-SR, the MNO or the SM-And transferring the profile information to the eUICC.

The eUICC of claim 21, wherein the eUICC further comprises a step of first decrypting the double encrypted profile with the secret key, and secondary decoding the secret key with the secret key corresponding to the eUICC public key to decrypt the original profile information A feature provisioning method.

22. The method of claim 21, wherein the eUICC is further operable to: transmit an activation request including eUICC identification information (eICCId) to the MNO; and verify status and technical capabilities of the eUICC between the MNO and the eUICC The method comprising the steps of:

Built-in UICC interworking with SM-SR (Secure Routing) and SM-DP (Data Preparation) devices that make up the Receiving MNO, Donor MNO, Subcription Manager (eUICC), the SM-SR having received an eUICC public key from the eUICC and transferring the eUICC public key to the receiving MNO, the receiving MNO having a carrier change to the donor MNO To the receiving MNO after the SM-DP first encrypts the profile with the eUICC public key received via the receiving MNO, and the receiving MNO sends the notification to the SM-SR Requesting a secondary encrypted profile with a separate security key for the primary encrypted profile, and the receiving MNO or the SM-SR sends the secondary encrypted encryption profile information to the eUICC Method MNO change comprises a; the method comprising.

26. The method of claim 24, wherein the eUICC sends an activation request that includes eUICC identification information (eICCId) to the receiving MNO, and verifies status and technical capabilities of the eUICC between the receiving MNO and the eUICC Further comprising the steps of: & lt; Desc / Clms Page number 13 &)

KR20130026351A METHOD AND APPARATUS FOR MANAGING PROFILE OF EMBEDDED UICC, PROVISIONING METHOD AND MNO-CHANGING METHOD USING THE SAME

Data originating from sources other than the EPO may not be accurate, complete, or up to date.

The wording below is an initial machine translation of the original publication. To generate a version using the latest translation technology, go to the original language text and use Patent Translate.

a profile management method of an eUICC, an eUICC and an eUICC-equipped terminal using the same, a provisioning method, and a MNO-changing method using the same,

[0001] The present invention relates to a method of managing an embedded UICC (euICC) profile, an eUICC using the eUICC, an eUICC equipped terminal, a provisioning method and an MNO changing method, credentials to manage or handle various profiles. The present invention also relates to an eUICC management method for dynamically generating a public key as a profile access credential in an SM function separation environment so that the eUICC uses the public key.

[0002] A UICC (Universal Integrated Circuit Card) is a smart card inserted in a terminal and used as a module for user authentication. The UICC may store the user's personal information and the carrier information of the mobile communication carrier to which the user subscribes. For example, the UICC may include an International Mobile Subscriber Identity (IMSI) for identifying a user. The UICC is also referred to as a SIM (Subscriber Identity Module) card for Global System for Mobile communications (GSM) and a Universal Subscriber Identity Module (USIM) card for WCDMA (Wideband Code Division Multiple Access).

[0003] When the user attaches the UICC to the user terminal, the user is automatically authenticated using the information stored in the UICC, so that the user can conveniently use the terminal. Also, when the user changes the terminal, the user can easily replace the terminal by mounting the UICC removed from the existing terminal to the new terminal.

[0004] When a terminal requiring miniaturization, for example, a machine to machine (Machine to Machine, M2M) communication, is manufactured with a structure capable of detaching the UICC, miniaturization of the terminal becomes difficult. Thus, an eUICC structure, a UICC that can not be detached, has been proposed. The eUICC shall record the user information using the UICC in the form of IMSI.

[0005] The existing UICC can be attached to / detached from the terminal, and the user can open the terminal without being concerned with the type of terminal or mobile communication provider. However, the IMSI in the eUICC can be allocated only when the terminal manufactured from the time of manufacturing the terminal is established to be used only for the specific mobile communication provider. Both the mobile communication service provider and the terminal manufacturer ordering the terminal are forced to pay attention to the product inventory and the product price is raised. The user is inconvenient that the mobile communication provider can not be changed with respect to the terminal. Therefore, even in the case of the eUICC, there is a need for a method by which the user can open the terminal regardless of the mobile communication service provider.

[0006] In recent years, due to the introduction of eUICC, it has become necessary to update subscriber information of a plurality of telecommunication carriers from a remote UICC. Accordingly, a Subscription Manager (hereinafter referred to as 'SM') or a profile A Profile Manager (PM) is being discussed.

[0007] These SMs are mainly discussed in terms of information management for eUICC, information management for various telecommunication carriers, authentication and remote information change for mobile telecommunication carrier change, etc. However, It has not been decided yet.

[0008] Also, in an environment where eUICC is used, an important profile can be provided to the eUICC, and a mechanism is needed to securely transmit and use such a profile.

The present invention provides a method for managing an eUICC. The present invention provides a method for managing or handling various profiles (provisioning profiles, operation profiles, etc.) using profile access

Petitioner Samsung Ex-1038, 0260

credentials in an eUICC. At least one set of profile access credentials (eg eUICC public keys) for securely provisioning various profiles (provisioning profiles, operation profiles, etc.) transmitted from an end point (eg SM) It is also an object of the present invention to provide a method of managing profile or profile management data transmitted and received from an endpoint that is reliably connected to an operator (MNO) system by an eUICC, which can not be accessed by an external entity such as a terminal or a terminal The present invention provides a method for managing Another object of the present invention is to provide a method of managing an eUICC in an environment in which an SM is separated into SM-SR (Secure Routing) and SM-DP (Data Preparation) (Public key, etc.) capable of encrypting security information in an environment in which the SM-SR is separated and implemented in the form of Secure Routing and SM-DP (Data Preparation). Another objective is to provide a method in which an MNO receives an encryption key allocated to a corresponding eUICC through an SM-SR in an environment in which the SM is separated into SM-SR (Secure Routing) and SM-DP (Data Preparation) Another object of the present invention is to provide a method for the MNO to dynamically obtain and use a cryptographic key (public key, etc.) from the corresponding eUICC through the SM-SR.

One embodiment of the present invention is a profile management method using an embedded UICC (eUICC) interworking with a communication provider (MNO) system and a subscription management system (SM), wherein the eUICC receives an encrypted profile from the MNO or SM And decrypting the profile using the profile access credential information stored in the eUICC. According to another embodiment of the present invention, there is provided a method of managing a profile of an eUICC,) System, a profile management method using an embedded UICC (eUICC) interworking with a subscription management system (SM), the SM performing a function of managing the eUICC, and the eUICC extracting profile- Profile means a combination of file structure, data and application to be provided to said eUICC; said eUICC is a pro File Access Credential - Data present in the profile or in the eUICC, meaning the profile structure and the data that allows the secure communication to be set up between the eUICC and the external entity to protect or manage the data. Processing or managing the received profile and the eUICC includes managing profile information processed using the received profile information or the profile access credential such that the terminal or terminal including the eUICC is inaccessible Another embodiment of the present invention is a built-in UICC (eUICC) interworking with a MNO system and a subscription management system (SM), wherein the eUICC includes a terminal Profile received from the MNO or SM such that the terminal or the terminal is inaccessible, Means a combination of a file structure, data and an application to be provided to the eUICC - a profile access credential information for managing the profile structure and the data existing in the eUICC or for protecting or managing the profile structure and its data eUICC & quot; means data that allows a secure communication to be set up between the eUICC and an external entity. Another embodiment of the present invention is a system and method for interworking with a subscriber management system (SM) Wherein the eUICC terminal includes an issuance processing module for generating and managing profile access credential information for managing a profile received from the MNO or the SM, The module uses the internal or separate internal security module to request the eUI Generates and responds to a public key that is profile access credential information for the CC, receives the profile information encrypted with the eUICC public key from the MNO or the SM, and decrypts the encrypted profile key using a secret key (or a private key) corresponding to the public key Another embodiment of the present invention is a built-in UICC (eUICC) interworking with a MNO system and a subscription management system (SM), in which an issuance processing module in the terminal equipped with the eUICC The security module further includes a function of generating a public key corresponding to the eUICC according to a request of the issuance processing module and delivering the public key to the external SM in response to a request from the issuance processing module Another embodiment of the present invention is an embedded UICC (eUICC) interworking with the MNO system and the subscription management system SM, System (COS), a SIM platform, and a SIM service management platform, wherein the SIM service management platform includes an operating profile (provider information) and security module for one or more MNOs, The eUICC generates and outputs the public key of the eUICC according to the request of the eUICC, and decrypts the encrypted profile received from the outside with the secret key corresponding to the eUICC public key. MNO, Subcription Manager; (EUICC) interworking with an SM-SR (Secure Routing) and an SM-DP (Data Preparation) device constituting the SM-SR, the SM- SR receives the eUICC public key from the eUICC, Forwarding the eUICC public key to the MNO; encrypting the profile with the eUICC public key received by the SM-DP through the MNO and then forwarding the profile to the MNO; Requesting a secondary encrypted profile for the primary encrypted profile with a separate security key, and forwarding the secondary encrypted encryption profile information to the eUICC by the MNO or the SM-SR Another embodiment of the present invention provides a method for provisioning a SM-SR (Subscriber Identity) system comprising a Receiving MNO, a Donor MNO, and a Subscription Manager Wherein the SM-SR receives an eUICC public key from the eUICC and transmits the eUICC public key to the receiving end of the receiving UICC (eUICC) using an embedded UICC (eUICC) interworking with the SM-DP (Secure Routing) To the MNO, the receiving MNO

Petitioner Samsung Ex-1038, 0261

transmitting a notification of the carrier change to the donor MNO, and a step of transmitting the notification of the carrier change to the donor MNO by using the e-UICC public key received through the receiving MNO Requesting a profile of the recipient MNO requesting the SM-SR to secondary-encrypt the primary encrypted profile with a separate security key, and sending the profile to the receiving MNO, And the SM-SR forwards the secondary encrypted encryption profile information to the eUICC.

[0025] Figure 1 shows the overall service architecture including the eSIM (eUICC) to which the present invention is applied. Figure 2 shows the system architecture of the SM separation environment to which the present invention may be applied. Figure 4 is an overall flowchart of a subscription change or MNO change process to which the present invention is applied Figure 5 shows the internal structure of an eUICC or eSIM according to an embodiment of the present invention Figure 6 Figure 7 shows a profile installation structure of a SIM service management platform led by an eUICC or an eSIM according to an embodiment of the present invention. FIG. 9 shows a flow of an MNO change process according to an embodiment of the present invention. Referring to FIG.

[0026] Hereinafter, some embodiments of the present invention will be described in detail with reference to exemplary drawings. It is to be noted that, in adding reference numerals to the constituent elements of the respective drawings, the same constituent elements are denoted by the same reference numerals whenever possible, even if they are shown in different drawings. In the following description of the present invention, a detailed description of known functions and configurations incorporated herein will be omitted when it may make the subject matter of the present invention rather unclear.

[0027] Since the M2M (Machine-to-Machine) terminal actively discussed in GSMA should be small in size, if a UICC is used, a module for mounting a UICC must be separately inserted in the M2M terminal. Therefore, The miniaturization of the M2M terminal becomes difficult.

[0028] Therefore, an embedded UICC structure which can not be detached from the UICC is being discussed. In this case, the eUICC installed in the M2M terminal is provided with information of a mobile network operator (MNO) (International Mobile Subscriber Identity, IMSI).

[0029] However, since the terminal manufactured from the manufacturing of the M2M terminal can be allocated to the IMSI in the eUICC only if it is assumed that the terminal manufactured only by the specific MNO, the MNO or M2M manufacturer that orders the M2M terminal or the UICC, And the price of the product is increased, which is a big obstacle to the expansion of the M2M terminal.

[0030] Unlike the conventional removable SIM, the built-in SIM (hereinafter referred to as eSIM or eUICC), which is integrally mounted on the terminal, has many issues such as the opening authority, the initiative of the supplementary service business, . To this end, the GSMA and ETSI international standardization organizations are carrying out standardization activities on relevant elements such as operators, manufacturers, SIM vendors, and other necessary elements including the top-level structure. As eSIM is discussed through standardization bodies, it is at the heart of the issue that SM issues an important profile (Operator Credential, MNO Credential, Profile, eUICC Profile, Profile Package, etc.) to eSIM, Or function / role that performs the overall management role for the eSIM.

[0031] Recently, GSMA proposed SM-DP (Data Preparation), which plays a role of generating provider information, and SM-SR (Secure Routing), which carries direct carrier information to eSIM. And does not mention the actual method of issuing technical information.

[0032] Accordingly, the present invention proposes a method of managing eSIM by utilizing dynamic encryption key (public key, etc.) generation in the SM role separation environment of GSMA.

[0033] In this specification, eSIM and eUICC are used as an equivalent concept.

[0034] The eSIM attaches the IC chip to the terminal circuit board in the terminal manufacturing stage and then transmits the software SIM data (activation information, supplementary service information, etc.) to OTA (Over the Air) or offline (technology based connection such as USB to PC) Is a new concept of SIM technology. IC chips used in eSIM generally support hardware based CCP (Crypto Co-Processor) to provide hardware-based public key generation. APIs that can be utilized based on applications (eg applets) , Java Card Platform, etc.).

The Java Card Platform (Java Card Platform) is one of the platforms that can provide multi-applications and services on smart cards and so on.

[0035] Because SIM has limited memory space and security reasons, it should not be possible for anyone to install an application in a SIM. Therefore, a SIM service management platform is required in addition to a platform for mounting an application. The SIM service management platform issues data to the SIM memory area through authentication and security through the management key. The global platform (GlobalPlatform) and Remote File Management (RFM) and Remote Application Management (EASI TS 102.226) Service management platform.

[0036] One of the important factors in eSIM environment, eSIM remotely issues communication and supplementary service data through management keys (UICC OTA Key, GP ISD Key, etc.).

[0037] Here, the management key or the eSIM management key or the eUICC management key is an access authentication key to the eSIM for securely transmitting business information to the eSIM, and is a concept distinct from a cryptographic key (public key, etc.) It may be expressed as eUICC access credentials as described below.

[0038] In GSMA, the role of SM is classified as SM-DP and SM-SR. In addition to the operation profile (or provider information), SM-DP builds securely the IMSI, K, OPc, supplementary service application, supplementary service data, etc. in the form of a Credential Package, SR is responsible for securely downloading the SM-DP generated credit package to eSIM through SIM remote management technology such as over-the-air (OTA) or GP SCP (Secure Communication Protocol).

[0039] In addition, we propose a structure called "Circle of Trust" shown in Fig. 1 below, and establish an end-to-end trust relationship between MNO and eSIM through overlapping of trust relations between each similar entity or entities And the concept of building. In other words, MNO1 forms a trust relationship with SM1, SM1 with SM4 and SM4 form a trust relationship with eSIM, thereby forming a trust relationship between MNO and eSIM.

[0040] Before describing the present invention, the terms used in this specification will be described first.

[0041] MNO (Mobile Network Operator) means a mobile communication service provider and means an entity that provides communication service to a customer through a mobile network.

[0042] The subscription manager (SM) is a subscription management device and performs management functions of the eUICC.

[0043] The eUICC supplier is the person who supplies the eUICC module and embedded software (such as firmware and operating system).

[0044] Device Vendor refers to the supplier of a device, especially a device that includes a wireless modem function via a mobile network driven by an MNO, and consequently a UICC (or eUICC) form of device.

[0045] Provisioning refers to the process of loading a profile into the eUICC, and a provisioning profile refers to a profile used by a device to connect to a communication network for the purpose of provisioning different provisioning profiles and operation profiles.

[0046] Subscription means a commercial relationship for providing services between a subscriber and a wireless communication service provider.

[0047] The eUICC access credentials refer to the data in the eUICC that enables secure communication between the eUICC and external entities to be set up to manage the profiles on the eUICC.

[0048] Profile access credentials are data residing within a profile or within an eUICC, which means that the secure communication between the eUICC and external entities can be set up to protect or manage the profile structure and its data .

[0049] A Profile is a combination of file structures, data, and applications that can be provisioned into an eUICC or managed within an eUICC, including an Operational Profile, a Provisioning Profile for provisioning, and other Policy Control Functions (PCFs) And all the information that may exist in the eUICC.

[0050] The Operation Profile or the Operator Information refers to all kinds of profiles related to Operational Subscribing.

[0051] Figure 1 illustrates an overall service architecture including an eSIM (eUICC) to which the present invention is applied.

[0052] The overall system is described as follows.

[0053] The eUICC system architecture to which the present invention may be applied may include a plurality of MNO systems, one or more SM systems, an eUICC manufacturer system, a device maker system including an eUICC, and an eUICC, The explanation is as follows.

[0054] In Fig. 1, a dotted line indicates a trust circle, and two solid lines indicate a secure link.

[0055] If a scenario where subscription information is stored and delivered is needed, it should be done under the approval of the MNO and under the control of the MNO. There must be only one active profile on a single eUICC at a particular time, which means that the active profile is added to a single HLR at a specific time.

[0056] The MNO and the eUICC should be able to decode the MNO Credentials information, i.e., the profile (operation profile, provisioning profile, etc.). The only exception to this may be a third entity, such as a SIM vendor, commissioned from a particular MNO. However, this is not a general function of a third party to do so.

[0057] The subscription can not be switched within the eUICC outside the operator policy control. The user must be aware of any changes in the MNO content and its activation subscription, be able to avoid security risks, and need a level of security sufficient to compete with the current UICC model.

[0058] The MNO credential or profile may refer to an affiliation credential, including K, an algorithm, an algorithm parameter, a supplementary service application, supplementary service data, and so on.

[0059] The delivery of MNO credentials or profiles shall be done in a secure manner from end to end. Transmissions can be made in successive stages without breaking the security chain, and all steps in the transport chain must be done with the recognition and approval of the MNO. No entity in the transport chain should be able to clearly see the MNO credential, but the only exception could be a third entity, such as a SIM vendor, delegated from a particular MNO. However, this is not a general function of a third party to do so.

[0060] Operators should have full control over their credentials, and operators should have strong supervisory and control over SM operations.

[0061] The SM function should be provided by the MNO or a third party, and if provided by a third party, there is a commercial relationship between the SM and the MNO.

[0062] SM does not have any direct relationship with MNO subscribers for subscription management. The MNO has to have a relationship with the subscriber and should be the entry point for joining the customer, but this is not the intent of the M2M service provider (the M2M service provider is the MNO subscriber) to have a contractual relationship with his / her customer.

[0063] While the MNO is being swapped, the donor and the receiving MNO may or may not have pre-contract with each other. There must be a mechanism to approve the pre-contract. The policy control function of the donor operator can define the removal condition of its own credential, and the policy control function (PCF) can implement this function.

[0064] The architecture introduces a function defined as SM, and the main role of the SM is to prepare a package or profile containing the MNO credential and forward it to the eUICC. The SM function may be provided directly by the MNO, or the MNO may contract with a third party to obtain the SM service.

[0065] The role of the SM can be divided into two sub functions such as SM-SR and SM-DP.

[0066] In practice, these SM-SR, SM-DP functions may be provided by other entities or by the same entity. Therefore, the functions of SM-DP and SM-SR need to be clearly bounded, and the interface between these entities needs to be defined.

[0067] The SM-DP is responsible for the secure preparation of the package or profile to be delivered to the eUICC and works with the SM-SR for actual transmission. The core functions of SM-DP are: 1) to manage the functional characteristics and certification level of the eUICC, and 2) to manage MNO credentials or profiles (eg IMSI, K, supplementary service application, , Some of which may potentially be encrypted (enciphered) by the MNO), and 3) the ability to compute an OTA package for downloading by SM-SR. It can be added.

[0068] If the SM-DP function is provided by a third party, the security and trust relationship becomes very important. In addition to real-time provisioning, SM-DP can have a significant amount of background processing capability, and performance, scalability and reliability requirements are expected to be important.

[0069] SM-SR is responsible for secure routing and delivery of the credit package to the corresponding eUICC. The core functions of SM-SR are: 1) to manage OTA communication with eUICC over ciphered VPN; and 2) to manage end-to-end eUICC with other SM-SR 3) the function of managing the eUICC data used for the SM-SR OTA communication provided by the eUICC supplier, and 4) the function of protecting the communication with the eUICC by filtering only the allowed entities (Firewall function).

[0070] The SM-SR database is provided by eUICC vendors and vendors (such as M2M terminals) and potentially MNOs and can be used by the MNO through the SM-SR mesh network.

[0071] Circle of trust enables an end-to-end security link during provisioning profile delivery, and SM-SR shares trust circles for secure routing of provisioning profiles and eUICC discovery. The MNO may be linked with the SM-SR and SM-DP entities in the trust circle and may provide this functionality on its own. In order to avoid illegal use of eUICC (illegal use of cloning, criminal use, denial of service, illegal MNO context change, etc.) without compromising the contractual and legal obligations of MNOs related to the customer, eUICC and MNO Credential A secure end-to-end link between the two is required.

[0072] 1, reference numeral 110 denotes a trust circle formed between SMs, more specifically SM-SR members, 120 is a trust circle of MNO partners, and 130 shows an end-to-end trust link.

[0073] Fig. 2 shows a configuration in which SM-SR and SM-DP are located in the system in the SM separation environment.

[0074] As shown in FIG. 2, the SM is divided into SM-DP for securely preparing a plurality of profiles related to the eUICC (MNO's operation profile and provisioning profile) and SM-SR for routing the SM. SR, and the SM-DP is linked to the MNO system.

[0075] Of course, the arrangement of the SM-DP and the MNO system can be implemented differently from that of FIG. (I.e., the SM-DP is interworked with the SM-SR, and the MNO system can be interworked with the SM-DP)

[0076] Under such an eUICC system architecture, the eUICC according to an embodiment of the present invention can guarantee integrity, confidentiality and authenticity for loading various profiles (provisioning profile, operation profile, etc.) Lt; / RTI &) mechanism. As an example of such a mechanism, an encryption / decryption mechanism using a public key and a secret key of the eUICC, which is a profile access credential, and an electronic signature using a public key and a private key of the SM are included Can be.

[0077] That is, because the profiles must be very securely protected within the eUICC architecture by a secure mechanism that ensures integrity, confidentiality and authenticity, and thus the profile is not transferred into the eUICC (rather than being provisioned at the manufacturing stage) A very secure mechanism is needed to protect it.

[0078] The eUICC according to an embodiment of the present invention can manage or handle various profiles (provisioning profile, operation profile, etc.) using the profile access credential in the eUICC.

[0079] More specifically, in the present invention, a profile access credential (for example, a proxy access profile) for safely provisioning various profiles (provisioning profile, operation profile, and the like) transmitted from an end point (e.g., eUICC's public key, etc.), and may decrypt the encrypted profile transmitted from the external entity using the profile access credential, as will be described in the embodiments below.

[0080] Also, in an embodiment of the present invention, it is preferable that only one activation profile exists in the eUICC, and the profile or management data is stored in the operator system In addition to being securely transported between a trusted endpoint and an eUICC, profile or profile management data must be inaccessible to external entities such as terminals or terminals. For this purpose, an embodiment of the present invention includes a method using an eUICC public key as a profile access credential capable of encrypting / decrypting the profile or profile management data below.

[0081] 3 is an overall flowchart of the provisioning process corresponding to the first subscription in the system to which the present invention is applied.

[0082] In the provisioning process, the eUICC transmits an activation request including the device identification information (IMEI, etc.) and the eUICC identification information (eICCid, etc.) to the MNO (Request activation: S310) State request and technical capability control request / confirmation are performed (eUICC status request and technical capability control; S320)

[0083] Although not shown, in step S320, the eUICC transmits PKI key information (key generation algorithm, key length, key generation method, etc.), which is its public key PK or profile access credential information, And providing it to the corresponding MNO system or SM-SR.

[0084] In step S330, the MNO collects eUICC identity verification and eUICC identity verification and collect information about device between the SM-SR and the MN. In step S330, the MNO may acquire an encryption key for the eUICC, specifically, a public key corresponding to the eUICC, from the SM-SR according to an embodiment of the present invention.

[0085] The acquisition of such a public key may be static or dynamic. When the eUICC is static, it is already publicly available in the corresponding eUICC, specifically in the eUICC through a cryptographic processor (CCP). Key and secret key are generated, the secret key is stored in the eUICC, and the public key is shared by all the SM-SRs so that the public key of the specific eUICC can be recognized. If there is a request from the MNO, the SM- and sends the public key for the eUICC to the MNO.

[0086] As described below with reference to FIGS. 8 and 9, when there is a request (including specific eUICC identification information) from the MNO, the SM-SR requests the corresponding eUICC to transmit the public key , The corresponding eUICC is an issuance processing module within the eUICC-equipped terminal (which is not limited to this term and can be referred to as a communication module, a provisioning module, an issuance module, an opening module and the like), communication with the outside of the terminal equipped with an eUICC for provisioning of eUICC,) Or a security module in the eUICC (a module that performs security computation using cryptographic key generation and encryption keys in the eUICC such as an encryption key generation module, a cryptographic key processing module, a security policy module, a Credential Manager, and a Profile Manager) And then transmits the generated public key to the SM-SR. This will be described in more detail below.

[0087] Here, one security module installed in the eUICC may be installed commonly in the eUICC according to the eUICC production phase or the eUICC policy thereafter, and a plurality of security modules may be installed for each MNO according to the eUICC policy and each MNO policy.

[0088] The MNO that obtained the public key (cryptographic key) of the eUICC generates a new eUICC profile for the MNO through SM-DP, encrypts the profile with the obtained eUICC public key (cryptographic key), and transfers the profile to the MNO. Primary encryption, step S340). At this time, the SM-DP can generate an additional digital signature with its own private key to provide authenticity. That is, in step S340, the SM-DP can sign the profile with its own private key or secret key for authentication.

[0089] Next, when the MNO transmits the primary encrypted (eUICC) profile to the SM-SR and requests the secondary encryption, the SM-SR uses the eUICC management key (eUICC OTA key, GP ISD key, etc.) The eUICC profile is secondarily encrypted and transferred to the MNO (step S350)

[0090] Then, the MNO transmits a Double Ciphered eUICC profile to the corresponding eUICC (S360). At this time, the public key or certificate of the SM-DP can be transmitted together with the eUICC to provide authentication have.

[0091] Since the eUICC already knows the eUICC management key, the eUICC decrypts the profile to be used for provisioning completely by decrypting it first, then secondary decoding it using the secret key (already known in the manufacturing or public key dynamic generation step) corresponding to the public key can do. In this case, the eUICC sends the public key of the SM-DP (in the case of the certificate, from a trusted third entity) to the certificate authority (to confirm that the eUICC profile is generated from the SM-DP corresponding to the public key obtained from the MNO) The validity of the certificate can be verified).

[0092] In step S370, the SM-SR database is updated between the eUICC and the SM-SR that have finished the provisioning according to the status request and the response thereto.

[0093] The main components of each of these steps are described as follows.

[0094] In step S310, the eUICC identification information (such as eICCid) is public data and must be integrated within the eUICC.

[0095] In S320 and S330, the status request and the technical possibility control provide proof of the eUICC identity (reliable eUICC), and it should be possible to confirm the eligibility of the eUICC characteristic for the MNO service.

[0096] In steps S340 to S360, a dual encryption mechanism is used for eUICC profile creation and transmission. That is, the creation profile linked to the eUICC by the SM-DP is encrypted by the encryption mechanism that can only be read by the target eUICC, and the digital signature is performed by the SM-DP to confirm that the profile is generated from the legitimate SM-DP And the SM-SR encrypts the generation profile with the eUICC management key to authenticate and protect the eUICC during delivery.

[0097] In step S370, the SM-SR database may be updated at the finishing stage of the subscription installation.

[0098] 4 is an overall flowchart of a subscription change or MNO change process to which the present invention is applied.

[0099] 3 (i.e., the new MNO after the change corresponds to the MNO in FIG. 3), but the new MNO performs the negotiation and right transfer process to the donor MNO before and after the profile creation for the new MNO (Step S440 ').

[0100] The difference between the MNO change process of FIG. 4 and the provisioning process of FIG. 3 is that the activation request is transmitted to the donor MNO OTA bearer using the provisioning or operation active profile, and the new MNO is changed to one of OTA or OTI To request a route from the SM-SR to download the profile.

[0101] The MNO changing process according to FIG. 4 will be described in detail as follows.

[0102] In order to change the MNO, the eUICC transmits an activation request including device identification information (IMEI) and eUICC identification information (eICCid, etc.) to the MNO (Requesting MNO) to be changed (Request activation: S410) An eUICC status request and a technical capability control request / confirmation are performed between the receiving MNO and the eUICC (eUICC status request and technical capability control; S420).

[0103] Also, although not shown, in step S420, the eUICC transmits PKI key information (key generation algorithm, key length, key generation method, etc.), which is its public key PK or profile access credential information, It is the same as S320 which is a provisioning process that a process to be provided to the corresponding MNO system or SM-SR may be included.

[0104] In step S430, the receiving MNO collects eUICC identity verification and information on the device (eUICC) between the SM-SR and the euICC (e-UICC identity verification and collect information about device). In step S430, the MNO may acquire an encryption key for the eUICC, specifically, a public key corresponding to the eUICC, from the SM-SR according to an exemplary embodiment of the present invention.

[0105] The acquisition of such a public key may be static or dynamic. When the eUICC is static, it is already publicly available in the corresponding eUICC, specifically in the eUICC through a cryptographic processor (CCP). Key and secret key are generated, the secret key is stored in the eUICC, and the public key is shared by all the SM-SRs so that the public key of the specific eUICC can be recognized. If there is a request from the MNO, the SM- and sends the public key for the eUICC to the MNO.

[0106] As described below with reference to FIGS. 8 and 9, when there is a request (including specific eUICC identification information) from the MNO, the SM-SR requests the corresponding eUICC to transmit the public key , The corresponding eUICC is an issuance processing module within the eUICC-equipped terminal (which is not limited to this term and can be referred to as a communication module, a provisioning module, an issuance module, an opening module and the like), communication with the outside of the terminal equipped with an eUICC for provisioning of eUICC,) Or a security module in the eUICC (a module that performs security computation using cryptographic key generation and encryption keys in the eUICC such as an encryption key generation module, a cryptographic key processing module, a security policy module, a Credential Manager, and a Profile Manager) And then transmits the generated public key to the SM-SR. This will be described in more detail below.

[0107] Here, one security module installed in the eUICC may be installed commonly in the eUICC according to the eUICC production phase or the eUICC policy thereafter, and a plurality of security modules may be installed for each MNO according to the eUICC policy and each MNO policy.

[0108] The receiving MNO that obtained the public key (cryptographic key) of the eUICC generates a new eUICC profile for the MNO through the SM-DP, encrypts the profile with the obtained eUICC public key (encryption key), and transmits the encrypted profile to the MNO (Primary Encryption, S440) At this time, the SM-DP can generate an additional digital signature with its own private key to provide authenticity. That is, in step S440, the SM-DP can sign the profile with its own private key or secret key for authentication.

[0109] Further, negotiation and rights transfer step (S440 ') before or after step S440 may be performed. The negotiation and right transmission step S440 'is a process such as requesting the new receiving MNO to transfer the eNICC to the previous MNO (donor MNO) and the rights (information) according to the MNO change .

[0110] That is, in step S440 ', a new MNO (Receiving MNO) requests authentication of the donor MNO for subscription switching, and such authentication may be provided by a policy control function.

[0111] Next, when the recipient MNO sends the primary encrypted (eUICC) profile to the SM-SR and requests secondary encryption, the SM-SR sends the eUICC management key (eUICC OTA key, GP ISD key, etc.) The eUICC profile is secondarily encrypted and transmitted to the MNO (step S450)

[0112] Then, the MNO transmits a double-ciphered eUICC profile to the corresponding eUICC (S460). At this time, the public key or certificate of the SM-DP can be transmitted together with the eUICC to provide authentication have.

[0113] Since the eUICC already knows the eUICC management key, it decrypts it first and then decrypts the profile to be used for MNO change completely by using the secret key corresponding to its own public key (already known in the manufacturing or public key dynamic generation step) It can be decoded. In this case, the eUICC sends the public key of the SM-DP (in the case of the certificate, from a trusted third entity) to the certificate authority (to confirm that the eUICC profile is generated from the SM-DP corresponding to the public key obtained from the MNO) The validity of the certificate can be verified).

[0114] In step S470, the SM-SR database is updated between the eUICC and the SM-SR that have finished the provisioning according to the status request and the response thereto.

[0115] The proposed SM role separation environment can be applied in eSIM environment where all business initiatives can be taken away from the SM by ensuring business initiative with appropriate flexibility (SMO-SR solves all MNO's need to interact with each MNO) The SM-DP role is generally expected to be performed by the MNO and has the advantage of being able to carry the communication information and the supplementary service provider information through the SM-DP). However, since there is no detailed eSIM management method based on this structure, there are difficulties such as ensuring the security of each provider information and definition of issuance flow when introducing eSIM system.

Petitioner Samsung Ex-1038, 0268

[0116] In the present invention, the eUICC interworking with the MNO system and the subscription management system (SM) can not access the terminal or the terminal including the eUICC, and the profile information for managing the profile information received from the MNO or the SM (EUICC public key, secret key, etc.), and proposes a structure for processing (decrypting, etc.) the received profile information using such profile access credential information.

[0117] Hereinafter, an embodiment of the present invention will be described, and a public key of eUICC and its corresponding secret key will be described as an example of the SM role separation environment proposed by GSMA and the profile access credential, no.

[0118] In the following, one of the provider information, the operation profile, or the provisioning profile is exemplarily described as the processed or managed profile information, but the present invention is not limited thereto, and the eUICC may be applied to all the information for which the eUICC must ensure authenticity.

[0119] In the following, eSIM is safely managed by using dynamic public key generation which is a profile access credential, and it is divided into basic open structure, third party movement structure, and process method.

[0120] The basic upper structure of the present invention is based on the eSIM structure of Fig. In the present specification, the SM specified in the figure may be a single SM entity or an SM entity of the & quot; Circle of Trust & quot ;.

[0121] FIG. 5 illustrates an internal structure of an eUICC or an eSIM according to an embodiment of the present invention.

[0122] The eUICC 520 according to an exemplary embodiment of the present invention is detachably included in a device or a terminal 510. The eUICC 520 includes a lowest level chip OS (COS) 521, SIM platform 522, its upper level SIM service management platform 523, and the like, and a provisioning profile 524 for various communication or supplementary M2M services exists on the COS.

[0123] In addition, the SIM service management module 523 may include business entity information 525 or an operation profile for each business entity and a security module 526 corresponding thereto.

[0124] The operation profile and the security module may be separately included for each provider or MNO, but it is preferable that only one operation profile is activated at a specific time.

[0125] In addition, the terminal 510 may include an issuance processing module 511 interlocked with the eUICC. The issuance processing module may be implemented in software as a module for processing communication and necessary processes required for issuing between the eSIM and the SM have. The function of this issuance processing module will be described in more detail with reference to Figs. 8 and 9 below.

[0126] 5, the entire system to which the present invention is applied includes an eUICC 520 including a provisioning profile 524, a device 510 equipped with an eUICC, an eUICC and an SM Issuance processing module 511 & quot; that handles the necessary communication and necessary processes for the e-commerce business, and an & quot; eUICC infrastructure (right part of Fig. 4) & quot; that includes SM-SR, MNO and SM-DP.

[0127] The & quot; issuance processing module 511 & quot; communicates with the & quot; eUICC infrastructure & quot; with the software existing in the device and performs the issuance process related to the eUICC. In this process, the "Issuance Processing Module" can perform secure communication such as TLS / SSL with the "eUICC Infrastructure", and the software module should be located in a safe space in the device and protected from external hacking.

[0128] In the "eUICC", there is a provisioning profile (Provisioning Profile) 524, and when an issuing process is required, all MNOs must be able to communicate between the eUICC-equipped device and the "eUICC infrastructure" based on the corresponding provisioning profile. Inside the & quot; eUICC & quot; includes but is not limited to an eUICC management key managed by the SM-SR, e.g., a UICC OTA key, a global platform IS (Issuer Security Domain) A SIM service management platform 524 for loading / managing carrier

information (MNO Profile or Operational Profile) and a security module 526, and a lower SIM platform 523 and a COS 521 are provided.

[0129] Here, the & quot; security module 526 & quot; plays a role of generating a pair of a public key and a private key (secret key) according to a PKI (Public Key Infrastructure) scheme such as RSA, ECC, An application such as an applet, or the like, or may be shared among business operators. In addition to the key pair generation, the & quot; security module 526 & quot; generates the private key (secret key) encrypted with the public key of the eUICC in cooperation with the & quot; issuance processing module 511 & quot; And verifies the digital signature of the digitally signed provider information with the private key of the provider.

[0130] The issuance processing module in this specification plays a role of communication and provisioning management with respect to the outside of the eUICC-equipped terminal for eUICC provisioning, and is not limited to the above-mentioned terminology but may be applied to a communication module, a provisioning module, an issuing module, It can be expressed in terms.

[0131] In addition, the security module in the eUICC performs cryptographic key generation such as a credential management, a profile manager, and security computation using a cryptographic key. The security module is not limited to the above-mentioned term, and may be used in other terms such as an encryption key generation module, Can be expressed.

[0132] FIG. 6 shows a structure of a provider information installation (led by an issuance process module) of an eUICC or eSIM according to an embodiment of the present invention, and FIG. 7 shows a structure of a provider information (MNO Profile) led by a SIM service management platform.

[0133] 6, an eUICC and a terminal equipped with the eUICC according to an embodiment of the present invention may first receive a double-encrypted profile from an external entity (for example, SM-SR or the like) As an example).

[0134] The double encrypted profile is encrypted with a public key (PKI), which is a profile accessing credential of the corresponding eUICC, and then encrypted with a separate security key such as an eUICC management key.

[0135] Upon receipt of the dual encrypted profile, the eUICC first performs a primary decryption with an eUICC management key or a security key that is already known by using the SIM service management platform (S610). Then, the profile information encrypted with the eUICC public key (PKI) , And the SIM service management platform delivers the PKI decryption request to the issuing module of the terminal (S620)

[0136] The issuance processing module transfers the decryption request in step S620 to the corresponding security module in the eUICC again and receives a final profile decrypted from the security module using the private key or the private key corresponding to the corresponding PKI (S630)

[0137] Thereafter, the issuance processing module transmits the completely decrypted service provider information to the SIM service management platform (S640)

[0138] 6 is a processing method led by the issuance processing module, and is not necessarily limited to such a method, and may be driven by the SIM service management module as shown in FIG.

[0139] That is, as shown in FIG. 7, the terminal receives a double-encrypted profile (e.g., provider information or an operation profile is exemplified in FIGS. 6 and 7) from an external entity (for example, SM-SR or the like).

[0140] The dual encrypted profile is encrypted with a public key (PKI), which is a profile access credential of the corresponding eUICC, and then encrypted with a separate security key such as an eUICC management key, as shown in the right side of FIG.

[0141] Upon receipt of the dual encrypted profile, the eUICC first performs a primary decryption with an eUICC management key or a security key that is already known using the SIM service management platform (S710). Then, the profile information encrypted with the eUICC public key (PKI) , And the SIM service management platform delivers the PKI decryption request directly to the security module (S720)

[0142] Then, the SIM service management module receives the final profile decrypted from the security module with the private key or the private key corresponding to the corresponding PKI, and installs it in response (S730)

[0143] That is, although data issuance through interlocking with the existing & quot; SIM service management platform & quot; is performed only through the eUICC management key or the secret key, in the present invention, after authentication and decryption through the eUICC management key or the secret key, The process of decrypting the provider information once again through the "security module" installed in eSIM for each provider should be added. The subject requesting the decryption to the "security module" may be an "issuance processing module" as shown in FIG. 6, and may be a "SIM service management platform" as shown in FIG. (The safety is higher in the case of Fig. 7).

[0144] FIG. 8 shows a flow of a provisioning (initial opening) process according to an embodiment of the present invention.

[0145] In the present invention, the eSIM or the eUICC is pre-loaded with a provisioning profile for performing issuance via all MNO (i.e., any MNO) network. In addition, "eUICC has eUICC identification information that identifies each eUICC according to the GSMA proposal structure, such as eICCID (not ICCID), and it plays a role of identifying each eUICC throughout the issuance.

[0146] The initial subscription in the present invention proceeds as follows using a provisioning profile pre-installed in the eUICC.

[0147] The eUICC-equipped device transmits an opening request to the MNO along with the eUICC-equipped device identification information and the eUICC identification information (IMEI, eICCID, etc.) through the provisioning profile using the "issuance processing module" (S810) And may be expressed as a request activation process.

[0148] Then, the MNO communicates with the & quot; issuance processing module & quot; of the eUICC-equipped device through the provisioning profile to acquire the eUICC status and information on the supporting network and additional functions (e.g., SIM additional service available). At this time, it is also possible to confirm whether or not the security module in the eUICC is installed. If the security module is already installed, the information about the public key of the corresponding eUICC (PKI key information including algorithm, length,). This step S820 may be expressed as an eUICC status request and a technical capability control (eUICC status request & technical capability control) process.

[0149] Next, the MNO requests the SM-SR to verify the eUICC identification information (eICCID and the like), install the security module, and transmit the encryption key (public key, etc.) generated in the eUICC (S830). Here, if the security module is already installed, the installation process may be omitted.

[0150] Next, in step S840, the SM-SR uses the eUICC management key or the security key to install a security module in the eUICC in cooperation with the & quot; SIM service management platform & quot; (Key generation algorithm, key length, etc.), as well as encryption keys (public keys, etc.) and, if necessary, encryption key information or public key information. Here, if the security module is already installed, the installation process may be omitted.

[0151] Next, the SM-SR transmits the cipher key (public key, etc.) (cipher key information (key generation algorithm, key length, etc.)) and device information generated in the eUICC to the MNO (S850).

[0152] The MNO transmits the cipher key (public key, etc.) (cipher key information (key generation algorithm, key length, etc.)) and eUICC identification information (eICCID etc.) to the SM-DP. It encrypts the profile of the provider information (communication data, supplementary service application, supplementary service data, etc.) for the corresponding eUICC identification information (eICCID, etc.) and responds to the MNO. At this time, the SM-DP can perform digital signature with its own private key for providing the certificate (S860)

[0153] Next, the MNO requests the SM-SR that the carrier information encrypted with the eUICC public key is encrypted with a separate eUICC management key or a security key to be loaded in the eUICC, and the SM-SR is encrypted with the eUICC management key or the security key Encryption) and transmits it to the MNO (S870), and the MNO issues the provider information in the device through the SM-SR (S880). At this time, if authentication is provided, the public key of the SM-DP may be transmitted to the device.

[0154] Lastly, the SM-SR communicates with the & quot; issuance processing module & quot; of the eUICC to perform status and DB update (S890)

[0155] The steps S810 to S890 of FIG. 8 may be integrated in one step or integrated into one as necessary.

[0156] FIG. 9 shows a flow of an MNO changing process according to an embodiment of the present invention.

[0157] The provider change process as shown in Fig. 8 can be configured as follows.

[0158] First, the eUICC-equipped device transmits an opening request to the receiving MNO B through the provisioning profile together with the eUICC-equipped device and the eUICC identification information (IMEI, eICCID, etc.) through the "issuance processing module" (S910)

[0159] Then, the receiving MNO B communicates with the & quot; issuance processing module & quot; of the eUICC-equipped device through the provisioning profile to acquire the eUICC status and information of the supporting network and additional functions (e.g., SIM additional service available) If the security module is already installed, information about the public key of the corresponding eUICC, that is, public key information (including PKI key information: algorithm, length, and method, etc.) is acquired can do.

[0160] Based on the information received, the receiving MNO A notifies the donor MNO A of MNO A about the change of the MNO, and receives the response value to MNO A. That is, a new receiving MNO may request a previous MNO (donor MNO) to negotiate whether the eUICC is legitimate and to transfer the rights (information) according to the MNO change. (S930)

[0161] The receiving MNO B requests the SM-SR to verify the eUICC identification information (eICCID, etc.), to install the security module, and to transmit the encryption key (public key, etc.) generated by the eUICC. Here, if the security module is already installed, the installation process may be omitted (S940)

[0162] The SM-SR establishes a security module in cooperation with the & quot; SIM service management platform & quot; through the & quot; issuance processing module & quot; utilizing a separate eUICC management key or a security key different from the eUICC public key, (Key generation algorithm, key length, etc.), if necessary (S950). Here, if the security module is already installed, the installation process may be omitted.

[0163] The SM-SR transmits the cipher key (public key, etc.) (cryptographic key information (key generation algorithm, key length, etc.)) and device information generated in the eUICC to the receiving MNO (S960)

[0164] The receiving MNO B sends the SM-DP a cryptographic key (public key, etc.) (if necessary cryptographic key information (key generation algorithm, key length, etc.)) and eUICC identification information (eICCID etc.) (Communication data, supplementary service application, supplementary service data, etc.) for the corresponding eUICC identification information (eICCID, etc.) with the received public key, and responds to the MNO B. At this time, the SM-DP can perform digital signature using its own private key to provide the certificate (S970)

[0165] Next, the MNO B requests the SM-SR to encrypt the carrier information encrypted with the public key using a separate eUICC management key or a security key, which is distinguished from the eUICC public key, so that the carrier information encrypted with the public key is loaded into the eUICC. And transmits it to the MNO B. (S980)

[0166] The MNO B issues the provider information in the device through the SM-SR (S990). In this case, when the authentication is provided, the public key of the SM-DP can be transmitted to the device.

[0167] Finally, the SM-SR communicates with the & quot; issuance processing module & quot; of the eUICC to perform status and DB update (S1000).

[0168] The steps S910 through S1000 of FIG. 9 may be integrated into one unit or integrated into one unit as needed.

[0169] According to one embodiment of the present invention, the eUICC can guarantee integrity, confidentiality and authenticity for loading various profiles (provisioning profile, operation profile, etc.).

[0170] In addition, secure mechanisms that ensure integrity, confidentiality, and authenticity can protect various profiles within the eUICC architecture very securely, and as such, profiles are not transferred into the eUICC (rather than being provisioned at the manufacturing stage) It can provide a very secure mechanism for protecting the profile.

[0171] In addition, the profile or profile management data must be transmitted securely between the eUICC and the endpoint that is reliably connected to the operator system that owns the profile or profile management data, It is impossible to access by an external entity such as & lt; RTI ID = 0.0 &)

[0172] In particular, according to an embodiment of the present invention, it is possible not only to utilize a fixed public key / private key pair, but also to secure the eUICC issuance of provider information by generating a public key and a private key pair dynamically at each issuance time . In addition, a minimal change in existing standard technologies can lead to a realistic eUICC-based issuance structure.

[0173] The description above is merely illustrative of the technical idea of the present invention, and various modifications and changes may be made by those skilled in the art without departing from the essential characteristics of the present invention. Therefore, the embodiments disclosed in the present invention are not intended to limit the scope of the present invention but to limit the scope of the technical idea of the present invention. The scope of protection of the present invention should be construed according to the following claims, and all technical ideas within the scope of equivalents thereof should be construed as being included in the scope of the present invention.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0026351
(43) 공개일자 2013년03월13일

(51) 국제특허분류(Int. Cl.)
H04L 9/14 (2006.01) *H04L 29/06* (2006.01)
H04W 8/18 (2009.01)
(21) 출원번호 10-2011-0097900
(22) 출원일자 2011년09월28일
심사청구일자 없음
(30) 우선권주장
1020110089638 2011년09월05일 대한민국(KR)
1020110096210 2011년09월23일 대한민국(KR)

(71) 출원인
주식회사 케이티
경기도 성남시 분당구 불정로 90 (정자동 206 번지)
(72) 발명자
박재민
서울특별시 서초구 태봉로 151, KT연구개발센터 (우면동)
이진형
서울특별시 서초구 태봉로 151, KT연구개발센터 (우면동)
(74) 대리인
송해모, 김은구

전체 청구항 수 : 총 25 항

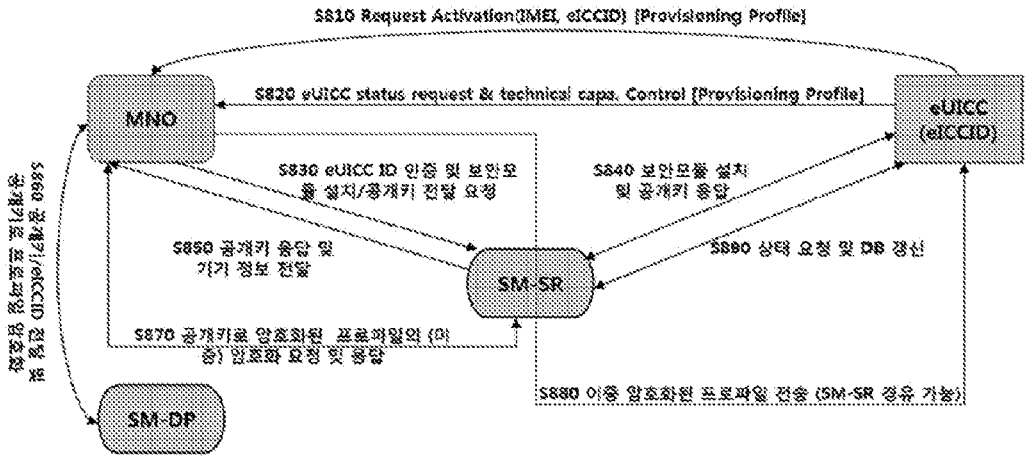
(54) 발명의 명칭 **eUICC의 프로파일 관리방법 및 그를 이용한 eUICC, eUICC 탑재 단말과, 프로비저닝 방법 및 MNO 변경 방법**

(57) 요 약

본 발명은 SM이 SM-SR(Secure Routing) 및 SM-DP(Data Preparation)으로 분리 구현되는 환경에서, MNO가 SM-SR을 통하여 해당 eUICC에게 할당된 암호키를 제공받는 방법을 제공하는 것, 즉, MNO가 SM-SR을 통하여 해당 eUICC로부터 동적으로 암호키(공개키 등)를 획득하여 사용하는 방법을 제공한다.

또한, 본 발명은 eUICC가 MNO 또는 SM으로부터 암호화된 프로파일을 수신하고, 그를 eUICC 내부에 저장되어 있는 프로파일 접근 크레덴셜 정보(eUICC 공개키에 대응되는 비밀키 등)를 이용하여 복호화하여 사용함으로써, 오퍼레이션 프로파일과 같이 중요한 데이터가 안전하게 전송되고, 단말 또는 터미널과 같은 외부 엔터티에 의해서 접근이 불가능하게 된다는 효과가 있다.

대 표 도



Petitioner Samsung Ex-1038, 0274

특허청구의 범위

청구항 1

통신사업자(MNO) 시스템, 가입 관리시스템(SM)과 연동되어 있는 내장 UICC(eUICC)를 이용한 프로파일 관리 방법으로서,

상기 eUICC가 상기 MNO 또는 SM으로부터 암호화된 프로파일을 수신하는 단계;

상기 eUICC 내부에 저장되어 있는 프로파일 접근 크레덴셜 정보를 이용하여 상기 프로파일을 복호화하는 단계를 포함하는 것을 특징으로 하는 eUICC의 프로파일 관리방법.

청구항 2

제1항에 있어서,

상기 암호화된 프로파일은 상기 eUICC의 공개키로 암호화되어 있으며, 상기 프로파일 접근 크레덴셜은 상기 eUICC 공개키에 대응되는 비밀키 또는 개인키 인 것을 특징으로 하는 eUICC의 프로파일 관리방법.

청구항 3

제2항에 있어서,

상기 SM은 SM-DP(Data Preparation) 및 SM-SR(Secure Routing) 장치를 포함하며, 상기 SM-DP는 상기 eUICC 공개키를 이용하여 상기 프로파일을 암호화하고, 상기 SM-SR은 eUICC 공개키로 1차 암호화된 프로파일을 별도의 관리키로 2차 암호화함으로써, 상기 암호화된 프로파일은 이중 암호화(Double Ciphered)된 프로파일 인 것을 특징으로 하는 eUICC의 프로파일 관리방법.

청구항 4

제4항에 있어서,

상기 프로파일은 프로비저닝을 위한 프로비저닝 프로파일, 오퍼레이션 프로파일, MNO 크레덴셜 정보 또는 MNO 크레덴셜 정보를 포함하는 패키지 정보, IMSI(International Mobile Subscriber Identity), 관리키(UICC OTA Key, GP ISD Key 등), 부가 서비스 어플리케이션, 부가 서비스 데이터 중 하나 이상의 정보를 포함하는 것을 특징으로 하는 eUICC의 프로파일 관리방법.

청구항 5

제2항에 있어서,

상기 암호화된 프로파일은 이중 암호화(Double Ciphered)된 프로파일이며, 상기 복호화 단계에서, eUICC는 별도의 관리키로 상기 프로파일을 1차 복호화하고, 상기 eUICC 공개키로 2차 복호화하는 것을 특징으로 하는 eUICC의 프로파일 관리방법.

청구항 6

통신사업자(MNO) 시스템, 가입 관리시스템(SM)과 연동되어 있는 내장 UICC(eUICC)를 이용한 프로파일 관리 방법으로서,

상기 SM은 상기 eUICC를 관리하는 기능을 수행하는 단계;

상기 eUICC는 상기 MNO 또는 SM으로부터 프로파일-프로파일은 상기 eUICC로 제공되어야 하는 파일 구조, 데이터 및 애플리케이션의 조합을 의미함-을 수신하는 단계;

상기 eUICC는 프로파일 접근 크레덴셜-프로파일 내부 또는 eUICC 내부에 존재하는 데이터로서, 프로파일 구조 및 그 데이터를 보호 또는 관리하기 위하여 eUICC 및 외부 엔터티 사이에 보안 통신이 셋업 될 수 있도록 하는 데이터를 의미함-을 이용하여 상기 수신된 프로파일을 처리 또는 관리하는 단계; 및,

상기 eUICC는 상기 eUICC를 포함하는 단말 또는 터미널이 접근할 수 없도록 상기 수신된 프로파일 정보 또는 상

Petitioner Samsung Ex-1038, 0275

기 프로파일 접근 크레덴셜을 이용하여 처리된 프로파일 정보를 관리하는 단계;

를 포함하는 것을 특징으로 하는 eUICC의 프로파일 관리방법.

청구항 7

제6항에 있어서,

상기 수신된 프로파일은 이중 암호화(Double Ciphered)된 프로파일이며, 상기 프로파일 접근 크레덴셜은 상기 eUICC에 고유한 공개키 또는 그에 대응되는 비밀키 또는 개인키 인 것을 특징으로 하는 eUICC의 프로파일 관리 방법.

청구항 8

제7항에 있어서,

상기 SM은 SM-DP(Data Preparation) 및 SM-SR(Secure Routing) 장치를 포함하는 것을 특징으로 하는 eUICC의 프로파일 관리방법.

청구항 9

통신사업자(MNO) 시스템, 가입 관리시스템(SM)과 연동되어 있는 내장 UICC(eUICC)로서,

상기 eUICC는 상기 eUICC를 포함하는 단말 또는 터미널이 접근할 수 없도록, 상기 MNO 또는 SM으로부터 수신한 프로파일-프로파일은 상기 eUICC로 제공되어야 하는 파일 구조, 데이터 및 애플리케이션의 조합을 의미함-을 관리하기 위한 프로파일 접근 크레덴셜 정보- 프로파일 내부 또는 eUICC 내부에 존재하는 데이터로서, 프로파일 구조 및 그 데이터를 보호 또는 관리하기 위하여 eUICC 및 외부 엔터티 사이에 보안 통신이 셋업 될 수 있도록 하는 데이터를 의미함-을 포함하는 것을 특징으로 하는 eUICC.

청구항 10

제9항에 있어서,

상기 프로파일 접근 크레덴셜 정보는 상기 eUICC에 고유하게 할당되는 공개키 또는 그에 대응되는 개인키인 것을 특징으로 하는 eUICC.

청구항 11

제10항에 있어서,

상기 eUICC는 상기 프로파일 접근 크레덴셜 정보를 이용하여 인증성(Authenticity)을 보장할 수 있는 것을 특징으로 하는 eUICC.

청구항 12

통신사업자(MNO) 시스템, 가입 관리시스템(SM)과 연동되어 있는 내장 UICC(eUICC)가 탑재된 eUICC 탑재 단말로서,

상기 eUICC 단말은 상기 MNO 또는 SM으로부터 수신한 프로파일을 관리하기 위한 프로파일 접근 크레덴셜 정보를 생성 및 관리하는 발급처리모듈을 포함하며,

상기 발급처리모듈은 상기 SM으로부터의 요청에 따라 자체적 또는 별도의 내부 보안모듈을 이용하여 상기 eUICC를 위한 프로파일 접근 크레덴셜 정보인 공개키를 생성하여 응답하며, 상기 eUICC 공개키로 암호화된 프로파일 정보를 MNO 또는 SM으로부터 수신한 후 상기 공개키에 대응되는 비밀키(또는 개인키)로 복호화를 수행하는 것을 특징으로 하는 eUICC 탑재 단말.

청구항 13

제12항에 있어서,

상기 SM은 SM-DP(Data Preparation) 및 SM-SR(Secure Routing) 장치를 포함하며, 상기 발급처리모듈은 상기 SM-SR로부터의 요청에 따라 상기 보안모듈을 설치하는 것을 특징으로 하는 eUICC 탑재 단말.

Petitioner Samsung Ex-1038, 0276

청구항 14

제13항에 있어서,

상기 발급처리모듈은 상기 SM-SR로 eUICC 공개키를 응답할 때, 상기 공개키의 암호화 정보-키생성 알고리즘, 키 길이 정보를 포함함-를 함께 전달하는 것을 특징으로 하는 eUICC 탑재 단말.

청구항 15

제13항에 있어서,

상기 암호화된 프로파일 정보는 상기 eUICC 공개키 및 eUICC 관리키로 이중 암호화(Double Ciphered)된 것을 특징으로 하는 eUICC 탑재 단말.

청구항 16

제15항에 있어서,

상기 이중 암호화된 프로파일 정보에는 상기 프로파일을 생성한 SM-DP 또는 MNO의 개인키로 생성된 전자서명 정보가 포함되는 것을 특징으로 하는 eUICC 탑재 단말.

청구항 17

제15항에 있어서,

상기 eUICC 관리키는 eUICC OTA 키, GP ISD 키 중 하나 이상인 것을 특징으로 하는 eUICC 탑재 단말.

청구항 18

통신사업자(MNO) 시스템, 가입 관리시스템(SM)과 연동되어 있는 내장 UICC(eUICC)로서,

상기 eUICC를 탑재한 단말내의 발급처리모듈로부터의 요청에 따라 암호화된 프로파일을 복호화하는 보안모듈을 포함하며,

상기 보안모듈은 상기 발급처리 모듈의 요청에 따라 상기 eUICC에 해당되는 공개키를 생성하여 외부 SM으로 전달하는 기능을 추가로 구비하는 것을 특징으로 하는 eUICC.

청구항 19

제18항에 있어서,

상기 보안모듈은 상기 eUICC의 공개키에 대응되는 비밀키를 이용하여 상기 프로파일에 대한 복호화를 수행하는 것을 특징으로 하는 eUICC.

청구항 20

통신사업자(MNO) 시스템, 가입 관리시스템(SM)과 연동되어 있는 내장 UICC(eUICC)로서,

칩 오퍼레이팅 시스템(COS)와, SIM 플랫폼 및 SIM 서비스 관리 플랫폼을 포함하며, 상기 SIM 서비스 관리 플랫폼 상에는 하나 이상의 MNO에 대한 오퍼레이팅 프로파일(사업자 정보) 및 보안모듈을 포함하며,

상기 보안모듈을 상기 SIM 서비스 관리 플랫폼의 요청에 따라 상기 eUICC의 공개키를 생성하여 출력하고, 외부로부터 수신된 암호화된 프로파일을 상기 eUICC 공개키에 대응되는 비밀키로 복호화하는 것을 특징으로 하는 eUICC.

청구항 21

사업자 시스템(MNO), 가입 관리 시스템(Subcription Manager; SM)을 구성하는 SM-SR(Secure Routing) 및 SM-DP(Data Preparation) 상치와 연동된 내상 UICC(eUICC)를 이용한 프로비저닝 방법으로서,

상기 SM-SR이 상기 eUICC로부터 eUICC 공개키를 전달받고, 상기 eUICC 공개키를 상기 MNO로 전달하는 단계;

상기 SM-DP가 상기 MNO를 통해 전달받은 상기 eUICC 공개키로 프로파일을 1차 암호화한 후에 상기 MNO로 전달하

Petitioner Samsung Ex-1038, 0277

는 단계;

상기 MNO가 SM-SR에게 요청하여 상기 1차 암호화된 프로파일에 대해서 별도의 보안키로 2차 암호화한 프로파일을 요청하는 단계;

상기 MNO 또는 상기 SM-SR이 상기 2차 암호화된 이중 암호화 프로파일 정보를 상기 eUICC로 전달하는 단계;

를 포함하는 것을 특징으로 하는 프로비저닝 방법.

청구항 22

제21항에 있어서,

상기 eUICC는 상기 이중 암호화 프로파일에 대해서 상기 보안키로 1차 복호화하고, 상기 eUICC 공개키에 대응되는 비밀키로 2차 복호화하여 원래의 프로파일 정보를 복호화하는 단계를 추가로 포함하는 것을 특징으로 하는 프로비저닝 방법.

청구항 23

제21항에 있어서,

상기 eUICC가 상기 MNO로 eUICC 식별정보(eICCId)를 포함하는 활성화 요청을 전송하는 단계;

상기 MNO와 상기 eUICC 사이에서 상기 eUICC의 상태 확인 및 기술 성능을 확인하는 단계를 추가로 포함하는 것을 특징으로 하는 프로비저닝 방법.

청구항 24

리시빙 사업자 시스템(Receiving MNO), 도너 사업자 시스템(Donor MNO), 가입 관리 시스템(Subcription Manager; SM)을 구성하는 SM-SR(Secure Routing) 및 SM-DP(Data Preparation) 장치와 연동된 내장 UICC(eUICC)를 이용한 MNO 변경 방법으로서,

상기 SM-SR이 상기 eUICC로부터 eUICC 공개키를 전달받고, 상기 eUICC 공개키를 상기 리시빙 MNO로 전달하는 단계;

상기 리시빙 MNO는 상기 도너 MNO로 사업자 변경에 대한 통지를 전달하는 단계;

상기 SM-DP가 상기 리시빙 MNO를 통해 전달받은 상기 eUICC 공개키로 프로파일을 1차 암호화한 후에 상기 리시빙 MNO로 전달하는 단계;

상기 리시빙 MNO가 SM-SR에게 요청하여 상기 1차 암호화된 프로파일에 대해서 별도의 보안키로 2차 암호화한 프로파일을 요청하는 단계;

상기 리시빙 MNO 또는 상기 SM-SR이 상기 2차 암호화된 이중 암호화 프로파일 정보를 상기 eUICC로 전달하는 단계;

를 포함하는 것을 특징으로 하는 MNO 변경 방법.

청구항 25

제24항에 있어서,

상기 eUICC가 상기 리시빙 MNO로 eUICC 식별정보(eICCId)를 포함하는 활성화 요청을 전송하는 단계;

상기 리시빙 MNO와 상기 eUICC 사이에서 상기 eUICC의 상태 확인 및 기술 성능을 확인하는 단계를 추가로 포함하는 것을 특징으로 하는 MNO 변경 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 내장 UICC(Embedded Universal Integrated Circuit Card; 이하 'eUICC'라 함) 프로파일 관리 방법

Petitioner Samsung Ex-1038, 0278

과, 그를 이용한 eUICC, eUICC 탑재 단말과, 프로비저닝 방법 및 MNO 변경 방법, 특히 eUICC에서 프로파일 접근 크레덴셜(Profile access credentials)을 이용하여 각종 프로파일을 관리 또는 핸들링하는 방법에 관한 것이다. 또한, SM 기능 분리 환경에서 프로파일 접근 크레덴셜로서의 공개키를 동적으로 생성하여 eUICC가 사용하도록 하는 eUICC 관리방법에 관한 것이다.

배경기술

[0002] UICC(Universal Integrated Circuit Card)는 단말기 내에 삽입되어 사용자 인증을 위한 모듈로서 사용될 수 있는 스마트 카드이다. UICC는 사용자의 개인 정보 및 사용자가 가입한 이동 통신 사업자에 대한 사업자 정보를 저장할 수 있다. 예를 들면, UICC는 사용자를 식별하기 위한 IMSI(International Mobile Subscriber Identity)를 포함할 수 있다. UICC는 GSM(Global System for Mobile communications) 방식의 경우 SIM(Subscriber Identity Module) 카드, WCDMA(Wideband Code Division Multiple Access) 방식의 경우 USIM(Universal Subscriber Identity Module) 카드로 불리기도 한다.

[0003] 사용자가 UICC를 사용자의 단말에 장착하면, UICC에 저장된 정보들을 이용하여 자동으로 사용자 인증이 이루어져 사용자가 편리하게 단말을 사용할 수 있다. 또한, 사용자가 단말을 교체할 때, 사용자는 기존의 단말에서 탈거한 UICC를 새로운 단말에 장착하여 용이하게 단말을 교체할 수 있다.

[0004] 소형화가 요구되는 단말, 예를 들면 기계 대 기계(Machine to Machine, M2M) 통신을 위한 단말은 UICC를 착탈할 수 있는 구조로 제조할 경우 단말의 소형화가 어려워진다. 그리하여, 착탈할 수 없는 UICC인 eUICC 구조가 제안되었다. eUICC는 해당 UICC를 사용하는 사용자 정보가 IMSI 형태로 수록되어야 한다.

[0005] 기존의 UICC는 단말에 착탈이 가능하여, 단말의 종류나 이동 통신 사업자에 구애받지 않고 사용자는 단말을 개통할 수 있다. 그러나, 단말을 제조할 때부터 제조된 단말은 특정 이동 통신 사업자에 대해서만 사용된다는 전제가 성립되어야 eUICC 내의 IMSI를 할당할 수 있다. 단말을 발주하는 이동 통신 사업자 및 단말 제조사는 모두 제품 재고에 신경을 쓸 수 밖에 없고 제품 가격이 상승하는 문제가 발생하게 된다. 사용자는 단말에 대해 이동 통신 사업자를 바꿀 수 없는 불편이 있다. 그러므로, eUICC의 경우에도 이동 통신 사업자에 구애받지 않고 사용자가 단말을 개통할 수 있는 방법이 요구된다.

[0006] 한편, 최근 eUICC의 도입으로 인하여 여러 이통통신 사업자의 가입자 정보를 원격에서 UICC로 업데이트 할 필요가 생기게 되었고, 그에 따라 가입자 정보 관리를 위한 가입 관리 장치(Subscription Manager; 이하 'SM' 이라 함) 또는 프로파일 관리장치(Profile Manager; 이하 'PM' 이라 함)가 논의되고 있다.

[0007] 이러한 SM은 주로 eUICC에 대한 정보 관리와, 여러 이통통신 사업자에 대한 정보 관리와, 이동통신 사업자 변경 시 그에 대한 인증 및 원격 정보 변경 등의 기능을 담당하는 것으로 논의되고 있으나, 정확한 기능이나 역할에 대해서는 아직 결정된 바가 없는 실정이다.

[0008] 또한, eUICC가 사용되는 환경에서, eUICC로 중요한 프로파일이 제공될 수 있는데, 이러한 프로파일을 안전하게 전달 및 사용할 수 있도록 하는 메커니즘이 필요하다.

발명의 내용

해결하려는 과제

[0009] 본 발명은 eUICC를 관리하기 위한 방법을 제공한다.

[0010] 본 발명은 eUICC에서 프로파일 접근 크레덴셜을 이용하여 각종 프로파일(프로비저닝 프로파일, 오퍼레이션 프로파일 등)을 관리 또는 핸들링하는 방법을 제공한다.

[0011] 본 발명은 eUICC에서 엔드 포인트(End point; 예를 들면 SM)로부터 전송되는 각종 프로파일(프로비저닝 프로파일, 오퍼레이션 프로파일 등)을 안전하게 프로비저닝 하기 위한 프로파일 접근 크레덴셜(예를 들면, eUICC의 공개키 등)을 최소한 1개 세트 이상 보유하도록 관리하는 방법을 제공한다.

[0012] 또한, 본 발명의 목적은 eUICC가 오퍼레이터(MNO) 시스템과 신뢰성 있게 연결된 엔드 포인트로부터 송수신되는 프로파일 또는 프로파일 관리 데이터를 단말 또는 터미널과 같은 외부 엔터티에 의해서 접근이 불가능하도록 관리하는 방법을 제공한다.

[0013] 본 발명의 다른 목적은 SM이 SM-SR(Secure Routing) 및 SM-DP(Data Preparation)으로 분리 구현되는 환경에서,

Petitioner Samsung Ex-1038, 0279

Petitioner Samsung Ex-1038, 0280

eUICC를 관리하는 방법을 제공하는 것이다.

[0014] 본 발명의 또다른 목적은 SM이 SM-SR(Secure Routing) 및 SM-DP(Data Preparation)으로 분리 구현되는 환경에서, SM-SR이 보안 정보를 암호화할 수 있는 암호키(공개키 등)를 보유/관리하는 방법을 제공하는 것이다.

[0015] 본 발명의 또다른 목적은 SM이 SM-SR(Secure Routing) 및 SM-DP(Data Preparation)으로 분리 구현되는 환경에서, MNO가 SM-SR을 통하여 해당 eUICC에게 할당된 암호키를 제공받는 방법을 제공하는 것이다.

[0016] 본 발명의 다른 목적은 MNO가 SM-SR을 통하여 해당 eUICC로부터 동적으로 암호키(공개키 등)를 획득하여 사용하는 방법을 제공하는 것이다.

발명의 해결 수단

[0017] 본 발명의 일 실시예는, 통신사업자(MNO) 시스템, 가입 관리시스템(SM)과 연동되어 있는 내장 UICC(eUICC)를 이용한 프로파일 관리 방법으로서, 상기 eUICC가 상기 MNO 또는 SM으로부터 암호화된 프로파일을 수신하는 단계와, 상기 eUICC 내부에 저장되어 있는 프로파일 접근 크레덴셜 정보를 이용하여 상기 프로파일을 복호화하는 단계를 포함하는 eUICC의 프로파일 관리방법을 제공한다.

[0018] 본 발명의 또다른 실시예는, 통신사업자(MNO) 시스템, 가입 관리시스템(SM)과 연동되어 있는 내장 UICC(eUICC)를 이용한 프로파일 관리 방법으로서, 상기 SM은 상기 eUICC를 관리하는 기능을 수행하는 단계와, 상기 eUICC는 상기 MNO 또는 SM으로부터 프로파일-프로파일은 상기 eUICC로 제공되어야 하는 파일 구조, 데이터 및 애플리케이션의 조합을 의미함-을 수신하는 단계와, 상기 eUICC는 프로파일 접근 크레덴셜-프로파일 내부 또는 eUICC 내부에 존재하는 데이터로서, 프로파일 구조 및 그 데이터를 보호 또는 관리하기 위하여 eUICC 및 외부 엔터티 사이에 보안 통신이 셋업 될 수 있도록 하는 데이터를 의미함-을 이용하여 상기 수신된 프로파일을 처리 또는 관리하는 단계 및 상기 eUICC는 상기 eUICC를 포함하는 단말 또는 터미널이 접근할 수 없도록 상기 수신된 프로파일 정보 또는 상기 프로파일 접근 크레덴셜을 이용하여 처리된 프로파일 정보를 관리하는 단계를 포함하는 eUICC의 프로파일 관리방법을 제공한다.

[0019] 본 발명의 다른 실시예는 통신사업자(MNO) 시스템, 가입 관리시스템(SM)과 연동되어 있는 내장 UICC(eUICC)로서, 상기 eUICC는 상기 eUICC를 포함하는 단말 또는 터미널이 접근할 수 없도록, 상기 MNO 또는 SM으로부터 수신한 프로파일-프로파일은 상기 eUICC로 제공되어야 하는 파일 구조, 데이터 및 애플리케이션의 조합을 의미함-을 관리하기 위한 프로파일 접근 크레덴셜 정보- 프로파일 내부 또는 eUICC 내부에 존재하는 데이터로서, 프로파일 구조 및 그 데이터를 보호 또는 관리하기 위하여 eUICC 및 외부 엔터티 사이에 보안 통신이 셋업 될 수 있도록 하는 데이터를 의미함-을 포함하는 eUICC를 제공한다.

[0020] 본 발명의 다른 실시예는 통신사업자(MNO) 시스템, 가입 관리시스템(SM)과 연동되어 있는 내장 UICC(eUICC)가 탑재된 eUICC 탑재 단말로서, 상기 eUICC 단말은 상기 MNO 또는 SM으로부터 수신한 프로파일을 관리하기 위한 프로파일 접근 크레덴셜 정보를 생성 및 관리하는 발급처리모듈을 포함하며, 상기 발급처리모듈은 상기 SM으로부터의 요청에 따라 자체적 또는 별도의 내부 보안모듈을 이용하여 상기 eUICC를 위한 프로파일 접근 크레덴셜 정보인 공개키를 생성하여 응답하며, 상기 eUICC 공개키로 암호화된 프로파일 정보를 MNO 또는 SM으로부터 수신한 후 상기 공개키에 대응되는 비밀키(또는 개인키)로 복호화를 수행하는 eUICC 탑재 단말을 제공한다.

[0021] 본 발명의 다른 실시예는, 통신사업자(MNO) 시스템, 가입 관리시스템(SM)과 연동되어 있는 내장 UICC(eUICC)로서, 상기 eUICC를 탑재한 단말내의 발급처리모듈로부터의 요청에 따라 암호화된 프로파일을 복호화하는 보안모듈을 포함하며, 상기 보안모듈은 상기 발급처리 모듈의 요청에 따라 상기 eUICC에 해당되는 공개키를 생성하여 외부 SM으로 전달하는 기능을 추가로 구비하는 eUICC을 제공한다.

[0022] 본 발명의 다른 실시예는 통신사업자(MNO) 시스템, 가입 관리시스템(SM)과 연동되어 있는 내장 UICC(eUICC)로서, 칩 오퍼레이팅 시스템(COS)와, SIM 플랫폼 및 SIM 서비스 관리 플랫폼을 포함하며, 상기 SIM 서비스 관리 플랫폼 상에는 하나 이상의 MNO에 대한 오퍼레이팅 프로파일(사업자 정보) 및 보안모듈을 포함하며, 상기 보안모듈을 상기 SIM 서비스 관리 플랫폼의 요청에 따라 상기 eUICC의 공개키를 생성하여 출력하고, 외부로부터 수신된 암호화된 프로파일을 상기 eUICC 공개키에 대응되는 비밀키로 복호화하는 eUICC를 제공한다.

[0023] 본 발명의 다른 실시예는, 사업자 시스템(MNO), 가입 관리 시스템(Subcription Manager; SM)을 구성하는 SM-

SR(Secure Routing) 및 SM-DP(Data Preparation) 장치와 연동된 내장 UICC(eUICC)를 이용한 프로비저닝 방법으로서, 상기 SM-SR이 상기 eUICC로부터 eUICC 공개키를 전달받고, 상기 eUICC 공개키를 상기 MNO로 전달하는 단계와, 상기 SM-DP가 상기 MNO를 통해 전달받은 상기 eUICC 공개키로 프로파일을 1차 암호화한 후에 상기 MNO로 전달하는 단계와, 상기 MNO가 SM-SR에게 요청하여 상기 1차 암호화된 프로파일에 대해서 별도의 보안키로 2차 암호화한 프로파일을 요청하는 단계와, 상기 MNO 또는 상기 SM-SR이 상기 2차 암호화된 이중 암호화 프로파일 정보를 상기 eUICC로 전달하는 단계를 포함하는 프로비저닝 방법을 제공한다.

[0024] 본 발명의 또다른 실시예는, 리시빙 사업자 시스템(Receiving MNO), 도너 사업자 시스템(Donor MNO), 가입 관리 시스템(Subcription Manager; SM)을 구성하는 SM-SR(Secure Routing) 및 SM-DP(Data Preparation) 장치와 연동된 내장 UICC(eUICC)를 이용한 MNO 변경 방법으로서, 상기 SM-SR이 상기 eUICC로부터 eUICC 공개키를 전달받고, 상기 eUICC 공개키를 상기 리시빙 MNO로 전달하는 단계와, 상기 리시빙 MNO는 상기 도너 MNO로 사업자 변경에 대한 통지를 전달하는 단계와, 상기 SM-DP가 상기 리시빙 MNO를 통해 전달받은 상기 eUICC 공개키로 프로파일을 1차 암호화한 후에 상기 리시빙 MNO로 전달하는 단계와, 상기 리시빙 MNO가 SM-SR에게 요청하여 상기 1차 암호화된 프로파일에 대해서 별도의 보안키로 2차 암호화한 프로파일을 요청하는 단계와, 상기 리시빙 MNO 또는 상기 SM-SR이 상기 2차 암호화된 이중 암호화 프로파일 정보를 상기 eUICC로 전달하는 단계를 포함하는 MNO 변경 방법을 제공한다.

도면의 간단한 설명

[0025] 도 1은 본 발명이 적용되는 eSIM(eUICC)을 포함한 전체 서비스 아키텍처를 도시한다.

도 2는 본 발명이 적용될 수 있는 SM 분리 환경의 시스템 아키텍처를 도시한다.

도 3은 본 발명이 적용되는 서비스 아키텍처에서 프로비저닝 과정의 전체 흐름도이다.

도 4는 본 발명이 적용되는 가입 변경 또는 MNO 변경 과정의 전체 흐름도이다.

도 5는 본 발명의 일 실시예에 의한 eUICC 또는 eSIM의 내부 구조를 도시한다.

도 6은 본 발명의 일 실시예에 의한 eUICC 또는 eSIM의 프로파일 설치 구조(발급처리 모듈 주도)를, 도 7은 SIM 서비스 관리 플랫폼 주도의 프로파일 설치 구조를 도시한다.

도 8은 본 발명의 일 실시예에 의한 프로비저닝(초기 개통)과정의 흐름을 도시한다.

도 9은 본 발명의 일 실시예에 의한 MNO 변경 과정의 흐름을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0026] 이하, 본 발명의 일부 실시예들을 예시적인 도면을 통해 상세하게 설명한다. 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 발명을 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.

[0027] 현재 GSMA에서 활발하게 논의되는 M2M(Machine-to-Machine) 단말은 특성상 크기가 작아야 하는데, 기존 UICC를 사용하는 경우에는, M2M 단말에 UICC를 장착하는 모듈을 별도 삽입해야 하므로, UICC를 탈착가능한 구조로 M2M 단말을 제조하게 되면, M2M 단말의 소형화가 힘들게 된다.

[0028] 따라서, UICC 착탈이 불가능한 내장(Embedded) UICC 구조가 논의되고 있는데, 이때 M2M 단말에 장착되는 eUICC에는 해당 UICC를 사용하는 이동통신 사업자(Mobile Network Operator; 이하 'MNO'라 함)정보가 국제 모바일 가입자 식별자(International Mobile Subscriber Identity, IMSI) 형태로 UICC에 저장되어 있어야 한다.

[0029] 그러나, M2M 단말을 제조할 때부터 제조된 단말은 특정 MNO에서만 사용한다는 전제가 성립되어야 eUICC내의 IMSI를 할당할 수 있으므로, M2M 단말 또는 UICC를 발주하는 MNO나 제조하는 M2M 제조사 모두 제품 재고에 많은 신경을 할당할 수 밖에 없고 제품 가격이 상승하게 되는 문제가 있어, M2M 단말 확대에 큰 걸림돌이 되고 있는 상황이다.

[0030] 이와 같이, 기존의 착탈식 형태의 SIM과는 달리 단말에 일체형으로 탑재되는 내장 SIM (이하 eSIM 또는 eUICC이라 함)은 그 물리적 구조 차이로 인해 개통 권한, 부가 서비스 사업 주도권, 가입자 정보 보안 등에 대한 많은

Petitioner Samsung Ex-1038, 0281

이슈들이 존재한다. 이를 위해 GSMA 및 ETSI의 국제 표준화 기관에서는 사업자, 제조사, SIM 제조사(Vendor) 등의 유관 회사들과 최상위 구조를 포함한 필요한 요소에 대해 표준화 활동을 전개하고 있다. eSIM이 표준화 단체들을 통해 논의되면서 이슈의 중심에 있는 것은 SM으로서, 중요한 프로파일(Operator Credential, MNO Credential, Profile, eUICC Profile, Profile Package 등으로 불릴 수 있음)를 eSIM에 발급하고 가입 변경에 대한 프로세스를 처리하는 등 eSIM에 대한 전반적인 관리 역할을 수행하는 개체 또는 그 기능/역할을 의미한다.

[0031] 최근 GSMA에서는 SM의 역할을 사업자 정보를 생성하는 역할을 수행하는 SM-DP (Data Preparation)과 eSIM에 사업자 정보의 직접적 운반을 수행하는 SM-SR (Secure Routing)로 분류한 구조를 제안하였으나, 세부적이며 기술적인 실제 발급 방식에 대해서는 언급하고 있지 않다.

[0032] 이에 본 발명에서는 GSMA의 SM 역할 분리 환경에서 동적 암호키 (공개 키 등) 생성을 활용하여 eSIM을 관리하는 방안을 제시한다.

[0033] 본 명세서에서는 eSIM과 eUICC를 동등한 개념으로 사용한다.

[0034] eSIM은 단말 제조 단계에서 IC칩을 단말 회로판 상에 부착시킨 후, 소프트웨어 형태의 SIM 데이터 (개통 정보, 부가 서비스 정보 등)를 OTA (Over The Air) 또는 오프라인 (PC와의 USB 등의 기술 기반 연결)을 통해 발급하는 방식의 새로운 개념의 SIM 기술이다. eSIM에서 사용되는 IC칩은 일반적으로 하드웨어 기반의 CCP (Crypto Co-Processor)를 지원하여 하드웨어 기반의 공개키 생성을 제공하며, 이를 어플리케이션 (예, 애플릿) 기반에서 활용할 수 있는 API를 SIM 플랫폼 (예, Java Card Platform 등)에서 제공한다. 자바 카드 플랫폼(Java Card Platform)은 스마트카드 등에서 멀티 어플리케이션을 탑재하고 서비스를 제공할 수 있는 플랫폼 중 하나이다.

[0035] SIM은 제한된 메모리 공간과 보안상의 이유로 누구나 SIM 내에 어플리케이션을 탑재해서는 안되며, 이로 인해 어플리케이션 탑재를 위한 플랫폼 이외에 SIM을 어플리케이션 탑재 및 관리를 담당하는 SIM 서비스 관리 플랫폼을 필요로 한다. SIM 서비스 관리 플랫폼은 관리키를 통한 인증 및 보안을 통해 SIM 메모리 영역에 데이터를 발급하며, 글로벌 플랫폼(GlobalPlatform)과 ETSI TS 102.226의 RFM (Remote File Management) 및 RAM (Remote Application Management)은 이와 같은 SIM 서비스 관리 플랫폼의 표준 기술이다.

[0036] eSIM 환경에서 중요한 요소 중의 하나인 SM은 eSIM은 원격으로 관리키(UICC OTA Key, GP ISD Key 등)를 통해 통신 및 부가 서비스 데이터를 발급하는 역할을 수행한다.

[0037] 여기서, 관리키 또는 eSIM 관리키 또는 eUICC 관리키는 eSIM으로의 접근 인증키로서 사업자 정보를 안전하게 eSIM으로 전달하기 위한 것이며, 본 발명에서 주로 다루는 암호키 (공개키 등)과는 구별되는 개념이며, 아래 설명할 바와 같이 eUICC 접근 크레덴셜(eUICC access credentials)로 표현될 수도 있을 것이다.

[0038] GSMA에서는 SM의 역할을 SM-DP와 SM-SR로 분류하였다. SM-DP는 오퍼레이션 프로파일(또는 사업자 정보) 이외에 IMSI, K, OPc, 부가 서비스 어플리케이션, 부가 서비스 데이터 등을 안전하게 빌드(Build)하여 크레덴셜 패키지 (Credential Package) 형태로 만드는 역할을 수행하며, SM-SR은 SM-DP가 생성한 크레덴셜 패키지를 OTA(Over-The-Air) 또는 GP SCP (Secure Communication Protocol)과 같은 SIM 원격 관리 기술을 통해 eSIM에 안전하게 다운로드하는 역할을 수행한다.

[0039] 그리고 아래 도 1의 "신뢰 서클(Circle of Trust)"이라는 구조를 제안하여 각 유사 개체 또는 엔터티 들간에 신뢰 관계의 중첩을 통해 MNO와 eSIM 간의 엔드-투-엔드(End-to-End) 신뢰 관계를 구축한다는 개념을 제안하였다. 즉, MNO1는 SM1과, SM1은 SM4, SM4는 eSIM과 신뢰관계를 형성하여, 이를 통해 MNO와 eSIM 간의 신뢰관계를 형성한다는 개념이다.

[0040] 본 발명을 설명하기 전에 우선 본 명세서에서 사용할 용어에 대하여 설명한다.

[0041] MNO(Mobile Network Operator)는 이동통신 사업자를 의미하며, 모바일 네트워크를 통해 고객에게 통신 서비스를 제공하는 엔터티를 의미한다.

[0042] SM(Subscription manager)는 가입 관리 장치로서, eUICC의 관리 기능을 수행한다.

[0043] eUICC 공급자(eUICC Supplier)는 eUICC 모듈과 내장 소프트웨어(펌웨어와 오퍼레이팅 시스템 등)를 공급하는 자를 의미한다.

[0044] 장치 공급자(Device Vendor)는 장치의 공급자, 특히 MNO에 의해서 구동되는 모바일 네트워크를 통한 무선 모뎀 기능을 포함하며, 따라서 결과적으로 UICC(또는 eUICC) 형태가 필요한 장치의 공급자를 의미한다.

Petitioner Samsung Ex-1038, 0282

[0045] 프로비저닝(Provisioning)은 eUICC 내부로 프로파일을 로딩하는 과정을 의미하며, 프로비저닝 프로파일은 다른 프로비저닝 프로파일 및 오퍼레이션 프로파일을 프로비저닝할 목적으로 장치가 통신 네트워크에 접속하는데 사용되는 프로파일을 의미한다.

[0046] 가입(Subscription)은 가입자와 무선통신 서비스 제공자 사이의 서비스 제공을 위한 상업적인 관계를 의미한다.

[0047] eUICC 접근 크레덴셜(eUICC access credentials)은 eUICC 상의 프로파일을 관리하기 위하여 eUICC 및 외부 엔터티 사이에 보안 통신이 셋업 될 수 있도록 하는 eUICC 내의 데이터를 의미한다.

[0048] 프로파일 엑세스 크레덴셜(Profile access credentials)은 프로파일 내부 또는 eUICC 내부에 존재하는 데이터로서, 프로파일 구조 및 그 데이터를 보호 또는 관리하기 위하여 eUICC 및 외부 엔터티 사이에 보안 통신이 셋업 될 수 있도록 하는 데이터를 의미한다.

[0049] 프로파일(Profile)은 eUICC로 프로비저닝 되거나 eUICC 내에서 관리될 수 있는 파일 구조, 데이터 및 애플리케이션의 조합으로서, 사업자 정보인 오퍼레이션 프로파일, 프로비저닝을 위한 프로비저닝 프로파일, 기타 정책 제어 기능(PCF; Policy Control Function)을 위한 프로파일 등 eUICC 내에 존재할 수 있는 모든 정보를 의미한다.

[0050] 오퍼레이션 프로파일(Operation Profile) 또는 사업자 정보는 사업자 가입(Operational Subcription)과 관련된 모든 종류의 프로파일을 의미한다.

[0051] 도 1은 본 발명이 적용되는 cSIM(cUICC)을 포함한 전체 서비스 아키텍처를 도시한다.

[0052] 전체 시스템에 대해서 설명하면 다음과 같다.

[0053] 본 발명이 적용될 수 있는 eUICC 시스템 아키텍처는 다수의 MNO 시스템과, 1 이상의 SM 시스템, eUICC 제조사 시스템, eUICC를 포함하는 장치(Device) 제조사 시스템 및 eUICC 등을 포함할 수 있으며, 각 엔터티 또는 주체에 대한 설명은 다음과 같다.

[0054] 도 1에서 점선은 신뢰 서클을 도시하고, 2개 실선은 안전한 링크를 의미한다.

[0055] 가입정보가 저장되어 전달되는 시나리오가 필요하면, MNO의 승인과 MNO의 컨트롤 하에서 이루어져야 한다. 특정 시각에 단일의 eUICC 상에는 1개만의 액티브 프로파일이 있어야 하며, 이 때 액티브 프로파일은 특정 시각에 단일 HLR에 부가되는 것을 의미한다.

[0056] MNO와 eUICC는 MNO 크레덴셜(Credentials) 정보, 즉 프로파일(오퍼레이션 프로파일, 프로비저닝 프로파일 등)를 복호할 수 있어야 한다. 이에 대한 유일한 예외는 예를 들면 SIM 벤더와 같이 특정 MNO으로부터 위임받은 제3 기관이 될 수 있다. 하지만, 이를 수행하기 위한 제3 기관의 일반적인 기능은 아니다.

[0057] 가입(Subscription)은 오퍼레이터 정책 제어의 외부에서는 eUICC 내에서 스위칭될 수 없다. 사용자는 MNO 컨텐스트와 그의 활성화 가입의 어떠한 변경도 알고 있어야 하며, 시큐리티 위험을 피할 수 있어야 하고, 현재의 UICC 모델과 대적할 수 있을 정도의 시큐리티 레벨이 필요하다.

[0058] MNO 크레덴셜 또는 프로파일은 K, 알고리즘, 알고리즘 파라미터, 부가 서비스 어플리케이션, 부가 서비스 데이터 등을 포함하는 가입 크레덴셜을 의미할 수 있다.

[0059] MNO 크레덴셜 또는 프로파일의 전달은 종단에서 종단까지 안전한 방식으로 이루어져야 한다. 전송은 시큐리티 체인을 깨지 않는 연속적인 단계로 이루어질 수 있으며, 전송 체인의 모든 단계는 MNO의 인식 및 승인 하에서 이루어져야 한다. 전송 체인 내의 어떠한 엔터티도 MNO 크레덴셜을 명확하게 볼 수 없어야 하지만, 유일한 예외는 예를 들면 SIM 벤더와 같이 특정 MNO으로부터 위임받은 제3 기관이 될 수 있다. 하지만, 이를 수행하기 위한 제3 기관의 일반적인 기능은 아니다.

[0060] 오퍼레이터는 자신의 크레덴셜에 대해서 완전한 제어권을 가져야 하며, 오퍼레이터는 SM 오퍼레이션에 대해서 강한 감독권과 제어권한을 가져야 한다.

[0061] SM 기능은 MNO 또는 제3 기관에 의하여 제공되어야 하며, 만약 제3 기관에 의하여 제공된다면 SM과 MNO 사이에는 상업적인 관계가 설정되어 있는 경우 등일 것이다.

[0062] SM은 가입 관리를 위해서 MNO 가입자와 어떠한 직접적인 관련도 없다. MNO가 가입자와 관계를 가지며 고객 가입을 위한 진입 포인트가 되어야 하지만, 이는 M2M 서비스 제공자(M2M 서비스 제공자는 MNO 가입자 임)가 자신의

Petitioner Samsung Ex-1038, 0283

고객과 가질 수 있는 계약 관계에 편승할 의도는 아니다.

[0063] MNO가 스왑(swap)되는 동안, 도너(Donor) 및 리시빙 MNO는 서로 사전 계약이 있을 수도 있고 없을 수도 있다. 사전 계약을 승인할 수 있는 메커니즘이 있어야 한다. 도너 오퍼레이터의 정책 제어(Policy Control) 기능은 자신의 크레덴셜의 제거 조건에 대하여 정의할 수 있으며, 정책 제어 기능(Policy Control Function; PCF)이 이러한 기능을 구현할 수 있다.

[0064] 아키텍처는 SM이라고 정의되는 기능을 도입하며, SM의 주요한 역할은 MNO 크레덴셜을 포함하는 패키지 또는 프로파일을 준비해서 eUICC로 전달하는 것이다. SM 기능은 MNO에 의하여 직접적으로 제공될 수도 있고, MNO가 SM 서비스를 획득하기 위하여 제3 기관과 계약할 수도 있을 것이다.

[0065] SM의 역할은 SM-SR, SM-DP와 같은 2개의 서브 기능으로 나뉘어 질 수 있다.

[0066] 실제로, 이러한 SM-SR, SM-DP 기능들은 다른 엔터티에 의하여 제공될 수도 있고, 동일한 엔터티에 의해서 제공될 수도 있다. 따라서, SM-DP와 SM-SR의 기능을 명확하게 경계지을 필요가 있고, 이들 엔터티들 사이의 인터페이스를 정의할 필요가 있다.

[0067] SM-DP는 eUICC로 전달될 패키지 또는 프로파일의 안전한 준비를 담당하며, 실제 전송을 위하여 SM-SR과 함께 동작한다. SM-DP의 핵심 기능은 1) eUICC의 기능적 특성 및 인증 레벨(Certification Level)을 관리하는 것과, 2) MNO 크레덴셜 또는 프로파일(예를 들면, IMSI, K, 부가 서비스 어플리케이션, 부가 서비스 데이터 중 하나 이상이며, 이들 중 일부는 잠재적으로 MNO에 의하여 암호화(Enciphered)되어 있을 수 있음)을 관리하는 것과, 3) SM-SR에 의한 다운로드를 위하여 OTA 패키지를 계산하는 기능 등이며, 추후 부가적인 기능이 추가될 수 있을 것이다.

[0068] 만일, SM-DP 기능이 제3주체(Third party)에 의하여 제공되는 경우에는 보안과 신뢰 관계가 아주 중요해진다. SM-DP는 실시간 프로비지닝(Provisioning) 기능 이외에도 상당한 정도의 백그라운드 프로세싱 기능을 보유할 수 있으며, 퍼포먼스, 스케러빌러티(Scalability) 및 신뢰도에 대한 요구사항이 중요할 것으로 예상된다.

[0069] SM-SR은 크레덴셜 패키지를 해당되는 eUICC로 안전하게 라우팅하고 전달하는 역할을 담당한다. SM-SR의 핵심 기능은 1) 사이퍼(Ciphered)된 VPN을 통한 eUICC와의 OTA 통신을 관리하는 것과, 2) eUICC까지 엔드-투-엔드(end-to-end)를 형성하기 위하여 다른 SM-SR과의 통신을 관리하는 기능과, 3) eUICC 공급자에 의하여 제공되는 SM-SR OTA 통신을 위해 사용되는 eUICC 데이터를 관리하는 기능과, 4) 오직 허용된 엔터티만을 필터링함으로써 eUICC와의 통신을 보호하는 기능(방화벽 기능) 등이다.

[0070] SM-SR 데이터베이스는 eUICC 벤더와 상치(M2M 단말 등) 벤더 및 잠재적으로 MNO에 의하여 제공되며, SM-SR 메시 네트워크를 통해서 MNO에 의하여 사용될 수 있다.

[0071] 신뢰 서클(Circle of trust)은 프로비저닝 프로파일 전달 동안 엔드-투-엔드 시큐리티 링크를 가능하게 하며, SM-SR은 프로비저닝 프로파일의 안전한 라우팅 및 eUICC 디스커버리를 위하여 신뢰 서클을 공유한다. MNO는 신뢰 써클내의 SM-SR 및 SM-DP 엔터티와 링크될 수 있으며, 자체적으로 이런 기능을 제공할 수도 있을 것이다. 고객과 관련된 MNO의 계약상 및 법률상 의무를 어기지 않고, eUICC의 불법적인 사용(클로닝, 크레덴셜의 불법 사용, 서비스 거부, 불법적인 MNO 컨텍스트 변경 등)을 방지하기 위하여, eUICC와 MNO 크레덴셜 사이의 안전한 엔드-투-엔드 링크가 필요하다.

[0072] 즉, 도 1에서 110은 SM들 끼리, 더 구체적으로는 SM-SR 멤버 사이에 형성되는 신뢰 서클을 나타내고, 120은 MNO 파트너들의 신뢰 서클이며, 130은 엔드투엔드 신뢰 링크를 도시한다.

[0073] 도 2는 SM 분리 환경에서 SM-SR 및 SM-DP가 시스템에 위치하는 구성을 도시한다.

[0074] 도 2와 같이, SM은 eUICC와 관련된 여러 프로파일(MNO의 오퍼레이션 프로파일, 프로비저닝 프로파일 등)을 안전하게 준비하는 SM-DP와, 그를 라우팅하기 위한 SM-SR로 구분되며, SM-SR은 다른 여러 SM-SR과 신뢰관계로 연동될 수 있고, SM-DP는 MNO 시스템에 연동되어 있다.

[0075] 물론, SM-DP와 MNO 시스템의 배치는 도 2와 다르게 구현될 수 있다. (즉, SM-DP가 SM-SR과 연동되고, MNO 시스템이 SM-DP와 연동될 수 있다)

[0076] 이러한 eUICC 시스템 아키텍처 하에서, 본 발명의 일 실시예에 의한 eUICC는 각종 프로파일(프로비저닝 프로파일, 오퍼레이션 프로파일 등)의 로딩을 위하여 무결성(Integrity), 비밀성(Confidentiality) 및 인증성(Authenticity)을 보장할 수 있는 메커니즘을 포함할 수 있다. 이러한 메커니즘의 일 예로서 아래 도 4 이하에

Petitioner Samsung Ex-1038, 0284

서 설명할 바와 같이 프로파일 접근 크레덴셜인 eUICC의 공개키 및 비밀키를 이용한 암/복호화 메커니즘 및 선택적으로 SM의 공개키 및 비밀키를 이용한 전자서명을 포함할 수 있다.

[0077] 즉, 무결성, 비밀성 및 인증성을 보장할 수 있는 안전한 메커니즘에 의하여 eUICC 아키텍처 내에서 각종 프로파일이 아주 안전하게 보호되어야 하며, 따라서 프로파일이 eUICC 내로 전송(제조 단계에서 프로비저닝되는 것이 아닌)되기 때문에 그러한 프로파일을 보호하기 위한 아주 안전한 메커니즘이 필요하다.

[0078] 본 발명의 일 실시예에 의한 eUICC는 eUICC내에서 프로파일 접근 크레덴셜을 이용하여 각종 프로파일(프로비저닝 프로파일, 오퍼레이션 프로파일 등)을 관리 또는 핸들링할 수 있다.

[0079] 더 구체적으로 설명하면, 본 발명에서는 eUICC에서 엔드 포인트(End point; 예를 들면 Subscription Manager)로부터 전송되는 각종 프로파일(프로비저닝 프로파일, 오퍼레이션 프로파일 등)을 안전하게 프로비저닝 하기 위한 프로파일 접근 크레덴셜(예를 들면, eUICC의 공개키 등)을 최소한 1개 세트 이상 보유하며, 아래 실시예에서 설명할 바와 같이, 외부 엔터티로부터 전송된 암호화된 프로파일을 상기 프로파일 접근 크레덴셜을 이용하여 복호할 수 있다.

[0080] 또한, 본 발명의 일 실시예에서는 eUICC 내에는 오직 1개의 활성화 프로파일(Active Profile)만이 존재하는 것이 바람직하며, 프로파일 또는 프로파일 관리 데이터(Profile management data)는 그 프로파일 또는 프로파일 관리 데이터를 소유하는 오퍼레이터 시스템과 신뢰성 있게 연결된 엔드 포인트와 eUICC 사이에서 안전하게 전송되어야 할 뿐 아니라, 프로파일 또는 프로파일 관리 데이터는 단말 또는 터미널과 같은 외부 엔터티에 의해서 접근이 불가능해야 한다. 그를 위하여, 본 발명의 일 실시예에서는 아래 프로파일 또는 프로파일 관리 데이터를 암/복호화할 수 있는 프로파일 접근 크레덴셜로서 eUICC 공개키를 이용하는 방식을 포함한다.

[0081] 도 3은 본 발명이 적용되는 시스템에서 제1차 가입에 해당되는 프로비저닝 과정의 전체 흐름도이다.

[0082] 프로비저닝 과정에서, eUICC는 기기 식별 정보 (IMEI 등)와 eUICC 식별 정보 (eICCid 등)를 포함하는 활성화 요청을 MNO로 전송한다.(Request activation; S310) 그런 다음, S320단계에서 MNO와 eUICC 사이에는 eUICC 상태 요청 및 기술적 능력 제어 요청/확인이 수행된다.(eUICC status request 및 technical capability control; S320)

[0083] 또한, 도시하지는 않았지만, 상기 S320 단계에서는 아래에서 설명할 바와 같이, eUICC가 자신의 공개키(PK) 또는 프로파일 접근 크레덴셜 정보인 PKI 키정보(키 생성 알고리즘, 키 길이, 키 생성 방식 등)를 해당 MNO 시스템 또는 SM-SR로 제공하는 과정이 포함될 수 있다.

[0084] S330단계에서 MNO는 SM-SR과 사이에서 eUICC 아이덴터티 검증과, 상치(eUICC)에 대한 정보를 수집한다(eUICC identity verification 및 collect information about device). S330단계에서, MNO는 본 발명의 일 실시예에 의하여 해당 eUICC에 대한 암호화 키, 구체적으로는 eUICC에 대응되는 공개키를 SM-SR로부터 획득할 수 있다.

[0085] 이러한 공개키의 획득은 정적(static) 또는 동적(Dynamic)으로 이루어질 수 있는바, 정적으로 이루어지는 경우 eUICC 제조시에 이미 해당 eUICC 내부적으로, 세부적으로는 eUICC 내의 암호 연산 프로세서 (CCP 등)를 통해 공개키와 비밀키가 생성되어 eUICC에는 비밀키가 저장되고, 공개키는 모든 SM-SR이 공유함으로써 특정한 eUICC에 대한 공개키를 인식할 수 있도록 하고, MNO로부터 요청이 있는 경우 SM-SR은 해당되는 eUICC에 대한 공개키를 MNO로 전달하는 방식이다.

[0086] 동적인 암호키 획득방법은 아래에서 도 8 및 도 9와 관련하여 설명할 바와 같이, MNO로부터 요청(특정 eUICC 식별정보 포함)이 있는 경우, SM-SR은 해당되는 eUICC에게 공개키 전송을 요청하고, 해당 eUICC는 eUICC 탑재 단말 내의 발급 처리 모듈(이 용어에 한정되지 않으며, 통신모듈, 프로비저닝 모듈, 발급 모듈, 개통 모듈 등으로 칭할 수 있으며, eUICC 프로비저닝을 위한 eUICC 탑재 단말 외부와의 통신 및 프로비저닝 관리의 역할을 수행함) 또는 eUICC 내의 보안모듈(암호키 생성 모듈, 암호키 처리 모듈, Security Policy 모듈, Credential Manager, Profile Manager 등 eUICC 내의 암호키 생성 및 암호키를 활용한 보안 연산을 수행하는 모듈)을 이용하여 공개키를 생성한 후 SM-SR로 전달하는 방식으로 수행될 수 있다. 이에 대해서는 아래에서 더 상세하게 설명한다.

[0087] 여기서, eUICC 내에 탑재되는 보안모듈은 eUICC 제작 단계 또는 그 이후 eUICC 정책에 따라 eUICC 내에 공통적으로 1개가 설치될 수 있으며, eUICC 정책 및 각 MNO 정책에 따라 각 MNO 별로 여러 개가 설치될 수 있다.

[0088] 해당 eUICC의 공개키(암호키)를 획득한 MNO는 SM-DP를 통해서 MNO에 맞는 새로운 eUICC 프로파일을 생성하고 그 프로파일을 획득한 eUICC 공개키(암호키)로 암호화한 후 MNO로 전달한다.(1차 암호화, S340 단계) 이때, 인증성

Petitioner Samsung Ex-1038, 0285

(Authenticity)을 제공하기 위해 SM-DP는 자신의 개인키로 추가적인 전자서명을 생성할 수 있다. 즉, S340 단계에서 SM-DP는 인증을 위한 자신의 개인키 또는 비밀키로 프로파일을 전자서명(Sign)할 수 있다.

[0089] 다음으로, MNO는 1차 암호화된 (eUICC) 프로파일을 SM-SR로 전달한 후 2차 암호화를 요청하면, SM-SR은 이미 저장하고 있는 eUICC 관리키(eUICC OTA 키, GP ISD 키 등)를 이용하여 eUICC 프로파일을 2차 암호화하여 MNO로 전달한다.(S350 단계)

[0090] 그런 다음, MNO는 이중 암호화(Double Ciphered)된 eUICC 프로파일을 해당 eUICC로 전송한다.(S360 단계) 이때, 인증성을 제공하기 위해 SM-DP의 공개키 또는 인증서(Certification)를 함께 eUICC로 전송할 수 있다.

[0091] eUICC는 이미 eUICC 관리키를 알고 있으므로 1차로 복호화한 후, 자신 공개키에 대응되는 비밀키(제조 또는 공개키 동적 생성 단계에서 이미 알고 있음)를 이용하여 2차 복호화함으로써 프로비저닝에 사용될 프로파일을 완전히 복호화 할 수 있다. 이때, eUICC는 인증서 확인 (MNO로부터 획득한 공개키에 해당되는 SM-DP로부터 생성된 eUICC 프로파일인지 확인하기 위해)을 위해 SM-DP의 공개키 (인증서의 경우, 신뢰할 수 있는 제 3의 개체로부터 해당 인증서의 유효성을 검증 받을 수 있음)로 서명 검증을 수행할 수 있다.

[0092] S370 단계에서는 프로비저닝을 종료한 eUICC와 SM-SR 사이에서 상태 요청과 그에 대한 응답에 의하여 SM-SR 데이터베이스를 업데이트 한다.

[0093] 이러한 각 단계에 대한 주요 구성을 추가로 설명하면 다음과 같다.

[0094] S310단계에서, eUICC 식별 정보(eICCid 등)는 공개된 데이터이며 eUICC 내부에 통합 보호되어야 한다.

[0095] S320, S330단계에서 상태 요청 및 기술적 가능성 제어는 eUICC 아이덴터티의 증명을 제공(신뢰할 수 있는 eUICC)하며, MNO 서비스를 위한 eUICC 특성의 적격성을 확인할 수 있어야 한다.

[0096] S340~S360 단계에서는 eUICC 프로파일 생성 및 전송을 위하여 이중 암호화 메커니즘이 사용된다. 즉, SM-DP에 의하여 eUICC에 링크된 생성 프로파일은 오직 목표 eUICC에 의해서만 읽힐 수 있는 암호화 메커니즘에 의하여 암호화되며, 정당한 SM-DP로부터 생성된 프로파일임을 확인하기 위해 SM-DP에 의해 전자서명이 수행될 수 있고, SM-SR은 생성 프로파일을 eUICC 관리키로 암호화하여 전달 동안 eUICC를 인증하고 보호한다.

[0097] S370 단계에서, SM-SR 데이터베이스는 가입 설치(Subscription installation)의 마무리 단계에서 업데이트 될 수 있다.

[0098] 도 4는 본 발명이 적용되는 가입 변경 또는 MNO 변경 과정의 전체 흐름도이다.

[0099] 전체적으로는 도 3의 프로비저닝 과정과 유사(즉, 변경 후 새로운 MNO가 도 3의 MNO에 해당)하며, 다만 새로운 MNO에 대한 프로파일 생성 전후에 새로운 MNO가 도너 MNO에게 협상 및 권리 전송 과정을 수행하는 점이 상이하다.(단계 S440')

[0100] 즉, 도 4의 MNO 변경과정과 도 3의 프로비저닝 과정을 차이점은, 프로비저닝 또는 오퍼레이션 액티브 프로파일을 이용하여, 액티베이션 요청이 도너 MNO OTA 베어러(Bearer)로 전송되고, 새로운 MNO는 OTA 또는 OTI 중 하나로 새로운 프로파일을 다운로드 하도록 SM-SR로부터 정보를 요청하는 것이다.

[0101] 도 4에 의한 MNO 변경 과정을 구체적으로 설명하면 다음과 같다.

[0102] MNO 변경을 위하여, eUICC는 기기 식별 정보 (IMEI 등)와 eUICC 식별 정보 (eICCid 등)를 포함하는 활성화 요청을 변경될 MNO(Receiving MNO)로 전송한다.(Request activation; S410) 그런 다음, S420단계에서 리시빙 MNO와 eUICC 사이에는 eUICC 상태 요청 및 기술적 능력 제어 요청/확인이 수행된다.(eUICC status request 및 technical capability control; S420)

[0103] 또한, 도시하지는 않았지만, 상기 S420 단계에서는 아래에서 설명할 바와 같이, eUICC가 자신의 공개키(PK) 또는 프로파일 접근 크레덴셜 정보인 PKI 키정보(키 생성 알고리즘, 키 길이, 키 생성 방식 등)를 해당 MNO 시스템 또는 SM-SR로 제공하는 과정이 포함될 수 있음은 프로비저닝 과정인 S320과 동일하다.

[0104] S430단계에서 리시빙 MNO는 SM-SR과 사이에서 eUICC 아이덴터티 검증과, 장치(eUICC)에 대한 정보를 수집한다 (eUICC identity verification 및 collect information about device). S430단계에서, MNO는 본 발명의 일 실시예에 의하여 해당 eUICC에 대한 암호화 키, 구체적으로는 eUICC에 대응되는 공개키를 SM-SR로부터 획득할 수 있다.

[0105] 이러한 공개키의 획득은 정적(static) 또는 동적(Dynamic)으로 이루어질 수 있는바, 정적으로 이루어지는 경우

Petitioner Samsung Ex-1038, 0286

eUICC 제조시에 이미 해당 eUICC 내부적으로, 세부적으로는 eUICC 내의 암호 연산 프로세서 (CCP 등)를 통해 공개키와 비밀키가 생성되어 eUICC에는 비밀키가 저장되고, 공개키는 모든 SM-SR이 공유함으로써 특정한 eUICC에 대한 공개키를 인식할 수 있도록 하고, MNO로부터 요청이 있는 경우 SM-SR은 해당되는 eUICC에 대한 공개키를 MNO로 전달하는 방식이다.

[0106] 동적인 암호키 획득방법은 아래에서 도 8 및 도 9와 관련하여 설명할 바와 같이, MNO로부터 요청(특정 eUICC 식별정보 포함)이 있는 경우, SM-SR은 해당되는 eUICC에게 공개키 전송을 요청하고, 해당 eUICC는 eUICC 탑재 단말 내의 발급 처리 모듈(이 용어에 한정되지 않으며, 통신모듈, 프로비저닝 모듈, 발급 모듈, 개통 모듈 등으로 칭할 수 있으며, eUICC 프로비저닝을 위한 eUICC 탑재 단말 외부와의 통신 및 프로비저닝 관리의 역할을 수행함) 또는 eUICC 내의 보안모듈(암호키 생성 모듈, 암호키 처리 모듈, Security Policy 모듈, Credential Manager, Profile Manager 등 eUICC 내의 암호키 생성 및 암호키를 활용한 보안 연산을 수행하는 모듈)을 이용하여 공개키를 생성한 후 SM-SR로 전달하는 방식으로 수행될 수 있다. 이에 대해서는 아래에서 더 상세하게 설명한다.

[0107] 여기서, eUICC 내에 탑재되는 보안모듈은 eUICC 제작 단계 또는 그 이후 eUICC 정책에 따라 eUICC 내에 공통적으로 1개가 실치될 수 있으며, eUICC 정책 및 각 MNO 정책에 따라 각 MNO 별로 여러 개가 실치될 수 있다.

[0108] 해당 eUICC의 공개키(암호키)를 획득한 리시빙 MNO는 SM-DP를 통해서 MNO에 맞는 새로운 eUICC 프로파일을 생성하고 그 프로파일을 획득한 eUICC 공개키(암호키)로 암호화한 후 MNO로 전달한다.(1차 암호화, S440 단계) 이때, 인증성(Authenticity)을 제공하기 위해 SM-DP는 자신의 개인키로 추가적인 전자서명을 생성할 수 있다. 즉, S440 단계에서 SM-DP는 인증을 위한 자신의 개인키 또는 비밀키로 프로파일을 전자서명(Sign)할 수 있다.

[0109] 또한, S440 단계 이전 또는 이후에 협상 및 권리 전송 단계(S440')가 수행될 수 있다. 이러한 협상 및 권리 전송 단계(S440')는 새로운 리시빙 MNO가 이전 MNO(도너 MNO)에게 해당 eUICC가 정당한지 여부와, MNO 변경에 따른 권리(정보)를 이전해 줄 것을 요청하는 등의 과정이다.

[0110] 즉, S440' 단계에서는 새로운 MNO(Receiving MNO)가 가입 스위칭에 대해서 도너 MNO의 인증을 요청하며, 이러한 인증은 정책 제어 기능(Policy Control Function)에 의해서 제공될 수 있다.

[0111] 다음으로, 리시빙 MNO는 1차 암호화된 (eUICC) 프로파일을 SM-SR로 전달한 후 2차 암호화를 요청하면, SM-SR은 이미 저장하고 있는 eUICC 관리키(eUICC OTA 키, GP ISD 키 등)를 이용하여 eUICC 프로파일을 2차 암호화하여 MNO로 전달한다.(S450 단계)

[0112] 그런 다음, MNO는 이중 암호화(Double Ciphered)된 eUICC 프로파일을 해당 eUICC로 전송한다.(S460 단계) 이때, 인증성을 제공하기 위해 SM-DP의 공개키 또는 인증서(Certification)를 함께 eUICC로 전송할 수 있다.

[0113] eUICC는 이미 eUICC 관리키를 알고 있으므로 1차로 복호화한 후, 자신 공개키에 대응되는 비밀키(제조 또는 공개키 동적 생성 단계에서 이미 알고 있음)를 이용하여 2차 복호화함으로써 MNO 변경에 사용될 프로파일을 완전히 복호화 할 수 있다. 이때, eUICC는 인증서 확인 (MNO로부터 획득한 공개키에 해당되는 SM-DP로부터 생성된 eUICC 프로파일인지 확인하기 위해)을 위해 SM-DP의 공개키 (인증서의 경우, 신뢰할 수 있는 제 3의 개체로부터 해당 인증서의 유효성을 검증 받을 수 있음)로 서명 검증을 수행할 수 있다.

[0114] S470 단계에서는 프로비저닝을 종료한 eUICC와 SM-SR 사이에서 상태 요청과 그에 대한 응답에 의하여 SM-SR 데이터베이스를 업데이트 한다.

[0115] 이러한 GSMA에서 제안한 SM 역할 분리 환경은 SM에게 모든 사업적 주도권을 뺏길 수 있는 eSIM 환경에서 적절한 유연성 (모든 MNO가 각 MNO와 연동해야 하는 부분을 SM-SR을 통해 해결함)과 함께 사업주도권 확보 (SM-DP 역할은 일반적으로 MNO가 수행하게 될 것으로 보이며, SM-DP를 통해 통신 및 부가 서비스의 사업자 정보가 빌드됨)를 동반할 수 있는 이점이 있다. 하지만 이 구조를 기반으로 세부적인 eSIM 관리 방안이 존재하지 않음으로써 각 사업자 정보의 안전성 확보, eSIM 시스템 도입 시 발급 흐름 정의 등의 어려움이 존재한다.

[0116] 이에 본 발명에서는 통신사업자(MNO) 시스템, 가입 관리시스템(SM)과 연동되어 있는 eUICC가 eUICC를 포함하는 단말 또는 터미널이 접근할 수 없도록, MNO 또는 SM으로부터 수신한 프로파일 정보를 관리하기 위한 프로파일 접근 크레덴셜 정보(eUICC의 공개키 및 비밀키 등)를 포함하며, 그러한 프로파일 접근 크레덴셜 정보를 이용하여 수신된 프로파일 정보를 처리(복호화 등)하는 구조를 제안한다.

[0117] 이하에서는 본 발명의 일 실시예에 대해서 설명하며, GSMA에서 제안한 SM 역할 분리 환경과, 상기 프로파일 접근 크레덴셜의 일 예로서 eUICC의 공개키 및 그에 대응되는 비밀키를 대표하여 설명하지만 그에 한정되는 것은

Petitioner Samsung Ex-1038, 0287

아니다.

[0118] 또한, 아래에서는 처리 또는 관리되는 프로파일 정보로서 사업자 정보 또는 오퍼레이션 프로파일 또는 프로비저닝 프로파일 중 하나를 예시적으로 설명하지만, 그에 한정되는 것은 아니며, eUICC가 인증성을 보장해야 하는 모든 정보에 적용될 수 있을 것이다.

[0119] 이하에서는 크게 프로파일 접근 크레덴셜인 동적 공개 키 생성을 활용하여 eSIM을 안전하게 관리 방안으로서, 세부적으로 기본 개통 구조, 타사 이동 구조 및 프로세스의 방안으로 나누어 설명한다.

[0120] 본 발명의 기본적인 상위 구조는 도 1의 eSIM 구조를 근간으로 한다. 본 명세서에서 그림 상에 명시된 SM은 단일 SM 개체이거나 "Circle of Trust" 의 SM 개체들일 수 있다.

[0121] 도 5는 본 발명의 일 실시예에 의한 eUICC 또는 eSIM의 내부 구조를 도시한다.

[0122] 본 발명의 일실시예에 의한 eUICC(520)는 장치 또는 단말(device or Terminal; 510) 내에 착탈 불가능하게 포함되며, eUICC 내부에는 가장 하위 레벨의 칩 OS(COS; 521)과, 그 상위 레벨의 SIM 플랫폼(522), 그 상위 레벨의 SIM 서비스 관리 플랫폼(523) 등을 포함하며, COS 상위에는 각종 통신 또는 부가 M2M 서비스를 위한 프로비저닝 프로파일(524)이 존재한다.

[0123] 또한, SIM 서비스 관리모듈(523) 상에는 각 사업자별 사업자 정보(525) 또는 오퍼레이션 프로파일과, 그에 대응되는 보안모듈(526)이 포함될 수 있다.

[0124] 오퍼레이션 프로파일 및 보안모듈은 각 사업자 또는 MNO별로 달리 포함될 수 있으나, 특정 시점에는 단지 1개의 오퍼레이션 프로파일만이 활성화(Active)되는 것이 바람직하다.

[0125] 또한, 단말(510) 내에는 eUICC와 연동되는 발급 처리모듈(511)이 포함될 수 있으며, 이러한 발급처리모듈은 eSIM과 SM 간의 발급에 필요한 통신 및 필요 프로세스들을 처리하는 모듈로서 소프트웨어 형태로 구현될 수 있다. 이러한 발급처리모듈의 기능은 아래 도 8 및 9를 참조하여 더 상세하게 설명한다.

[0126] 다시 도 5에 의한 구조를 설명하면, 본 발명이 적용되는 전체 시스템은 프로비저닝 프로파일(Provisioning Profile; 524)을 포함하는 eUICC(520), eUICC가 탑재된 기기 (Device; 510), eUICC와 SM 간의 발급에 필요한 통신 및 필요 프로세스들을 처리하는 "발급처리모듈(511)" 그리고 SM-SR, MNO 및 SM-DP 등을 포함하는 "eUICC 인프라(도 4의 우측부분)"로 구성될 수 있다.

[0127] "발급처리모듈(511)"은 기기(Device) 내에 존재하는 소프트웨어로 "eUICC 인프라"와 통신하여 eUICC 관련 발급 과정을 수행한다. 이 과정에서 "발급처리모듈"은 "eUICC 인프라"와 TLS/SSL 등의 보안 통신을 수행할 수 있으며, 해당 소프트웨어 모듈은 기기 내의 안전한 공간에 위치하고 동작하여 외부 해킹으로부터 보호되어야 한다.

[0128] "eUICC" 내부에는 프로비저닝 프로파일(Provisioning Profile; 524)이 존재하여, 발급 처리가 필요할 경우, 모든 MNO들은 해당 프로비저닝 프로파일을 토대로 eUICC 탑재 기기와 "eUICC 인프라" 간의 통신이 가능해야 한다. 또한, "eUICC" 내부에는 SM-SR에서 관리하는 eUICC 관리키 -예를 들면, UICC OTA 키(Key), GP(global Platform) ISD(Issuer Security Domain) 키 등을 포함하지만 그에 한정되지는 않음-와 연동하여 사업자정보(MNO Profile 또는 Operational Profile) 및 보안모듈(526)을 탑재/관리하는 SIM 서비스 관리 플랫폼(524)과 그 하부 SIM 플랫폼(523) 및 COS(521)가 존재한다.

[0129] 여기서, "보안모듈(526)"은 각 사업자별 PKI (Public Key Infrastructure) 방식- 예를 들면, RSA, ECC, DH 등-에 따른 공개키 및 개인키(비밀키) 쌍을 생성하는 역할을 수행하는 애플릿 등의 어플리케이션으로 각 사업자별로 존재할 수 있으며 또는 사업자 간에 공유되어 사용될 수 있다. "보안모듈(526)"은 키 쌍 생성 이외에 "발급처리모듈(511)" 또는 "SIM 서비스 관리 플랫폼(523)"과 연동하여 eUICC의 공개키로 암호화된 사업자 정보를 생성된 개인키(비밀키)로 복호화 하는 역할을 수행하며, 사업자의 개인키로 전자서명된 사업자 정보의 전자서명에 대한 검증을 수행한다.

[0130] 본 명세서에서의 발급 처리 모듈은 eUICC 프로비저닝을 위한 eUICC 탑재 단말 외부와의 통신 및 프로비저닝 관리의 역할을 수행하는 것으로서, 상기 용어에 한정되는 것은 아니며, 통신모듈, 프로비저닝 모듈, 발급 모듈, 개통 모듈 등 다른 용어로 표현될 수 있다.

[0131] 또한, eUICC 내의 보안모듈은 크레덴셜 관리, 프로파일 메니저 등 암호키 생성 및 암호키를 활용한 보안 연산을 수행하는 것으로서, 상기 용어에 한정되지 않으며 암호키 생성 모듈, 암호키 처리 모듈 등 기타 다른 용어로 표

Petitioner Samsung Ex-1038, 0288

현될 수 있다.

[0132] 도 6은 본 발명의 일 실시예에 의한 eUICC 또는 eSIM의 사업자 정보 설치 구조(발급처리 모듈 주도)를, 도 7은 SIM 서비스 관리 플랫폼 주도의 사업자 정보(MNO Profile) 설치 구조를 도시한다.

[0133] 도 6을 참조하면, 우선 본 발명의 일 실시예에 의한 eUICC 및 그를 탑재하는 단말은 외부 엔터티(예를 들면, SM-SR 등)로부터 이중 암호화된 프로파일(도 6 및 7에서는 사업자 정보 또는 오퍼레이션 프로파일을 예로 든다)를 수신한다.

[0134] 이러한 이중 암호화된 프로파일은 도 6의 오른쪽과 같이 1차적으로 해당 eUICC의 프로파일 접근 크레덴셜인 공개키(PKI)로 암호화된 후, 다시 eUICC 관리키와 같은 별도의 보안키로 암호화된 상태이다.

[0135] 이러한 이중 암호화된 프로파일을 수신하면, eUICC는 먼저 SIM 서비스 관리 플랫폼을 이용하여 이미 알고 있는 eUICC 관리키 또는 보안키로 1차 복호화한다(S610) 그러면, eUICC 공개키(PKI)로만 암호화된 프로파일 정보가 생성되고, SIM 서비스 관리 플랫폼은 그를 단말의 발급처리모듈로 전달하면서 PKI 복호화 요청을 전달한다(S620)

[0136] 발급처리모듈은 S620의 복호화 요청을 다시 eUICC 내의 해당되는 보안모듈로 전달하고, 보안모듈로부터 해당 PKI에 대응되는 비밀키 또는 개인키로 복호화한 최종 프로파일을 응답받는다(S630),

[0137] 그 후 발급처리모듈은 완전히 복호화된 사업자 정보를 SIM 서비스 관리 플랫폼으로 전달하여 설치한다(S640)

[0138] 이상의 도 6의 과정은 발급처리 모듈이 주도가 된 처리방식으로서, 반드시 이러한 방식에 한정되는 것은 아니며, 도 7과 같이 SIM 서비스 관리 모듈의 주도로 진행될 수도 있다.

[0139] 즉, 도 7에서와 같이, 단말은 외부 엔터티(예를 들면, SM-SR 등)로부터 이중 암호화된 프로파일(도 6 및 7에서는 사업자 정보 또는 오퍼레이션 프로파일을 예로 든다)를 수신한다.

[0140] 이러한 이중 암호화된 프로파일은 도 7의 오른쪽과 같이 1차적으로 해당 eUICC의 프로파일 접근 크레덴셜인 공개키(PKI)로 암호화된 후, 다시 eUICC 관리키와 같은 별도의 보안키로 암호화된 상태이다.

[0141] 이러한 이중 암호화된 프로파일을 수신하면, eUICC는 먼저 SIM 서비스 관리 플랫폼을 이용하여 이미 알고 있는 eUICC 관리키 또는 보안키로 1차 복호화한다(S710) 그러면, eUICC 공개키(PKI)로만 암호화된 프로파일 정보가 생성되고, SIM 서비스 관리 플랫폼은 그를 보안모듈로 직접 PKI 복호화 요청을 전달한다(S720)

[0142] 그런다음, SIM 서비스 관리 모듈은 보안모듈로부터 해당 PKI에 대응되는 비밀키 또는 개인키로 복호화한 최종 프로파일을 응답받아 설치한다(S730)

[0143] 즉, 기존의 "SIM 서비스 관리 플랫폼"과의 연동을 통한 데이터 발급은 eUICC 관리키 또는 보안키를 통해서만 이뤄지지만, 본 발명에서는 eUICC 관리키 또는 보안키를 통한 인증 및 복호화 후, 공개키로 암호화 되어 있는 사업자 정보를 각 사업자별로 eSIM에 설치된 "보안모듈"을 통해 다시 한번 복호화 하는 과정이 추가되어야 한다. 복호화를 "보안모듈"에 요청하는 주체는 도 6과 같이 "발급처리모듈"이 될 수 있으며, 도 7과 같이 "SIM 서비스 관리 플랫폼"이 될 수 있다. (안전성은 도 7의 경우가 더 높다.)

[0144] 도 8은 본 발명의 일 실시예에 의한 프로비저닝(초기 개통)과정의 흐름을 도시한다.

[0145] 본 발명에서 eSIM 또는 eUICC에는 모든 MNO (즉, 임의의 MNO) 네트워크를 통한 발급 수행을 위한 프로비저닝 프로파일이 선탑재(Pre-load)되어 있다. 또한, "eUICC에는 GSMA 제안 구조에 따라 각 eUICC을 식별하는 eUICC 식별정보-예를 들면 eICCID (ICCID 아님) 등-가 존재하며, 이를 통해 발급 전반에 걸쳐 각 eUICC을 식별하는 역할을 수행한다.

[0146] 본 발명에서의 초기 개통(First Subscription)은 eUICC에 선탑재된 프로비지닝 프로파일(Provisioning Profile)을 활용하여 다음과 같이 진행된다.

[0147] 우선 eUICC 탑재 기기는 "발급처리모듈"을 이용하여 프로비저닝 프로파일을 통해 eUICC 탑재 기기 식별정보 및 eUICC 식별 정보 (IMEI 및 eICCID 등)와 함께 개통 요청을 MNO에 전달한다.(S810) 이러한 개통 요청 과정은 활성화 요청(Request Activation) 과정으로 표현될 수도 있다.

[0148] 그러면, MNO는 eUICC 탑재 기기의 "발급처리모듈"과 프로비저닝 프로파일 을 통해 통신하여 eUICC 상태 및 지원 네트워크 및 부가 기능 (예, SIM 부가 서비스 가능 등) 정보를 획득한다. 이때, eUICC 내의 보안모듈 설치 여부도 함께 확인할 수 있으며, 보안모듈이 이미 설치된 경우에는 해당 eUICC의 공개키에 대한 정보 (PKI 키정

Petitioner Samsung Ex-1038, 0289

보; 알고리즘, 길이, 방식 등 포함 가능)를 획득할 수 있다(S820). 이러한 S820 단계는 eUICC 상태 요청 및 기술 성능 제어(eUICC status request & technical capa. Control) 과정으로 표현될 수 있다.

[0149] 다음으로, MNO는 SM-SR에 eUICC 식별 정보 (eICCID 등) 검증 및 보안모듈의 설치와 eUICC 에서 생성된 암호키(공개키 등) 전달을 요청한다(S830). 여기서, 보안모듈이 이미 설치된 경우 설치 과정은 생략될 수 있다.

[0150] 다음으로 S840 단계에서, SM-SR은 eUICC 관리키 또는 보안키를 활용하여 "발급처리모듈"을 통해 "SIM 서비스 관리 플랫폼"과 연동하여 eUICC 내에 보안모듈을 설치하고 eUICC의 보안모듈에 의해 생성된 암호키(공개키 등) 및 필요한 경우 암호키 정보 또는 공개키 정보(키 생성 알고리즘, 키 길이 등)를 전달 받는다. 여기서, 보안모듈이 이미 설치된 경우 설치 과정은 생략될 수 있다.

[0151] 다음으로, SM-SR은 MNO에게 eUICC에서 생성된 암호키(공개키 등), (필요한 경우 암호키 정보 (키 생성 알고리즘, 키 길이 등))와 기기 정보를 전달한다(S850).

[0152] MNO는 SM-DP에게 암호키(공개키 등), (필요한 경우 암호키 정보 (키 생성 알고리즘, 키 길이 등)) 및 eUICC 식별정보(eICCID 등)를 전달하고, SM-DP는 전달 받은 공개키로 해당 eUICC 식별 정보(eICCID 등)에 대한 사업자 정보 (통신 데이터, 부가 서비스 어플리케이션 및 부가 서비스 데이터 등)의 프로파일을 암호화하여 MNO에게 응답한다. 이때, 인증서 제공을 위해 SM-DP는 자신의 개인키로 전자서명을 수행할 수 있다.(S860)

[0153] 다음으로, MNO는 eUICC 공개키로 암호화된 사업자 정보가 eUICC에 탑재되기 위해 별도의 eUICC 관리키 또는 보안키로 암호화 해줄 것을 SM-SR에 요청하고, SM-SR은 eUICC 관리키 또는 보안키로 암호화(2차 암호화) 수행 후 이를 MNO에게 전달하고(S870), MNO는 SM-SR을 통해 기기 내에 사업자 정보를 발급한다(S880). 이때, 인증성을 제공할 경우, SM-DP의 공개키를 기기에게 전달할 수도 있을 것이다.

[0154] 마지막으로, SM-SR은 eUICC의 "발급처리모듈"과 통신하여 상태 및 DB 업데이트를 수행한다.(S890)

[0155] 상기 도 8의 S810 내지 S890 단계는 필요에 따라서 여러 단계가 하나로 통합 구현되거나 하나로 통합 표현될 수 있다.

[0156] 도 9는 본 발명의 일 실시예에 의한 MNO 변경 과정의 흐름을 도시한다.

[0157] 도 8과 같은 사업자 변경과정은, 아래와 같이 구성될 수 있다.

[0158] 우선 eUICC 탑재 기기는 "발급처리모듈"을 통해 eUICC 탑재 기기 및 eUICC 식별 정보 (IMEI 및 eICCID 등)와 함께 개통 요청을 리시빙 MNO인 MNO B에 프로비저닝 프로파일(Provisioning Profile)을 통해 전달한다.(S910)

[0159] 그러면, 리시빙 MNO B는 eUICC 탑재 기기의 "발급처리모듈"과 프로비저닝 프로파일 을 통해 통신하여 eUICC 상태(Status) 및 지원 네트워크 및 부가 기능 (예, SIM 부가 서비스 가능 등) 정보를 획득한다.(S920) 이때, eUICC 내의 보안모듈 설치 여부도 함께 획득하며, 보안모듈이 이미 설치된 경우에는 해당 eUICC의 공개키에 대한 정보, 즉 공개키 정보 (PKI 키정보; 알고리즘, 길이, 방식 등 포함 가능)를 획득할 수 있다.

[0160] 리시빙 MNO B는 전달 받은 정보들을 토대로 도너 MNO인 MNO A에게 사업자 변경에 대하여 통지(Notification)를 전달하고 그에 대한 응답값을 전달 받는다. 즉, 새로운 리시빙 MNO가 이전 MNO(도너 MNO)에게 해당 eUICC가 정당한지 여부와, MNO 변경에 따른 권리(정보)를 이전해 줄 것을 요청하는 등의 과정인 협상 및 권리 전송 단계가 수행될 수 있다.(S930)

[0161] 리시빙 MNO B는 SM-SR에 eUICC 식별 정보 (eICCID 등) 검증 및 보안모듈의 설치와 eUICC에서 생성된 암호키 (공개키 등) 전달을 요청한다. 여기서, 보안모듈이 이미 설치된 경우 설치 과정은 생략될 수 있다.(S940)

[0162] SM-SR은 상기 eUICC 공개키와 구분되는 별도의 eUICC 관리키 또는 보안키를 활용하여 "발급처리모듈"을 통해 "SIM 서비스 관리 플랫폼"과 연동하여 보안모듈을 설치하고 eSIM의 보안모듈에 의해 생성된 암호키(공개키 등) 및 필요한 경우 암호키 정보 (키 생성 알고리즘, 키 길이 등)를 전달 받는다.(S950) 여기서, 보안모듈이 이미 설치된 경우 설치 과정은 생략될 수 있다.

[0163] SM-SR은 리시빙 MNO에게 eUICC에서 생성된 암호키(공개키 등), (필요한 경우 암호키 정보 (키 생성 알고리즘, 키 길이 등))와 기기 정보를 전달한다.(S960)

[0164] 리시빙 MNO B는 SM-DP에게 암호키(공개키 등), (필요한 경우 암호키 정보 (키 생성 알고리즘, 키 길이 등)) 및 eUICC 식별정보(eICCID 등)를 전달하고, SM-DP는 전달 받은 공개키로 해당 eUICC 식별 정보(eICCID 등)에 대한 사업자 정보 (통신 데이터, 부가 서비스 어플리케이션 및 부가 서비스 데이터 등)를 암호화하여 MNO B에게 응답

Petitioner Samsung Ex-1038, 0290

Petitioner Samsung Ex-1038, 0291

한다. 이때, 인증서 제공을 위해 SM-DP는 자신의 개인키로 전자서명을 수행할 수 있다.(S970)

[0165] 다음으로, MNO B는 공개키로 암호화된 사업자 정보가 eUICC에 탑재되기 위해 eUICC 공개키와 구분되는 별도의 eUICC 관리키 또는 보안키로 암호화 해줄 것을 SM-SR에 요청하고, SM-SR은 eUICC 관리키로 암호화 수행 후 이를 MNO B에게 전달한다.(S980)

[0166] MNO B는 SM-SR을 통해 기기 내에 사업자 정보를 발급한다.(S990) 이때, 인증성을 제공할 경우, SM-DP의 공개키를 기기에게 전달할 수 있다.

[0167] 마지막으로, SM-SR은 eUICC의 "발급처리모듈"과 통신하여 상태 및 DB 업데이트를 수행한다.(S1000)

[0168] 상기 도 9의 S910 내지 S1000단계는 필요에 따라서 여러 단계가 하나로 통합 구현되거나 하나로 통합 표현될 수 있다.

[0169] 본 발명의 일 실시예를 이용하면, eUICC는 각종 프로파일(프로비저닝 프로파일, 오퍼레이션 프로파일 등)의 로딩을 위하여 무결성(Integrity), 비밀성(Confidentiality) 및 인증성(Authenticity)을 보장할 수 있다.

[0170] 또한, 무결성, 비밀성 및 인증성을 보장할 수 있는 안전한 메커니즘에 의하여 eUICC 아키텍처 내에서 각종 프로파일이 아주 안전하게 보호될 수 있으며, 따라서 프로파일이 eUICC 내로 전송(제조 단계에서 프로비저닝되는 것이 아닌)되기 때문에 그러한 프로파일을 보호하기 위한 아주 안전한 메커니즘을 제공할 수 있다.

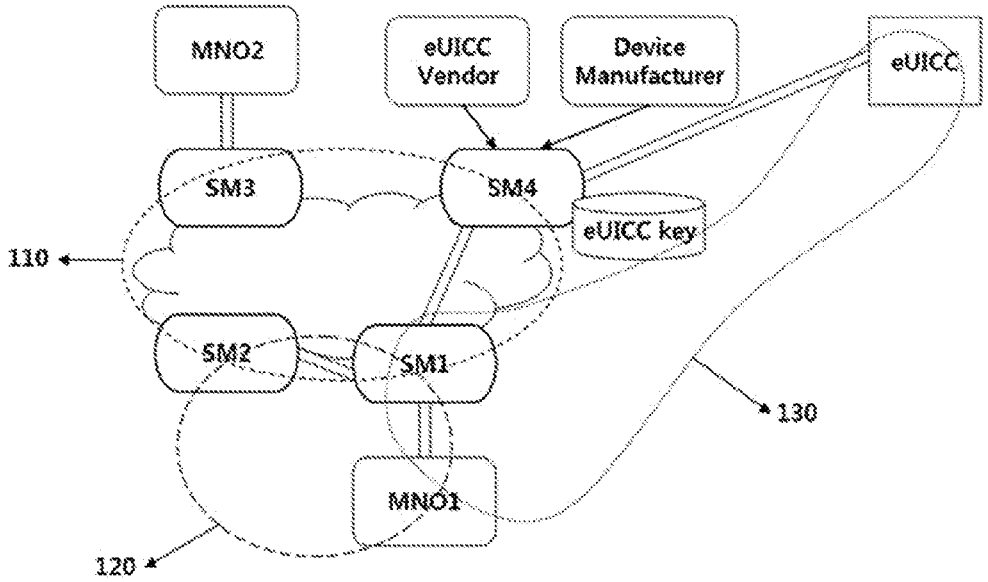
[0171] 또한, 프로파일 또는 프로파일 관리 데이터(Profile management data)는 그 프로파일 또는 프로파일 관리 데이터를 소유하는 오퍼레이터 시스템과 신뢰성 있게 연결된 엔드 포인트와 eUICC 사이에서 안전하게 전송되어야 할 뿐 아니라, 프로파일 또는 프로파일 관리 데이터는 단말 또는 터미널과 같은 외부 엔터티에 의해서 접근이 불가능하게 된다는 효과가 있다.

[0172] 특히, 본 발명의 일 실시예에 의하면, 고정된 공개키/개인키 쌍을 활용하는 것이 아니라 발급 시점마다 동적으로 공개키 및 개인키 쌍을 생성함으로써 사업자 정보의 eUICC 발급에 대한 안전성을 높일 수 있다. 또한, 기존 표준 기술들의 최소한의 변경을 통해 현실성 있는 eUICC 기반 발급 구조를 가져갈 수 있다.

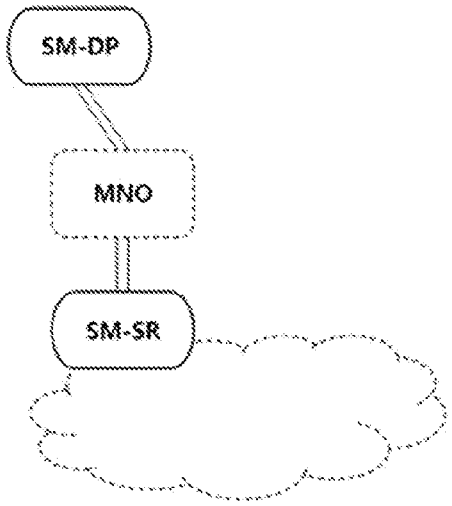
[0173] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 발명에 개시된 실시 예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시 예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

도면

도면1

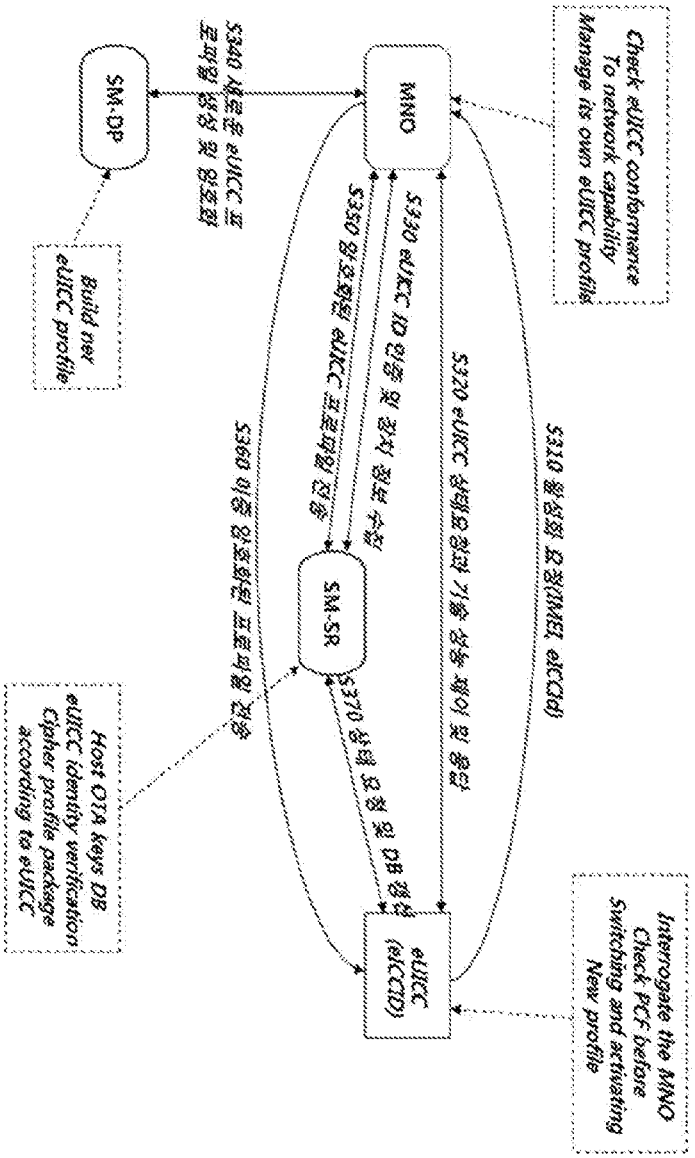


도면2



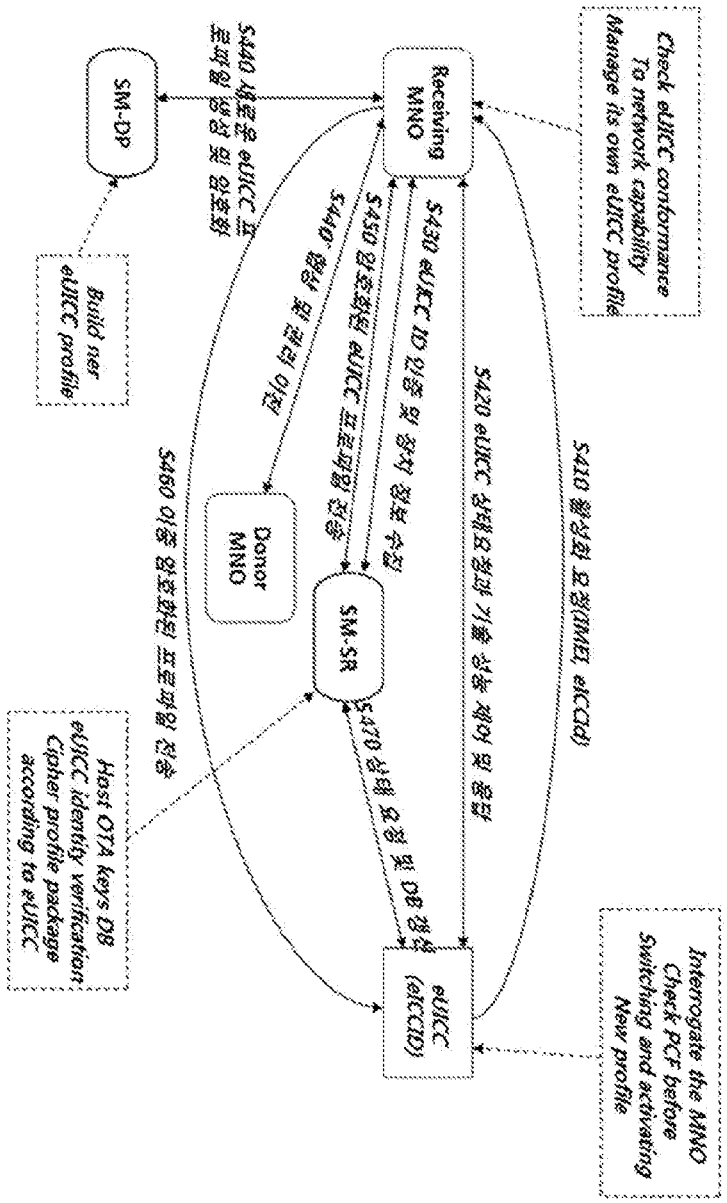
Petitioner Samsung Ex-1038, 0292

도면3



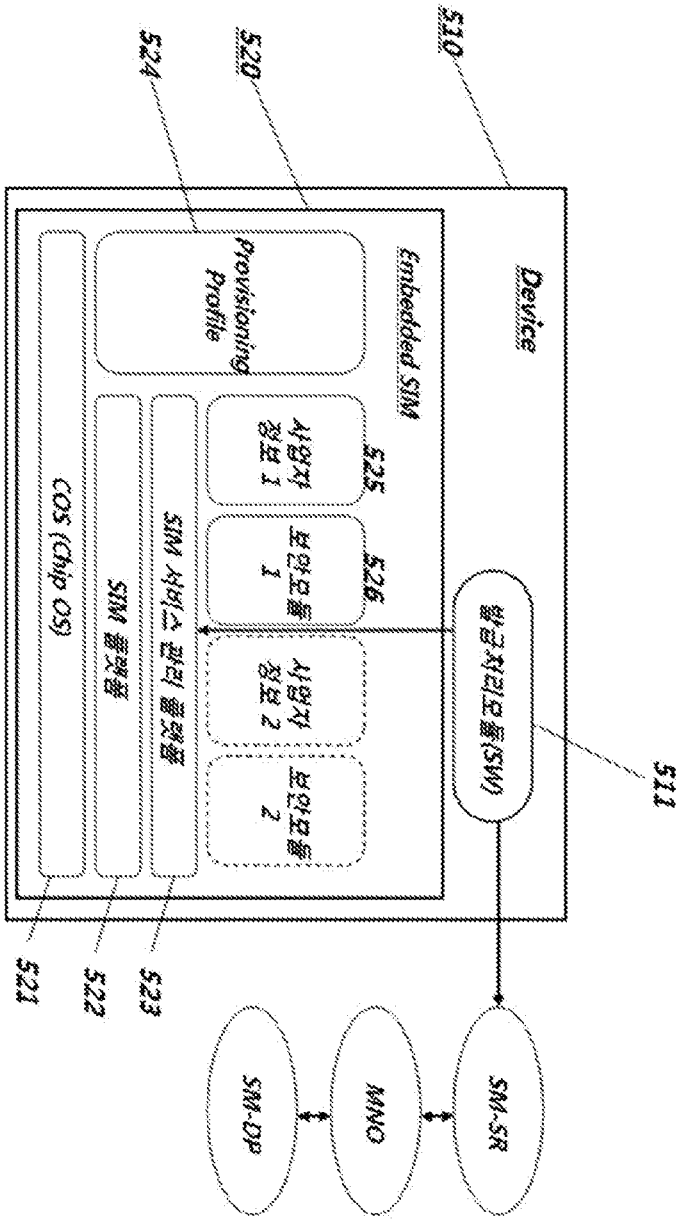
Petitioner Samsung Ex-1038, 0293

도면4



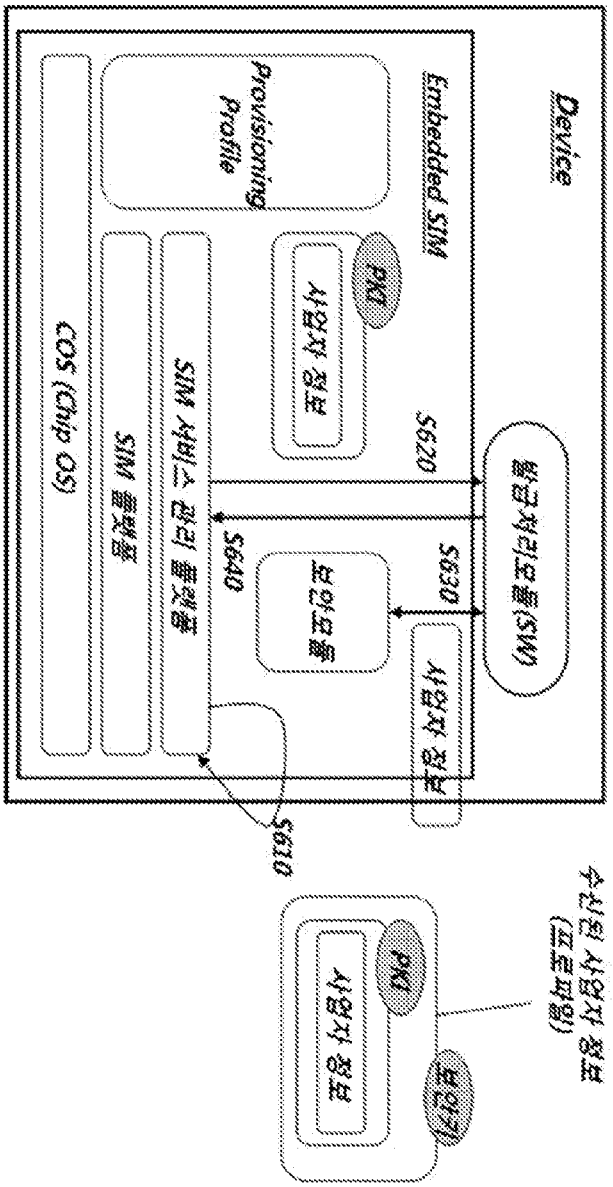
Petitioner Samsung Ex-1038, 0294

도면5



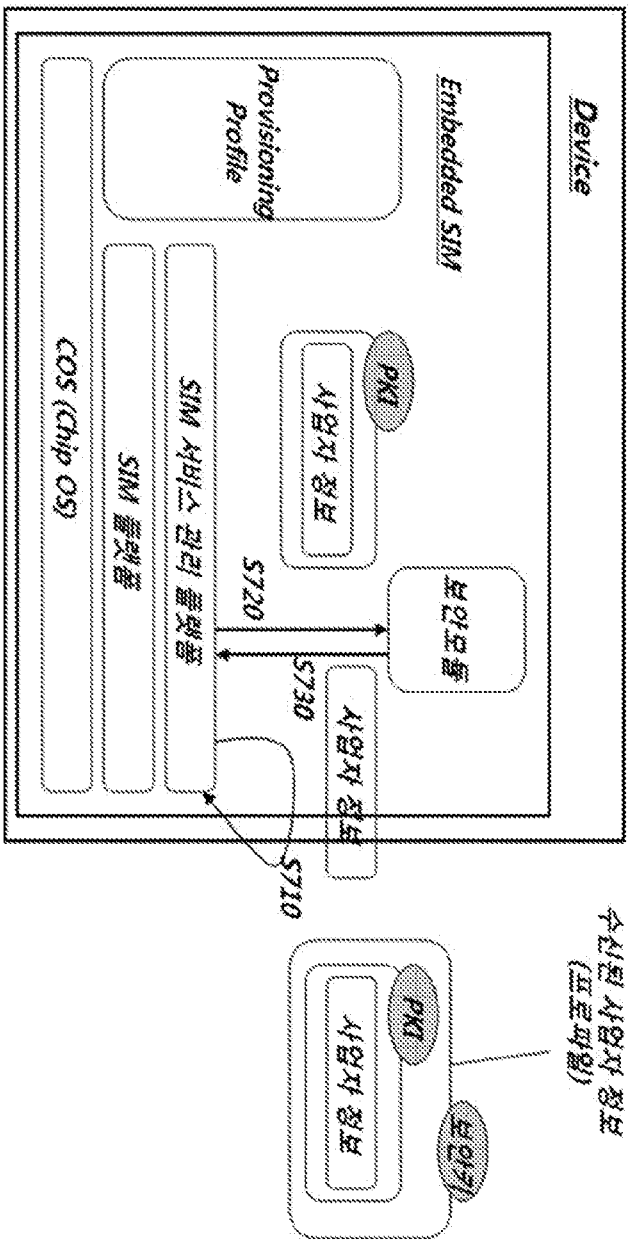
Petitioner Samsung Ex-1038, 0295

도면6



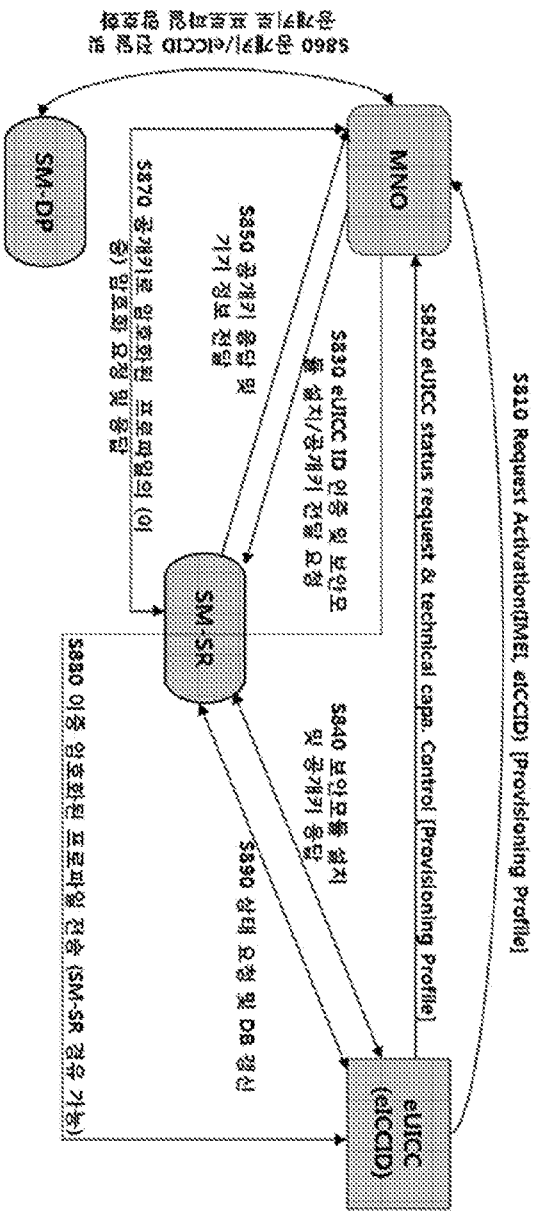
Petitioner Samsung Ex-1038, 0296

도면7



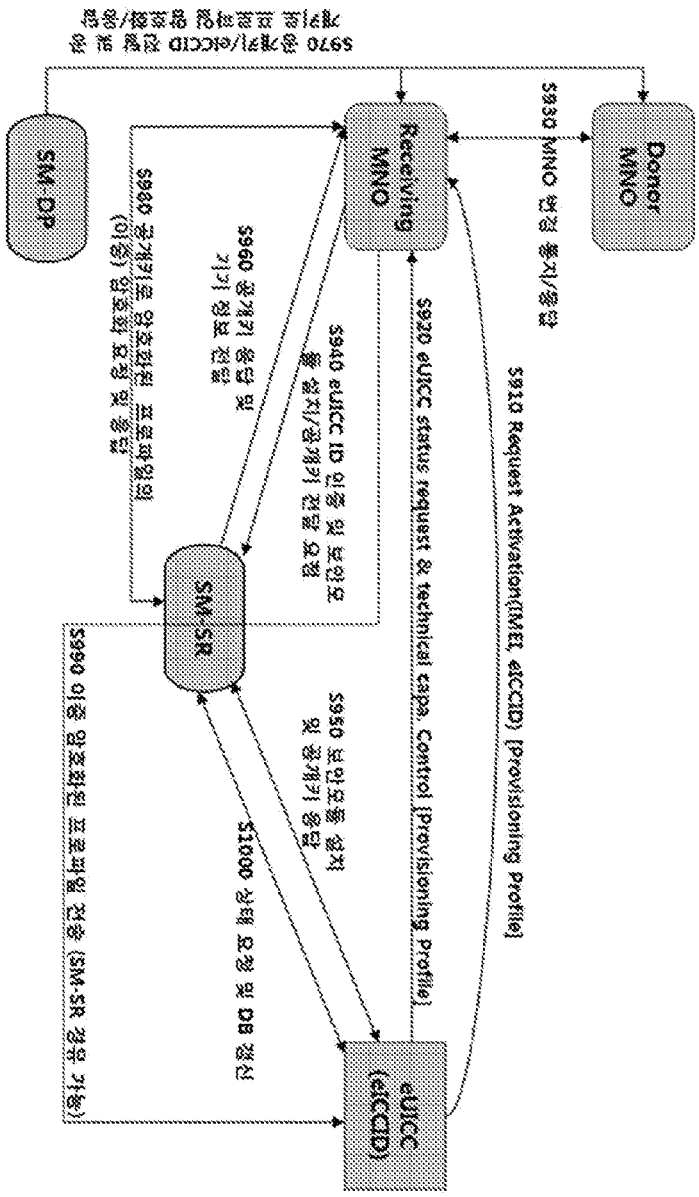
Petitioner Samsung Ex-1038, 0297

도면8



Petitioner Samsung Ex-1038, 0298

도면9



Petitioner Samsung Ex-1038, 0299

Espacenet

WO2013048084A2 PROFILE MANAGEMENT METHOD, EMBEDDED UICC, AND DEVICE PROVIDED WITH THE EMBEDDED UICC

Applicants: KT CORP [KR]

Inventors: PARK JAEMIN [KR]

Classifications:
IPC ***H04W4/50; H04W4/70;***

CPC **H04L67/30 (EP,US); H04L67/303 (US); H04L67/306 (US); H04L9/006 (EP,US); H04W12/04 (EP,US); H04W12/06 (US); H04W12/086 (US); H04W12/35 (EP,US); H04W12/42 (EP,US); H04W4/50 (EP,US); H04W4/70 (EP,US); H04W8/183 (US); H04W8/20 (US); H04W8/205 (EP,US);**

Priorities: KR20110097901A 2011-09-28

Application: KR2012007705W 2012-09-25

Publication: WO2013048084A2 2013-04-04

Published as: **KR20140086950A; US10341845B2; US10694369B2; US2014237101A1; US2017289792A1; US2019268756A1; US9712996B2;** WO2013048084A2;**WO2013048084A3**

PROFILE MANAGEMENT METHOD, EMBEDDED UICC, AND DEVICE PROVIDED WITH THE EMBEDDED UICC

Abstract

The present invention relates to a method for managing a profile in an embedded UICC, and more particularly, to a method for managing a profile in an embedded UICC that enables management information on the profile provided within the embedded UICC to play an essential role for providing communication and additional services, to be provided to a device existing outside the embedded UICC. The present invention also relates to an embedded UICC and to a device provided with the embedded UICC for the method.

Petitioner Samsung Ex-1038, 0300

WO2013048084A2 PROFILE MANAGEMENT METHOD, EMBEDDED UICC, AND DEVICE PROVIDED WITH THE EMBEDDED UICC

Data originating from sources other than the EPO may not be accurate, complete, or up to date.

The wording below is an initial machine translation of the original publication. To generate a version using the latest translation technology, go to the original language text and use Patent Translate.

A profile management method in an embedded UICC (eUICC) interworking with an MNO (Mobile Network Operator) and an SM (Subscription Manager)

And providing at least one of information about a type of a profile activated by the eUICC and information about a profile list to an external entity.

The method according to claim 1,

In the providing step, the eUICC includes:

Providing at least one of information about the type of the activated profile and information about the profile list to the external entity as management information necessary for using the profile, wherein at least one of the profile identification information and the profile description information is further provided as the management information Wherein the profile management method comprises the steps of:

3. The method of claim 2,

The management information includes:

The MNO, the SM, the MN, and the SM. & Lt; Desc / Clms Page number 13 &)

3. The method of claim 2,

The management information includes:

Wherein the management information is managed through the management profile in the eUICC.

5. The method of claim 4,

Before the providing step,

Wherein the management profile further comprises receiving a management information request from the external entity.

The method according to claim 1,

The external entity comprising:

The eUICC-equipped device on which the eUICC is mounted, the MNO, and the SM.

It is an embedded UICC (eUICC: embedded Universal Integrated Circuit Card) interworking with MNO (Mobile Network Operator) and SM (Subscription Manager)

Wherein the eUICC includes a management information providing module for providing at least one of information about a type of an activated profile and information about a profile list to an external entity.

8. The method of claim 7,

Wherein the management information providing module is the management profile in the eUICC.

9. The method of claim 8,

Petitioner Samsung Ex-1038, 0301

A network authentication module that provides the profile list to the eUICC-equipped device as the external entity and then performs network authentication with the MNO based on the profile selected from the profile list; And

And a management profile update module for updating the management profile based on the activated profile in cooperation with the MNO.

8. The method of claim 7,

Wherein the management information providing module comprises:

Providing at least one of information about the type of the activated profile and information about the profile list as management information necessary for using the profile as the external entity, wherein at least one of the profile identification information and the profile description information is further provided as the management information & Lt; / RTI &)

It is a device equipped with an embedded UICC (eUICC: embedded Universal Integrated Circuit Card) interworking with MNO (Mobile Network Operator) and SM (Subscription Manager)

And a management information acquisition unit for acquiring at least one of information about a type of the activated profile and information about the profile list from the eUICC.

12. The method of claim 11,

The management information obtaining unit obtains,

Acquiring at least one of information about a type of the activated profile and information about a profile list as management information necessary for using a profile,

Wherein the management information is managed through the management profile in the eUICC.

13. The method of claim 12,

A profile list display unit displaying the profile list;

A network authentication unit for performing network authentication with the MNO based on a profile selected from the profile list; And

And a management profile updating unit operable to update the management profile in association with the active profile in cooperation with the MNO.

A profile management method in an embedded UICC (eUICC) interworking with a MNO (Mobile Network Operator)

Performing network authentication with the eUICC-equipped device based on the profile selected by the NNO in the profile list provided by the eUICC; And

And the MNO updating the management profile managing the profile list in the eUICC based on the activated profile.

15. The method of claim 14,

When the MNO creates a new profile in the eUICC or deletes an existing profile, updates the management profile according to the profile status in the eUICC.

WO2013048084A2 PROFILE MANAGEMENT METHOD, EMBEDDED UICC, AND DEVICE PROVIDED WITH THE EMBEDDED UICC

Data originating from sources other than the EPO may not be accurate, complete, or up to date.

The wording below is an initial machine translation of the original publication. To generate a version using the latest translation technology, go to the original language text and use Patent Translate.

Profile management method, built-in UICC and built-in UICC equipped device

The present invention relates to a method of managing a profile in a built-in UICC and a built-in UICC and a built-in UICC-equipped device therefor. In particular, the present invention relates to a method for externally confirming and utilizing information on a profile in a built-in UICC.

A UICC (Universal Integrated Circuit Card) is a smart card inserted in a terminal and used as a module for user authentication. The UICC can store the user's personal information and the carrier information of the mobile communication carrier to which the user subscribes. For example, the UICC may include an International Mobile Subscriber Identity (IMSI) for identifying a user.

Such a UICC may also be referred to as a Subscriber Identity Module (SIM) card for Global System for Mobile communications (GSM) and a Universal Subscriber Identity Module (USIM) card for a Wideband Code Division Multiple Access (WCDMA) method.

When the user mounts the UICC on the user terminal, the user is automatically authenticated using the information stored in the UICC, so that the user can conveniently use the terminal. Also, when the user changes the terminal, the user can easily replace the terminal by attaching the UICC removed from the existing terminal to the new terminal.

When a terminal requiring miniaturization, for example, a machine to machine (Machine to Machine, M2M) communication, is manufactured with a detachable UICC structure, miniaturization of the terminal becomes difficult. Thus, a built-in UICC (Embedded UICC) structure, which is a non-removable UICC, has been proposed. The embedded UICC shall record the user information using the corresponding UICC in the form of IMSI.

The existing UICC can be attached to or detached from the terminal, and the user can open the terminal without being concerned with the type of terminal or the mobile communication provider. However, the IMSI in the built-in UICC can be allocated only when a terminal manufactured from the time of manufacturing the terminal is used only for a specific mobile communication provider. Both the mobile communication service provider and the terminal manufacturer ordering the terminal are forced to pay attention to the product inventory and the product price rises. The user is inconvenient that the mobile communication provider can not be changed for the terminal. Therefore, even in the case of the built-in UICC, there is a need for a method by which the user can open the terminal regardless of the mobile communication service provider.

Meanwhile, due to the introduction of the built-in UICC, it has become necessary to update the subscriber information of a plurality of mobile communication providers from a remote UICC, and accordingly, a subscription manager (hereinafter referred to as "SM") A Profile Manager (hereinafter referred to as & quot; PM & quot;) is being discussed.

In this way, unlike the existing detachable UICC, the built-in UICC (hereinafter referred to as "eSIM" or "eUICC"), which is integrated in the terminal, can not be opened due to its physical structure, There are many issues about. To this end, the GSMA and ETSI international standardization organizations are carrying out standardization activities for related companies such as operators, manufacturers, SIM vendors, and other necessary elements including the top-level structure.

In this way, as the eUICC is discussed through the standardization bodies, the issue at the center is issued to the eUICC with the profile (Operator Credential, Profile) as an SM called Subscription Manager and the process of the subscription change is processed Or function / role that performs the overall management role for the eUICC.

Petitioner Samsung Ex-1038, 0303

However, there is no way to provide management information such as profile type / identification information / list, which is necessary for providing communication and supplementary services, installed outside the eUICC outside the eUICC (for example, a terminal equipped with the eUICC) .

It is an object of the present invention to provide a profile method in an eUICC that enables management information on a profile, which is mounted in the eUICC and is essential for providing communication and additional services, to be provided outside the eUICC.

It is another object of the present invention to provide a method of using management information on profiles in the eUICC from the eUICC.

It is another object of the present invention to propose a management profile that efficiently manages management information on a profile in an eUICC and enables easy interoperation with an eUICC external entity (e.g., terminal, MNO, SM, etc.).

An embodiment of the present invention is a profile management method in an embedded UICC (eUICC) interworking with a Mobile Network Operator (MMNO) and a Subscription Manager (SM) And providing at least one of information on the profile list to an external entity.

Another embodiment of the present invention is an embedded Universal Integrated Circuit Card (eUICC) (eUICC) interworking with a Mobile Network Operator (MNO) and a Subscription Manager (SM) And an eUICC including a management information providing module for providing at least one of information on the external entity (External Entity).

Another embodiment of the present invention is a device including an Embedded Universal Integrated Circuit Card (eUICC) interworking with a Mobile Network Operator (MNO) and a Subscription Manager (SM) And an eUICC managing a profile in the eUICC including a management information obtaining unit for obtaining one or more pieces of information on the profile list from the eUICC.

According to another embodiment of the present invention, there is provided a profile management method in an embedded UICC (eUICC) interworking with a NO (Mobile Network Operator), wherein the NNO searches for a profile selected from a profile list provided in the eUICC, And performing network authentication with the device including the network; And updating the management profile in which the MNO manages the profile list in the eUICC, based on the activated profile.

1 illustrates an overall service architecture including an eSIM (eUICC) to which the present invention is applied.

Figure 2 illustrates the system architecture of an SM isolation environment to which the present invention may be applied.

3 is an overall flow diagram of a provisioning process in a service architecture to which the present invention is applied.

4 is an overall flowchart of a subscription change or MNO change process to which the present invention is applied.

5 is a diagram illustrating a basic structure of a profile management method according to an embodiment of the present invention.

6 is a block diagram of an apparatus including an eUICC according to an embodiment of the present invention.

7 is a block diagram of an eUICC according to an embodiment of the present invention.

FIG. 8 is a flowchart of an application method of a profile management method according to an embodiment of the present invention.

Hereinafter, some embodiments of the present invention will be described in detail with reference to exemplary drawings. It is to be noted that, in adding reference numerals to the constituent elements of the drawings, the same constituent elements are denoted by the same reference numerals even though they are shown in different

Petitioner Samsung Ex-1038, 0304

drawings. In the following description of the present invention, a detailed description of known functions and configurations incorporated herein will be omitted when it may make the subject matter of the present invention rather unclear.

Since the M2M (Machine-to-Machine) terminal actively discussed in GSMA should be small in size, if a UICC is used, a module for mounting a UICC must be separately inserted in the M2M terminal. Therefore, The miniaturization of the M2M terminal becomes difficult.

Therefore, an embedded UICC structure that can not be detached from the UICC is being discussed. In this case, information of a mobile network operator (MNO) using the corresponding UICC is transmitted to an euICC installed in the M2M terminal, And must be stored in the UICC in the form of an International Mobile Subscriber Identity (IMSI).

However, since the terminal manufactured from the manufacturing of the M2M terminal must be used only by the specific MNO, the IMSI in the eUICC can be allocated so that the MNO or the M2M maker that manufactures the M2M terminal or the UICC, And the price of the product is increased, which is a big obstacle to the expansion of the M2M terminal.

As described above, the built-in SIM (hereinafter referred to as & quot; eSIM & quot; or & quot; eUICC & quot;), which is integrally mounted on the terminal unlike the existing detachable SIM, There are many issues to be addressed. To this end, the GSMA and ETSI international standardization organizations have been carrying out standardization activities on related factors such as operators, manufacturers, SIM vendors and other necessary elements including top-level structure. As eSIM is discussed through standardization bodies, it is at the heart of the issue that SM issues an important profile (Operator Credential, MNO Credential, Profile, eUICC Profile, Profile Package, etc.) to eSIM, Or function / role that performs the overall management role for the eSIM.

In recent GSMA, the role of SM has been proposed as SM-DP (Data Preparation), which plays a role of creating provider information, and SM-SR (Secure Routing), which carries direct carrier information to eSIM. And does not mention the actual method of issuing technical information.

Accordingly, the present invention proposes a method of managing eSIM by utilizing dynamic encryption key (public key, etc.) generation in the SM role separation environment of GSMA.

In this specification, eSIM and eUICC are used as an equivalent concept.

The eSIM attaches the IC chip to the terminal circuit board at the terminal manufacturing stage and then inserts the SIM type data (opening information, supplementary service information, etc.) in the form of software in the form of over-the-air (OTA) Which is a new concept of SIM technology. IC chips used in eSIM generally support hardware based CCP (Crypto Co-Processor) to provide hardware-based public key generation. APIs that can be utilized based on applications (eg applets) , Java Card Platform, etc.). The Java Card Platform (Java Card Platform) is one of the platforms that can provide multi-applications and services on smart cards and so on.

Because SIM has limited memory space and security reasons, it should not be possible for anyone to install an application in SIM. Therefore, a SIM service management platform is required to mount and manage the SIM application in addition to the platform for mounting the application. The SIM service management platform issues data to the SIM memory area through authentication and security through the management key. The global platform (GlobalPlatform) and Remote File Management (RFM) and Remote Application Management (EASI TS 102.226) It is a standard technology of service management platform.

SM, which is one of the important elements in eSIM environment, eSIM remotely issues communication and supplementary service data through management keys (UICC OTA Key, GP ISD Key, etc.).

Here, the management key or the eSIM management key or the eUICC management key is an access authentication key to the eSIM for securely transmitting the business entity information to the eSIM, and is a concept distinct from a cryptographic key (a public key, etc.) It may be expressed as eUICC access credentials as described below.

In GSMA, the roles of SM are classified as SM-DP and SM-SR. In addition to the operation profile (or provider information), SM-DP builds securely the IMSI, K, OPc, supplementary service application, supplementary

Petitioner Samsung Ex-1038, 0305

service data, etc. in the form of a Credential Package, SR is responsible for securely downloading the SM-DP-generated credential package to eSIM via SIM remote management technology such as Over-The-Air (OTA) or GP SCP (Secure Communication Protocol).

Then, we propose a structure called "Circle of Trust" in Fig. 1 below, and establish an end-to-end trust relationship between the MNO and the eSIM through overlapping of trust relationships between each similar entity or entities And the concept of building. That is, MNO1 forms a trust relationship with SM1, SM1 with SM4, and SM4 form a trust relationship with eSIM, thereby forming a trust relationship between MNO and eSIM.

Before describing the present invention, the terms used in this specification will be described first.

MNO (Mobile Network Operator) means a mobile communication service provider and means an entity providing communication service to a customer through a mobile network.

The subscription manager (SM) is a subscription management device and performs management functions of the eUICC.

The eUICC supplier (eUICC Supplier) refers to the person who supplies the eUICC module and embedded software (such as firmware and operating system).

Device Vendor refers to the supplier of a device, especially a device that includes a wireless modem function via a mobile network driven by an MNO, and consequently requires a UICC (or eUICC) form.

Provisioning refers to the process of loading a profile into an eUICC, and a provisioning profile refers to a profile used by a device to connect to a communications network for the purpose of provisioning different provisioning profiles and operation profiles.

Subscription means a commercial relationship for providing services between a subscriber and a wireless communication service provider.

EUICC access credentials refer to data in the eUICC that enables secure communication between the eUICC and external entities to be set up to manage profiles on the eUICC.

Profile access credentials are data residing within a profile or within an eUICC, which means data that allows secure communication to be established between the eUICC and external entities in order to protect or manage the profile structure and its data .

A Profile is a combination of file structure, data, and applications that can be provisioned into an eUICC or managed within an eUICC, including an Operational Profile, a Provisioning Profile for provisioning, and other Policy Control Functions (PCFs) And all the information that may exist in the eUICC.

The Operation Profile or the Operator Information refers to all kinds of profiles related to Operational Subscribing.

1 illustrates an overall service architecture including an eSIM (eUICC) to which the present invention is applied.

The overall system is described as follows.

The eUICC system architecture to which the present invention may be applied may include a plurality of MNO systems, one or more SM systems, an eUICC manufacturer system, a device manufacturer system including an eUICC, an eUICC, and the like for each entity or subject The explanation is as follows.

In Fig. 1, the dotted line shows the trust circle, and the two solid lines indicate the secure link.

If a scenario where subscription information is stored and delivered is needed, it should be done under the approval of the MNO and under the control of the MNO. At a specific time, there should be only one active profile on a single eUICC, which means that the active profile is added to a single HLR at a specific time.

Petitioner Samsung Ex-1038, 0306

The MNO and the eUICC must be able to decode the MNO Credentials information, i.e., the profile (operation profile, provisioning profile, etc.). The only exception to this could be a third party, such as a SIM vendor, commissioned from a particular MNO. However, this is not a general function of a third party to do so.

The subscription can not be switched within the eUICC outside the operator policy control. The user must be aware of any changes to the MNO content and its activation subscription, be able to avoid security risks, and have a level of security sufficient to counter the current UICC model.

The MNO credential or profile may refer to an affiliate credential, including K, an algorithm, an algorithm parameter, a supplementary service application, additional service data, and so on.

The delivery of the MNO Credentials or Profile shall be done in a secure manner from end to end. Transmissions can be made in successive stages without breaking the security chain, and all steps in the transport chain must be done with the recognition and approval of the MNO. No entity in the transport chain should be able to clearly see the MNO credential, but the only exception could be a third entity, such as a SIM vendor, delegated from a particular MNO. However, this is not a general function of a third party to do so.

Operators should have full control over their credentials, and operators should have strong supervisory and control over SM operations.

The SM function must be provided by the MNO or a third party, and if provided by a third party, a commercial relationship between the SM and the MNO is established.

SM does not have any direct relationship with MNO subscribers for subscription management. The MNO has to have a relationship with the subscriber and should be an entry point for joining the customer, but it is not intended to fit into the contractual relationship that the M2M service provider (the M2M service provider is the MNO subscriber) can have with his or her customer.

While the MNO is being swapped, the donor and the receiving MNO may or may not have pre-contract with each other. There must be a mechanism to approve the pre-contract. The policy control function of the donor operator can define the removal condition of its own credential, and the policy control function (PCF) can implement this function.

The architecture introduces a function defined as SM, and the main role of the SM is to prepare a package or profile containing the MNO credential and forward it to the eUICC. The SM function may be provided directly by the MNO, or the MNO may contract with a third party to obtain the SM service.

The role of the SM can be divided into two sub functions such as SM-SR and SM-DP.

In practice, these SM-SR, SM-DP functions may be provided by other entities or by the same entity. Therefore, the functions of SM-DP and SM-SR need to be clearly bounded, and the interface between these entities needs to be defined.

The SM-DP is responsible for the secure preparation of the package or profile to be delivered to the eUICC and works with the SM-SR for actual transmission. The key functions of SM-DP are: 1) to manage the functional characteristics and certification level of the eUICC, and 2) to manage MNO credentials or profiles (eg IMSI, K, supplementary service application, , Some of which may potentially be encrypted (enciphered) by the MNO), 3) the ability to compute an OTA package for downloading by SM-SR, and additional features It can be added.

If the SM-DP function is provided by a third party, the security and trust relationship becomes very important. In addition to real-time provisioning, SM-DP can have a significant amount of background processing capability, and performance, scalability and reliability requirements are expected to be important.

SM-SR is responsible for routing and delivering the credit package securely to the corresponding eUICC. The key functions of SM-SR are: 1) to manage OTA communication with eUICC over ciphered VPN; and 2) to manage end-to-end eUICC with other SM-SR 3) the ability to manage the eUICC data used for SM-SR OTA communication provided by the eUICC provider, and 4) the ability to protect communication with the eUICC by filtering only the allowed entities (Firewall function).

The SM-SR database is provided by eUICC vendors and vendors (such as M2M endpoints) and potentially MNOs, and can be used by the MNO through the SM-SR mesh network.

Circle of trust enables an end-to-end security link during provisioning profile delivery, and SM-SR shares trust circles for secure routing of provisioning profiles and eUICC discovery. The MNO may be linked to the SM-SR and SM-DP entities in the trust circle and may provide this functionality on its own. In order to avoid illegal use of eUICC (illegal use of clustering, criminal use, denial of service, illegal MNO context change, etc.) without compromising the contractual and legal obligations of MNOs related to customers, eUICC and MNO Credential A secure end-to-end link between the two is required.

1, reference numeral 110 denotes a trust circle formed between SMs, more particularly SM-SR members, 120 is a trust circle of MNO partners, and 130 is an end-to-end trust link.

Fig. 2 shows a configuration in which SM-SR and SM-DP are located in the system in the SM separation environment.

As shown in FIG. 2, the SM is divided into SM-DP, which securely prepares various profiles related to the eUICC (MNO's operation profile, provisioning profile, etc.) and SM- SR, and the SM-DP is linked to the MNO system.

Of course, the arrangement of the SM-DP and the MNO system can be implemented differently from that of Fig. (I.e., the SM-DP is interlocked with the SM-SR, and the MNO system can be interlocked with the SM-DP)

3 is an overall flowchart of the provisioning process corresponding to the first subscription in the system to which the present invention is applied.

In the provisioning process, the eUICC transmits an activation request including device identification information (IMEI, etc.) and eUICC identification information (eICCid, etc.) to the MNO (Request activation: S310). Then, in step S320, Status request and technical capability control request / confirmation are performed (eUICC status request and technical capability control; S320)

Also, although not shown, in step S320, the eUICC transmits PKI key information (key generation algorithm, key length, key generation method, etc.), which is its public key PK or profile access credential information, And providing it to the corresponding MNO system or SM-SR.

In step S330, the MNO collects eUICC identity verification and eUICC identity verification and collect information about device between the SM-SR. In step S330, the MNO may obtain an encryption key for the corresponding eUICC, specifically, a public key corresponding to the eUICC, from the SM-SR according to an exemplary embodiment of the present invention.

The acquisition of such a public key may be static or dynamic. When the eUICC is static, it is already publicly available in the eUICC internally and in detail through a cryptographic operation processor (CCP, etc.) in the eUICC. Key and secret key are generated and the private key is stored in the eUICC, and the public key is shared by all the SM-SRs so that the public key of the specific eUICC can be recognized. If there is a request from the MNO, the SM- And transmits the public key for the eUICC to the MNO.

As described below with reference to FIGS. 8 and 9, when there is a request (including specific eUICC identification information) from the MNO, the SM-SR requests the corresponding eUICC to transmit the public key , The corresponding eUICC is an issuance processing module in the eUICC-equipped terminal (which is not limited to this term and can be called a communication module, a provisioning module, an issuance module, an opening module, etc.), communication with the outside of the terminal equipped with an eUICC for provisioning of eUICC,), Or a security module in the eUICC (a module that performs cryptographic key generation in eUICC such as cryptographic key generation module, cryptographic key processing module, Security Policy module, Credential Manager, Profile Manager, etc.) To generate the public key, and then transmits the generated public key to the SM-SR. This will be described in more detail below.

In this case, one security module installed in the eUICC may be installed in the eUICC according to the eUICC manufacturing process or the eUICC policy thereafter, and a plurality of security modules may be installed for each MNO according to the eUICC policy and each MNO policy.

Petitioner Samsung Ex-1038, 0308

The MNO that obtained the eUICC's public key (cryptographic key) generates a new eUICC profile for the MNO through the SM-DP, encrypts the profile with the obtained eUICC public key (cryptographic key), and sends it to the MNO. Primary encryption, step S340). At this time, the SM-DP can generate an additional digital signature with its own private key to provide authenticity. That is, in step S340, the SM-DP can sign the profile with its own private key or secret key for authentication.

Next, when the MNO transmits the primary encrypted (eUICC) profile to the SM-SR and requests the secondary encryption, the SM-SR uses the eUICC management key (eUICC OTA key, GP ISD key, etc.) The eUICC profile is secondarily encrypted and transferred to the MNO (step S350)

Then, the MNO transmits a double ciphered eUICC profile to the corresponding eUICC (step S360). At this time, the public key or certificate of the SM-DP can be transmitted together with the eUICC to provide authentication is.

Since the eUICC already knows the eUICC management key, the eUICC decrypts the profile to be used for provisioning completely by decrypting it first, and then performing secondary decoding using the secret key (already known at the manufacturing or public key dynamic generation step) corresponding to the public key of the eUICC can do. In this case, the eUICC sends the public key of the SM-DP (in the case of a certificate, from a trusted third entity) to the certificate authority (to confirm that the eUICC profile is generated from the SM-DP corresponding to the public key obtained from the MNO) The validity of the certificate can be verified).

In step S370, the SM-SR database is updated between the eUICC and the SM-SR that have finished the provisioning according to the status request and the response thereto.

The major components of each of these steps are described as follows.

In step S310, the eUICC identification information (such as eICCid) is public data and must be integrated within the eUICC.

In S320 and S330, the status request and the technical possibility control provide proof of the eUICC identity (trusted eUICC), and it should be possible to confirm the eligibility of the eUICC characteristic for the MNO service.

In steps S340 to S360, a dual encryption mechanism is used for eUICC profile creation and transmission. That is, the generation profile linked to the eUICC by the SM-DP is encrypted by a cryptographic mechanism that can only be read by the target eUICC, and the digital signature is performed by the SM-DP to confirm that the profile is generated from the legitimate SM-DP , And the SM-SR encrypts the generation profile with the eUICC management key to authenticate and protect the eUICC during delivery.

In step S370, the SM-SR database may be updated at the final stage of the subscription installation.

4 is an overall flowchart of a subscription change or MNO change process to which the present invention is applied.

3 is similar to the provisioning process of FIG. 3 (i.e., the new MNO after the change corresponds to the MNO of FIG. 3), but a new MNO performs a negotiation and right transfer process to the donor MNO before and after the profile creation of the new MNO (Step S440 ').

The difference between the MNO change process of FIG. 4 and the provisioning process of FIG. 3 is that the activation request is transmitted to the donor MNO OTA bearer using the provisioning or operation active profile, and the new MNO is changed to one of OTA or OTI To request a route from the SM-SR to download the profile.

The MNO changing process according to FIG. 4 will be described in detail as follows.

In order to change the MNO, the eUICC transmits the activation request including the device identification information (IMEI) and the eUICC identification information (eICCid, etc.) to the MNO (Receiving MNO) to be changed (Request activation: S410) The eUICC status request and the technical capability control request / confirmation are performed between the receiving MNO and the eUICC (eUICC status request and technical capability control; S420).

Although not shown, in step S420, the eUICC transmits PKI key information (key generation algorithm, key length, key generation method, etc.), which is its public key PK or profile access credential information, It is the same as S320 which is a provisioning process that a process to be provided to the corresponding MNO system or SM-SR may be included.

In step S430, the receiving MNO collects eUICC identity verification and eUICC identity verification and collect information about device between the SM-SR. In step S430, the MNO may obtain an encryption key for the eUICC, specifically, a public key corresponding to the eUICC, from the SM-SR according to an embodiment of the present invention.

The acquisition of such a public key may be static or dynamic. When the eUICC is static, it is already publicly available in the eUICC internally and in detail through a cryptographic operation processor (CCP, etc.) in the eUICC. Key and secret key are generated and the private key is stored in the eUICC, and the public key is shared by all the SM-SRs so that the public key of the specific eUICC can be recognized. If there is a request from the MNO, the SM- And transmits the public key for the eUICC to the MNO.

As described below with reference to FIGS. 8 and 9, when there is a request (including specific eUICC identification information) from the MNO, the SM-SR requests the corresponding eUICC to transmit the public key , The corresponding eUICC is an issuance processing module in the eUICC-equipped terminal (which is not limited to this term and can be called a communication module, a provisioning module, an issuance module, an opening module, etc.), communication with the outside of the terminal equipped with an eUICC for provisioning of eUICC,), Or a security module in the eUICC (a module that performs cryptographic key generation in eUICC such as cryptographic key generation module, cryptographic key processing module, Security Policy module, Credential Manager, Profile Manager, etc.) To generate the public key, and then transmits the generated public key to the SM-SR. This will be described in more detail below.

In this case, one security module installed in the eUICC may be installed in the eUICC according to the eUICC manufacturing process or the eUICC policy thereafter, and a plurality of security modules may be installed for each MNO according to the eUICC policy and each MNO policy.

The receiving MNO that has obtained the public key (encryption key) of the corresponding eUICC generates a new eUICC profile for the MNO through the SM-DP, encrypts the profile with the obtained eUICC public key (encryption key), and transmits the encrypted profile to the MNO (Primary encryption, step S440). At this time, the SM-DP can generate an additional digital signature with its own private key to provide authenticity. That is, in step S440, the SM-DP can sign the profile with its own private key or secret key for authentication.

Also, the negotiation and right transfer step (S440 ') before or after step S440 may be performed. This negotiation and right transfer step S440 'is a process such that the new receiving MNO requests the previous MNO (donor MNO) whether the corresponding eUICC is legitimate and transfers the rights (information) according to the MNO change .

That is, in step S440 ', a new MNO (Receiving MNO) requests authentication of the donor MNO for subscription switching, and such authentication may be provided by a policy control function.

Next, when the recipient MNO sends the primary encrypted (eUICC) profile to the SM-SR and then requests the secondary encryption, the SM-SR sends the eUICC management key (eUICC OTA key, GP ISD key, etc.) The eUICC profile is secondarily encrypted and transmitted to the MNO (step S450)

Then, the MNO transmits a double ciphered eUICC profile to the corresponding eUICC (S460). At this time, the public key or certificate of the SM-DP can be transmitted together with the eUICC to provide authentication. is.

Since the eUICC already knows the eUICC management key, it decrypts it first and then decrypts the profile to be used for MNO change completely by using the secret key corresponding to its own public key (already known at the manufacturing or public key dynamic generation step) It can be decoded. In this case, the eUICC sends the public key of the SM-DP (in the case of a certificate, from a trusted third entity) to the certificate authority (to confirm that the eUICC profile is generated from the SM-DP corresponding to the public key obtained from the MNO) The validity of the certificate can be verified).

In step S470, the SM-SR database is updated by the status request and the response therebetween between the eUICC and the SM-SR that have finished the provisioning.

1 to 4, the eSIM attaches the IC chip on the terminal circuit board in the terminal manufacturing step, and then transmits SIM type software (opening information, additional service information, etc.) in the form of OTA (over the air) (A technology-based connection to a PC with a USB or the like). IC chips used in eSIM generally support hardware based CCP (Crypto Co-Processor) to provide hardware-based public key generation. APIs that can be utilized based on applications (eg applets) , Java Card Platform, etc.). The Java Card Platform is one of the platforms that can provide multi-applications and services on smart cards and so on.

Because SIM has limited memory space and security reasons, it should not be possible for anyone to install an application in SIM. Therefore, a SIM service management platform is required to mount and manage the SIM application in addition to the platform for mounting the application. The SIM service management platform issues data to the SIM memory area through authentication and security through the management key. The GlobalPlatform and the Remote File Management (RFM) and Remote Application Management (RAM) of ETSI TS 102.226 are used for the SIM service management platform It is standard technology.

One of the important factors in the eSIM environment is SM, eSIM is responsible for issuing communication and supplementary service data through management key remotely. In GSMA, the roles of SM are classified as SM-DP and SM-SR. The SM-DP can securely build the profile (IMSI, K, OPc, supplementary service data, etc.) into a Credential Package form. The SM-SR can transfer the Credential Package generated by the SM-DP to the OTA or GP SCP Secure Communication Protocol (eSIM). The GSMA proposed the concept of "Circle of Trust" in the figure below and suggested the concept of establishing an end-to-end trust relationship between MNO and eSIM through overlapping of trust relations between each similar entity. In other words, MNO defines a trust relationship with SM1, SM1 with SM4, and SM4 with eSIM, thereby forming a trust relationship between MNO and eSIM

ESIM provides communication and additional services by issuing profiles by software from external entities such as SM. However, the profile type information (e.g., Operational Profile, Provisioning Profile, PCF (Policy Control Function, Value-Added Service) Profile, etc.), the type of active profile and identification information), And the list of profiles installed in the eSIM is not clear.

Accordingly, a method of managing a profile in an eSIM according to an embodiment of the present invention and a utilization method thereof will be described below. Hereinafter, the embedded type smart card which can be called an embedded SIM (eSIM) or an embedded UICC (eUICC) is unified with the eUICC.

5 is a diagram illustrating a basic structure of a profile management method according to an embodiment of the present invention.

Referring to FIG. 5, a profile management method according to an embodiment of the present invention is directed to a profile management method in an eUICC 510 interworking with a Mobile Network Operator (MNO) and a Subscription Manager (SM) (S502) of providing at least one of the information about the type of the activated profile and the information about the profile list to the external entity as management information necessary for utilizing the profile, and the like.

Here, the external entity may be one of the eUICC-equipped device 500, the MNO, and the SM that mounts the eUICC 510. However, for convenience of explanation, the external entity may be an eUICC-equipped device 500 are assumed to be external entities. In the following description, it is assumed that the eUICC 510 provides the management information necessary for using the profile to the eUICC-equipped device 500. [

In this specification, a "profile" may mean a combination of a file structure, data, an application (eg, an applet, etc.) in the eUICC 510, a profile for communication, Can mean similar forms of information.

As described above, the eUICC 510 provides the external entity 500 with at least one of the information about the type of the activated profile and the information about the profile list, as management information necessary for utilizing the profile. As the management information, one or more of profile identification information (e.g., profile ID) and profile description information (e.g., LTE profile of carrier A, 3G profile of carrier A, etc.).

As described above, the & quot; management information & quot; provided by the eUICC 510 as an external entity may be type information, identification information, list information, explanation information, etc. for the

Petitioner Samsung Ex-1038, 0311

activated profile. The eUICC 510 Type information, identification information, list information, explanation information, etc. for all or some of the profiles installed in the network.

Such management information is stored in a profile form in the eUICC 510 and can be accessed according to access control.

In addition, the management information may have a file structure in the form of a TLV (Type Length Value) based on the current SIM technology, or may be stored in an application form such as an EF form and an applet.

Also, the management information can be accessed and managed by access control through at least one of a security key and a PIN (Personal Identification Number), and the management information can be managed by using SM (SM-SR, SM-DP, It can be updated, activated or deactivated only by an authorized entity that contains one or more. However, the management information can be freely read by the external entity. Of course, the access rights may differ depending on the eUICC 510 security policy.

In this specification, the management information can be managed through the management profile 511 that manages the profile information in the eUICC 510. Here, the management profile 511 may be, for example, a profile for the PCF (Policy Control Function), a General Profile, a Common Profile, an Administration Profile, an Administrative Profile, an Information Profile, and the like.

5, the basic structure for the profile management method according to the embodiment of the present invention includes a management profile 511 for managing profile information in the eUICC 510, Can be.

In step S502, the eUICC 510 transmits, to the eUICC-equipped device 500, at least one of the information about the type of the activated profile and the profile list, May directly provide the management information without receiving any request from the eUICC-equipped device 500 or after receiving the management information request from the eUICC-equipped device 500, provide the management information as a response to the management information request It is possible.

5, the management information is provided through a request-response process. If the management information is provided through the request-response process as shown in FIG. 5, step S502 The management profile 511 in the eUICC 510 may previously perform the step S500 of receiving a management information request from an external entity (e.g., the eUICC-equipped device 500, etc.).

Hereinafter, with reference to the profile management method according to the embodiment of the present invention, the eUICC-equipped device 500 will be described in more detail with reference to Fig.

6 is a block diagram of an eUICC-equipped device 500 according to an embodiment of the present invention.

The eUICC-equipped device 500 according to the embodiment of the present invention shown in FIG. 6 is a device including an eUICC 510 interworking with an MNO (Mobile Network Operator) and an SM (Subscription Manager).

Referring to FIG. 6, the eUICC-equipped device 500 according to an embodiment of the present invention may include at least one of information about the type of the activated profile and information about the profile list, And a management information obtaining unit 610 that obtains the management information from the management information obtaining unit 610 and the like.

The management information acquiring unit 610 may include at least one of information about the type of the activated profile and information about the profile list as management information necessary for utilizing the profile, Information or the like can be further obtained as management information.

The management information obtaining unit 610 also stores the type, list, identification information, description information, and the like for all or some of the profiles installed in the eUICC 510 as the management information necessary for using the profile, It can also be obtained.

6, the eUICC-equipped device 500 according to the embodiment of the present invention includes a profile list display unit 620 that displays a profile list, And a management profile updating unit 640 for updating the management profile 511 based on the activated profile in cooperation with the MNO after network authentication is completed is.

Hereinafter, the eUICC 510, which is embedded in the eUICC-equipped device 500 having the configuration as shown in Fig. 6, will be described in more detail with reference to Fig.

7 is a block diagram of an eUICC 510 in accordance with an embodiment of the present invention.

Referring to FIG. 7, the eUICC 510 according to the embodiment of the present invention is an embedded Universal Integrated Circuit Card (eUICC) interworking with an MNO (Mobile Network Operator) and an SM (Subscription Manager) And a management information providing module 710 for providing at least one of information on the type of the profile list and the like to the external entity as management information necessary for using the profile.

Here, the external entity may be one of the eUICC-equipped device 500, the MNO, and the SM. However, for convenience of explanation, it is assumed that the eUICC-equipped device 500 is an external entity.

For example, the management information providing module 710 may be a management profile 511 in the eUICC 510. In some cases, the management information providing module 710 may not be in the same profile format as the management profile 511, Or a Profile Manager as a logical entity in the eUICC 510 that is being accessed.

Referring to FIG. 7, the eUICC 510 according to an embodiment of the present invention provides a profile list as management information necessary for using a profile to an eUICC-equipped device 500 as an external entity, And a management profile update module 730 for updating the management profile 511 based on the activated profile in cooperation with the MNO, and the like is.

The above-mentioned management information may include at least one of category information, identification information, list information, and explanatory information for the installed or activated profile in the eUICC 510, as described above.

Such management information may have a file structure in the form of a TLV (Type Length Value), or may have an application type file structure.

Further, such management information can be accessed and managed by access control through at least one of a security key and a PIN (Personal Identification Number). Thus, the management information may be modified, activated or deactivated by an authorized entity including one or more of MNO, SM, and the like.

Hereinafter, examples of utilization of the above-described profile management method will be described. In this example of utilization, it is assumed that the eUICC 510 provides information on the profile list to the eUICC-equipped device 500. [

FIG. 8 is a flowchart of an application method of a profile management method according to an embodiment of the present invention.

Referring to FIG. 8, a profile management method in an embedded UICC (eUICC) interworking with the MNO 800 according to an embodiment of the present invention includes a profile list providing step S800, A user selection step S802, a network authentication progress step S804, and a management profile update step S806.

Providing the profile list (S800): The eUICC 510 provides the profile list to the eUICC-equipped device 500. At this time, the eUICC 510 receives a request for the profile list as management information necessary for profile utilization from the eUICC-equipped device 500, and transmits the profile list to the eUICC-equipped device 500 as a response to the request .

Display and user selection of profile list (S802): The eUICC-equipped device 500 receives the profile list from the eUICC 510, displays the received profile list, and selects one of the profiles You can enter selection information for a profile.

At this time, the eUICC-equipped device 500 may provide the MNO 800 or the eUICC 510 with selection information on the profile selected by the user.

Petitioner Samsung Ex-1038, 0313

- Network Authentication Proceeding Step (S804): The NNO 800 proceeds network authentication with the eUICC-equipped device 500 based on the profile selected by the user or the like in the profile list provided by the eUICC 510.

- Management Profile Update Step (S806): After the network authentication is completed, the NNO 800 updates the management profile 511 managing the profile list in the eUICC 510 based on the activated profile.

At this time, the NNO 800 can update the management profile 511, which manages the profile list in the eUICC 510, based on the activated profile, in cooperation with the SM (SM-SR, etc.).

On the other hand, when the MNO 800 creates a new profile in the eUICC 510 or deletes an existing profile, the MN can update the management profile according to the profile status in the eUICC.

According to the present invention as described above, the eUICC-equipped device 500 can know the profile type and identification information activated in the eUICC 510 and the list of installed profiles.

Accordingly, when a plurality of profiles in the eUICC 510 are mounted or activated, basic information that can efficiently and conveniently specify the operation of the eUICC-equipped device 500 and interworking with the external system through the management profile of the present invention It is easy and convenient to use.

The description above is merely illustrative of the technical idea of the present invention, and various changes and modifications may be made by those skilled in the art without departing from the essential characteristics of the present invention. Therefore, the embodiments disclosed in the present invention are intended to illustrate rather than limit the scope of the present invention, and the scope of the technical idea of the present invention is not limited by these embodiments. The scope of protection of the present invention should be construed according to the following claims, and all technical ideas within the scope of equivalents should be interpreted as being included in the scope of the present invention.

CROSS-REFERENCE TO RELATED APPLICATION

This patent application claims priority under 35 USC § 119 (a) to U.S. Patent Application No. 119 (a), U.S. Patent Application No. 10-2011-0097901, filed on September 28, 2011, All content is incorporated herein by reference. In addition, this patent application is also incorporated in the present patent application as a reference, if the priority is given to any country other than the United States for the same reason as above.

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2013 년 4 월 4 일 (04.04.2013)

WIPO | PCT

(10) 국제공개번호
WO 2013/048084 A2

(51) 국제특허분류: 미분류

(21) 국제출원번호: PCT/KR2012/007705

(22) 국제출원일: 2012 년 9 월 25 일 (25.09.2012)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2011-0097901 2011 년 9 월 28 일 (28.09.2011) KR

(71) 출원인: 주식회사 케이티 (KT CORPORATION) [KR/KR]; 463-815 경기도 성남시 분당구 정자동 206, Gyeonggi-do (KR).

(72) 발명자: 박재민 (PARK, Jaemin); 137-140 서울시 서초구 우면동 17 KT 연구개발센터, Seoul (KR).

(74) 대리인: 김은구 (KIM, Eungu) 등; 135-908 서울특별시 강남구 역삼동 636-15 상원빌딩 2 층, Seoul (KR).

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

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

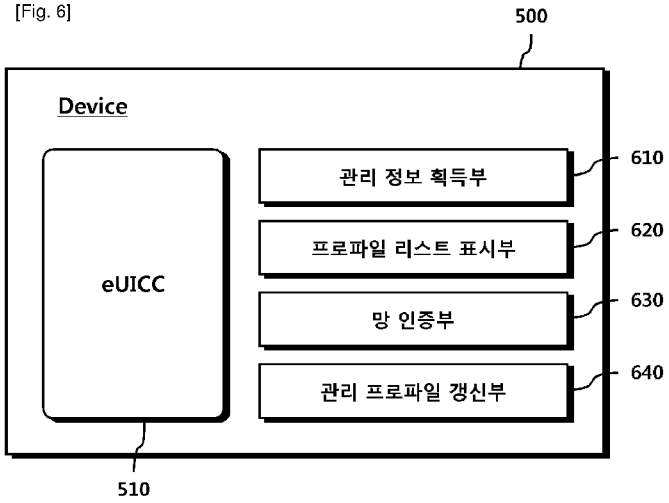
공개:

— 국제조사보고서 없이 공개하며 보고서 접수 후 이를 별도 공개함 (규칙 48.2(g))

(54) Title: PROFILE MANAGEMENT METHOD, EMBEDDED UICC, AND DEVICE PROVIDED WITH THE EMBEDDED UICC

(54) 발명의 명칭 : 프로파일 관리 방법, 내장 U I C C 및 내장 U I C C 탑재 기기

[Fig. 6]



500 ... Device
610 ... Management information acquiring unit
620 ... Profile list display unit
630 ... Network authentication unit
640 ... Management profile update unit

(57) Abstract: The present invention relates to a method for managing a profile in an embedded UICC, and more particularly, to a method for managing a profile in an embedded UICC that enables management information on the profile provided within the embedded UICC to play an essential role for providing communication and additional services, to be provided to a device existing outside the embedded UICC. The present invention also relates to an embedded UICC and to a device provided with the embedded UICC for the method.

(57) 요약서: 본 발명은 내장 UICC 내 프로파일 관리 방법에 관한 것으로서, 더욱 상세하게는, 내장 UICC 내에 탑재되어 통신 및 부가 서비스를 제공하는데 필수적인 프로파일에 대한 관리 정보를 내장 UICC 외부로 제공할 수 있도록 해주는 내장 UICC 내 프로파일 방법과, 이를 위한 내장 UICC 및 내장 UICC 탑재 기기에 관한 것이다.

WO 2013/048084 A2

Petitioner Samsung Ex-1038, 0315

명세서

발명의 명칭: 프로파일 관리 방법, 내장 U I C C 및 내장 U I C C 탑재 기기

기술분야

[1] 본 발명은 내장 UICC 내 프로파일을 관리하는 방법과, 이를 위한 내장 UICC 및 내장 UICC 탑재 기기에 관한 것이다. 특히, 내장 UICC 내 프로파일에 대한 정보를 외부에서 확인하고 활용하기 위한 방법에 관한 것이다.

배경기술

[2] UICC(Universal Integrated Circuit Card)는 단말기 내에 삽입되어 사용자 인증을 위한 모듈로서 사용될 수 있는 스마트 카드이다. UICC는 사용자의 개인 정보 및 사용자가 가입한 이동 통신 사업자에 대한 사업자 정보를 저장할 수 있다. 예를 들면, UICC는 사용자를 식별하기 위한 IMSI(International Mobile Subscriber Identity)를 포함할 수 있다.

[3] 이러한 UICC는 GSM(Global System for Mobile communications) 방식의 경우 SIM(Subscriber Identity Module) 카드, WCDMA(Wideband Code Division Multiple Access) 방식의 경우 USIM(Universal Subscriber Identity Module) 카드로 불리기도 한다.

[4] 사용자가 UICC를 사용자의 단말에 장착하면, UICC에 저장된 정보들을 이용하여 자동으로 사용자 인증이 이루어져 사용자가 편리하게 단말을 사용할 수 있다. 또한, 사용자가 단말을 교체할 때, 사용자는 기존의 단말에서 탈거한 UICC를 새로운 단말에 장착하여 용이하게 단말을 교체할 수 있다.

[5] 소형화가 요구되는 단말, 예를 들면 기계 대 기계(Machine to Machine, M2M) 통신을 위한 단말은 UICC를 착탈할 수 있는 구조로 제조할 경우 단말의 소형화가 어려워진다. 그리하여, 착탈할 수 없는 UICC인 내장 UICC(Embedded UICC) 구조가 제안되었다. 내장 UICC는 해당 UICC를 사용하는 사용자 정보가 IMSI 형태로 수록되어야 한다.

[6] 기존의 UICC는 단말에 착탈이 가능하여, 단말의 종류나 이동 통신 사업자에 구애받지 않고 사용자는 단말을 개통할 수 있다. 그러나, 단말을 제조할 때부터 제조된 단말은 특정 이동 통신 사업자에 대해서만 사용된다는 전제가 성립되어야 내장 UICC 내의 IMSI를 할당할 수 있다. 단말을 발주하는 이동 통신 사업자 및 단말 제조사는 모두 제품 재고에 신경을 쓸 수밖에 없고 제품 가격이 상승하는 문제가 발생하게 된다. 사용자는 단말에 대해 이동 통신 사업자를 바꿀 수 없는 불편이 있다. 그러므로, 내장 UICC의 경우에도 이동 통신 사업자에 구애받지 않고 사용자가 단말을 개통할 수 있는 방법이 요구된다.

[7] 한편, 최근 내장 UICC의 도입으로 인하여 여러 이동 통신 사업자의 가입자 정보를 원격에서 UICC로 업데이트 할 필요가 생기게 되었고, 그에 따라 가입자

Petitioner Samsung Ex-1038, 0316

정보 관리를 위한 가입 관리 장치(Subscription Manager; 이하 "SM"이라 함) 또는 프로파일 관리장치(Profile Manager; 이하 "PM"이라 함)가 논의되고 있다.

[8] 이와 같이, 기존의 착탈식 형태의 UICC와는 달리 단말에 일체형으로 탑재되는 내장 UICC(이하 "eSIM" 또는 "eUICC"라고 함)은 그 물리적 구조 차이로 인해 개통 권한, 부가 서비스 사업 주도권, 가입자 정보 보안 등에 대한 많은 이슈들이 존재한다. 이를 위해 GSMA 및 ETSI의 국제 표준화 기관에서는 사업자, 제조사, SIM Vendor 등의 유관 회사들과 최상위 구조를 포함한 필요한 요소에 대해 표준화 활동을 전개하고 있다.

[9] 이와 같이, eUICC가 표준화 단체들을 통해 논의되면서 이슈의 중심에 있는 것은 가입 관리 장치(Subscription Manager)라고 불리는 SM으로 프로파일(Operator Credential, Profile)를 eUICC에 발급하고 가입(Subscription) 변경에 대한 프로세스를 처리하는 등 eUICC에 대한 전반적인 관리 역할을 수행하는 개체 또는 그 기능/역할을 의미한다.

[10] 하지만, eUICC 내에 탑재되어 통신 및 부가 서비스를 제공하는데 필수적인 프로파일의 종류/식별정보/리스트 등의 관리 정보를 eUICC 외부 (예: eUICC를 탑재하는 단말 등)에 제공하고 이를 활용하는 방안은 존재하지 않는다.

발명의 상세한 설명

기술적 과제

[11] 본 발명의 목적은 eUICC 내에 탑재되어 통신 및 부가 서비스를 제공하는데 필수적인 프로파일에 대한 관리 정보를 eUICC 외부로 제공할 수 있도록 해주는 eUICC 내 프로파일 방법을 제공하는 데 있다.

[12] 본 발명의 다른 목적은 eUICC 내 프로파일에 대한 관리 정보를 eUICC로부터 제공받아 활용하는 방안을 제공하는 데 있다.

[13] 본 발명의 다른 목적은, eUICC 내의 프로파일에 대한 관리 정보를 효율적으로 관리하고, eUICC 외부 엔티티(예: 단말, MNO, SM 등)와 편리하게 연동할 수 있도록 해주는 관리 프로파일을 제안하는 데 있다.

과제 해결 수단

[14] 본 발명의 일 실시예는, MMNO(Mobile Network Operator), SM(Subscription Manager)과 연동되는 내장 UICC(eUICC: embedded Universal Integrated Circuit Card) 내 프로파일 관리 방법으로서, eUICC가 활성화된 프로파일의 종류에 대한 정보와 프로파일 리스트에 대한 정보 중 하나 이상을 외부 엔티티(External Entity)로 제공하는 단계를 포함하는 프로파일 관리 방법을 제공한다.

[15] 본 발명의 다른 실시예는, MNO(Mobile Network Operator), SM(Subscription Manager)와 연동하는 내장 UICC(eUICC: embedded Universal Integrated Circuit Card)로서, 상기 eUICC는 활성화된 프로파일의 종류에 대한 정보와 프로파일 리스트에 대한 정보 중 하나 이상을 외부 엔티티(External Entity)로 제공하는 관리 정보 제공 모듈을 포함하는 eUICC를 포함한다.

Petitioner Samsung Ex-1038, 0317

[16] 본 발명의 또 다른 실시예는, MNO(Mobile Network Operator), SM(Subscription Manager)과 연동하는 내장 UICC(eUICC: embedded Universal Integrated Circuit Card)를 포함하는 기기로서, 활성화된 프로파일의 종류에 대한 정보와 프로파일 리스트에 대한 정보 중 하나 이상을 eUICC로부터 획득하는 관리 정보 획득부를 포함하는 eUICC 내 프로파일을 관리하는 eUICC를 포함하는 기기를 포함한다.

[17] 본 발명의 또 다른 실시예는, NO(Mobile Network Operator)와 연동되는 내장 UICC(eUICC: embedded Universal Integrated Circuit Card) 내 프로파일 관리 방법으로서, 상기 NNO가 상기 eUICC에서 제공된 프로파일 리스트에서 선택된 프로파일을 토대로 eUICC를 포함하는 기기와 망 인증을 진행하는 단계; 및 상기 MNO가 상기 eUICC 내에서 상기 프로파일 리스트를 관리하는 관리 프로파일을 활성화된 프로파일을 기준으로 갱신하는 단계를 포함하는 프로파일 관리 방법을 제공한다.

도면의 간단한 설명

[18] 도 1은 본 발명이 적용되는 eSIM(eUICC)을 포함한 전체 서비스 아키텍처를 도시한다.

[19] 도 2는 본 발명이 적용될 수 있는 SM 분리 환경의 시스템 아키텍처를 도시한다.

[20] 도 3은 본 발명이 적용되는 서비스 아키텍처에서 프로비저닝 과정의 전체 흐름도이다.

[21] 도 4는 본 발명이 적용되는 가입 변경 또는 MNO 변경 과정의 전체 흐름도이다.

[22] 도 5는 본 발명의 실시예에 따른 프로파일 관리 방법을 위한 기본적인 구조를 나타낸 도면이다.

[23] 도 6은 본 발명의 실시예에 따른 eUICC를 포함하는 기기에 대한 블록도이다.

[24] 도 7은 본 발명의 실시예에 따른 eUICC에 대한 블록도이다.

[25] 도 8은 본 발명의 실시예에 따른 프로파일 관리 방법의 활용 방안에 대한 흐름도이다.

발명의 실시를 위한 형태

[26] 이하, 본 발명의 일부 실시예들을 예시적인 도면을 통해 상세하게 설명한다. 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 발명을 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.

[27] 현재 GSMA에서 활발하게 논의되는 M2M(Machine-to-Machine) 단말은 특성상 크기가 작아야 하는데, 기존 UICC를 사용하는 경우에는, M2M 단말에 UICC를 장착하는 모듈을 별도 삽입해야 하므로, UICC를 탈착가능한 구조로 M2M단말을 제조하게 되면, M2M 단말의 소형화가 힘들게 된다.

[28] 따라서, UICC 착탈이 불가능한 내장(Embedded) UICC 구조가 논의되고 있는데,

Petitioner Samsung Ex-1038, 0318

이때 M2M 단말에 장착되는 eUICC에는 해당 UICC를 사용하는 이동통신 사업자(Mobile Network Operator; 이하 "MNO"라 함)정보가 국제 모바일 가입자 식별자(International Mobile Subscriber Identity, IMSI) 형태로 UICC에 저장되어 있어야 한다.

[29] 그러나, M2M 단말을 제조할 때부터 제조된 단말은 특정 MNO에서만 사용한다는 전제가 성립되어야 eUICC내의 IMSI를 할당할 수 있으므로, M2M 단말 또는 UICC를 발주하는 MNO나 제조하는 M2M 제조사 모두 제품 재고에 많은 신경을 할당할 수 밖에 없고 제품 가격이 상승하게 되는 문제가 있어, M2M 단말 확대에 큰 걸림돌이 되고 있는 상황이다.

[30] 이와 같이, 기존의 착탈식 형태의 SIM과는 달리 단말에 일체형으로 탑재되는 내장 SIM (이하 "eSIM" 또는 "eUICC"라 함)은 그 물리적 구조 차이로 인해 개통 권한, 부가 서비스 사업 주도권, 가입자 정보 보안 등에 대한 많은 이슈들이 존재한다. 이를 위해 GSMA 및 ETSI의 국제 표준화 기관에서는 사업자, 제조사, SIM 제조사(Vendor) 등의 유관 회사들과 최상위 구조를 포함한 필요한 요소에 대해 표준화 활동을 전개하고 있다. eSIM이 표준화 단체들을 통해 논의되면서 이슈의 중심에 있는 것은 SM으로서, 중요한 프로파일(Operator Credential, MNO Credential, Profile, eUICC Profile, Profile Package 등으로 불릴 수 있음)를 eSIM에 발급하고 가입 변경에 대한 프로세스를 처리하는 등 eSIM에 대한 전반적인 관리 역할을 수행하는 개체 또는 그 기능/역할을 의미한다.

[31] 최근 GSMA에서는 SM의 역할을 사업자 정보를 생성하는 역할을 수행하는 SM-DP (Data Preparation)과 eSIM에 사업자 정보의 직접적 운반을 수행하는 SM-SR (Secure Routing)로 분류한 구조를 제안하였으나, 세부적이며 기술적인 실제 발급 방식에 대해서는 언급하고 있지 않다.

[32] 이에 본 발명에서는 GSMA의 SM 역할 분리 환경에서 동적 암호키 (공개 키 등) 생성을 활용하여 eSIM을 관리하는 방안을 제시한다.

[33] 본 명세서에서는 eSIM과 eUICC를 동등한 개념으로 사용한다.

[34] eSIM은 단말 제조 단계에서 IC칩을 단말 회로판 상에 부착시킨 후, 소프트웨어 형태의 SIM 데이터 (개통 정보, 부가 서비스 정보 등)를 OTA (Over The Air) 또는 오프라인 (PC와의 USB 등의 기술 기반 연결)을 통해 발급하는 방식의 새로운 개념의 SIM 기술이다. eSIM에서 사용되는 IC칩은 일반적으로 하드웨어 기반의 CCP (Crypto Co-Processor)를 지원하여 하드웨어 기반의 공개키 생성을 제공하며, 이를 어플리케이션 (예, 애플릿) 기반에서 활용할 수 있는 API를 SIM 플랫폼 (예, Java Card Platform 등)에서 제공한다. 자바 카드 플랫폼(Java Card Platform)은 스마트카드 등에서 멀티 어플리케이션을 탑재하고 서비스를 제공할 수 있는 플랫폼 중 하나이다.

[35] SIM은 제한된 메모리 공간과 보안상의 이유로 누구나 SIM 내에 어플리케이션을 탑재해서는 안되며, 이로 인해 어플리케이션 탑재를 위한 플랫폼 이외에 SIM을 어플리케이션 탑재 및 관리를 담당하는 SIM 서비스 관리

Petitioner Samsung Ex-1038, 0319

플랫폼을 필요로 한다. SIM 서비스 관리 플랫폼은 관리키를 통한 인증 및 보안을 통해 SIM 메모리 영역에 데이터를 발급하며, 글로벌 플랫폼(GlobalPlatform)과 ETSI TS 102.226의 RFM (Remote File Management) 및 RAM (Remote Application Management)은 이와 같은 SIM 서비스 관리 플랫폼의 표준 기술이다.

[36] eSIM 환경에서 중요한 요소 중의 하나인 SM은 eSIM은 원격으로 관리키(UICC OTA Key, GP ISD Key 등)를 통해 통신 및 부가 서비스 데이터를 발급하는 역할을 수행한다.

[37] 여기서, 관리키 또는 eSIM 관리키 또는 eUICC 관리키는 eSIM으로의 접근 인증키로서 사업자 정보를 안전하게 eSIM으로 전달하기 위한 것이며, 본 발명에서 주로 다루는 암호키 (공개키 등)과는 구별되는 개념이며, 아래 설명할 바와 같이 eUICC 접근 크레덴셜(eUICC access credentials)로 표현될 수도 있을 것이다.

[38] GSMA에서는 SM의 역할을 SM-DP와 SM-SR로 분류하였다. SM-DP는 오퍼레이션 프로파일(또는 사업자 정보) 이외에 IMSI, K, OPc, 부가 서비스 어플리케이션, 부가 서비스 데이터 등을 안전하게 빌드(Build)하여 크레덴셜 패키지(Credential Package) 형태로 만드는 역할을 수행하며, SM-SR은 SM-DP가 생성한 크레덴셜 패키지를 OTA(Over-The-Air) 또는 GP SCP (Secure Communication Protocol)과 같은 SIM 원격 관리 기술을 통해 eSIM에 안전하게 다운로드하는 역할을 수행한다.

[39] 그리고 아래 도 1의 "신뢰 서클(Circle of Trust)"이라는 구조를 제안하여 각 유사 개체 또는 엔터티 들간에 신뢰 관계의 중첩을 통해 MNO와 eSIM 간의 엔드-투-엔드(End-to-End) 신뢰 관계를 구축한다는 개념을 제안하였다. 즉, MNO1는 SM1과, SM1은 SM4, SM4는 eSIM과 신뢰관계를 형성하여, 이를 통해 MNO와 eSIM 간의 신뢰관계를 형성한다는 개념이다.

[40] 본 발명을 설명하기 전에 우선 본 명세서에서 사용할 용어에 대하여 설명한다.

[41] MNO(Mobile Network Operator)는 이동통신 사업자를 의미하며, 모바일 네트워크를 통해 고객에게 통신 서비스를 제공하는 엔터티를 의미한다.

[42] SM(Subscription manager)는 가입 관리 장치로서, eUICC의 관리 기능을 수행한다.

[43] eUICC 공급자(eUICC Supplier)는 eUICC 모듈과 내장 소프트웨어(펌웨어와 오퍼레이팅 시스템 등)를 공급하는 자를 의미한다.

[44] 장치 공급자(Device Vendor)는 장치의 공급자, 특히 MNO에 의해서 구동되는 모바일 네트워크를 통한 무선 모뎀 기능을 포함하며, 따라서 결과적으로 UICC(또는 eUICC) 형태가 필요한 장치의 공급자를 의미한다.

[45] 프로비저닝(Provisioning)은 eUICC 내부로 프로파일을 로딩하는 과정을 의미하며, 프로비저닝 프로파일은 다른 프로비저닝 프로파일 및 오퍼레이션 프로파일을 프로비저닝할 목적으로 장치가 통신 네트워크에 접속하는데 사용되는 프로파일을 의미한다.

Petitioner Samsung Ex-1038, 0320

[46] 가입(Subscription)은 가입자와 무선통신 서비스 제공자 사이의 서비스 제공을 위한 상업적인 관계를 의미한다.

[47] eUICC 접근 크레덴셜(eUICC access credentials)은 eUICC 상의 프로파일을 관리하기 위하여 eUICC 및 외부 엔터티 사이에 보안 통신이 셋업 될 수 있도록 하는 eUICC 내의 데이터를 의미한다.

[48] 프로파일 엑세스 크레덴셜(Profile access credentials)은 프로파일 내부 또는 eUICC 내부에 존재하는 데이터로서, 프로파일 구조 및 그 데이터를 보호 또는 관리하기 위하여 eUICC 및 외부 엔터티 사이에 보안 통신이 셋업 될 수 있도록 하는 데이터를 의미한다.

[49] 프로파일(Profile)은 eUICC로 프로비저닝 되거나 eUICC 내에서 관리될 수 있는 파일 구조, 데이터 및 애플리케이션의 조합으로서, 사업자 정보인 오퍼레이션 프로파일, 프로비저닝을 위한 프로비저닝 프로파일, 기타 정책 제어 기능(PCF; Policy Control Function)을 위한 프로파일 등 eUICC 내에 존재할 수 있는 모든 정보를 의미한다.

[50] 오퍼레이션 프로파일(Operation Profile) 또는 사업자 정보는 사업자 가입(Operational Subcription)과 관련된 모든 종류의 프로파일을 의미한다.

[51] 도 1은 본 발명이 적용되는 eSIM(eUICC)을 포함한 전체 서비스 아키텍처를 도시한다.

[52] 전체 시스템에 대해서 설명하면 다음과 같다.

[53] 본 발명이 적용될 수 있는 eUICC 시스템 아키텍처는 다수의 MNO 시스템과, 1 이상의 SM 시스템, eUICC 제조사 시스템, eUICC를 포함하는 장치(Device) 제조사 시스템 및 eUICC 등을 포함할 수 있으며, 각 엔터티 또는 주체에 대한 설명은 다음과 같다.

[54] 도 1에서 점선은 신뢰 서클을 도시하고, 2개 실선은 안전한 링크를 의미한다.

[55] 가입정보가 저장되어 전달되는 시나리오가 필요하면, MNO의 승인과 MNO의 컨트롤 하에서 이루어져야 한다. 특정 시각에 단일의 eUICC 상에는 1개만의 액티브 프로파일이 있어야 하며, 이 때 액티브 프로파일은 특정 시간에 단일 HLR에 부가되는 것을 의미한다.

[56] MNO와 eUICC는 MNO 크레덴셜(Credentials) 정보, 즉 프로파일(오퍼레이션 프로파일, 프로비저닝 프로파일 등)를 복호할 수 있어야 한다. 이에 대한 유일한 예외는 예를 들면 SIM 벤더와 같이 특정 MNO으로부터 위임받은 제3 기관이 될 수 있다. 하지만, 이를 수행하기 위한 제3 기관의 일반적인 기능은 아니다.

[57] 가입(Subscription)은 오퍼레이터 정책 제어의 외부에서는 eUICC 내에서 스위칭될 수 없다. 사용자는 MNO 컨텐스트와 그의 활성화 가입의 어떠한 변경도 알고 있어야 하며, 시큐리티 위험을 피할 수 있어야 하고, 현재의 UICC 모델과 대적할 수 있을 정도의 시큐리티 레벨이 필요하다.

[58] MNO 크레덴셜 또는 프로파일은 K, 알고리즘, 알고리즘 파라미터, 부가 서비스 어플리케이션, 부가 서비스 데이터 등을 포함하는 가입 크레덴셜을 의미할 수

Petitioner Samsung Ex-1038, 0321

있다.

[59] MNO 크레덴셜 또는 프로파일의 전달은 종단에서 종단까지 안전한 방식으로 이루어져야 한다. 전송은 시큐리티 체인을 깨지 않는 연속적인 단계로 이루어질 수 있으며, 전송 체인의 모든 단계는 MNO의 인식 및 승인 하에서 이루어져야 한다. 전송 체인 내의 어떠한 엔터티도 MNO 크레덴셜을 명확하게 볼 수 없어야 하지만, 유일한 예외는 예를 들면 SIM 벤더와 같이 특정 MNO으로부터 위임받은 제3 기관이 될 수 있다. 하지만, 이를 수행하기 위한 제3 기관의 일반적인 기능은 아니다.

[60] 오퍼레이터는 자신의 크레덴셜에 대해서 완전한 제어권을 가져야 하며, 오퍼레이터는 SM 오퍼레이션에 대해서 강한 감독권과 제어권한을 가져야 한다.

[61] SM 기능은 MNO 또는 제3 기관에 의하여 제공되어야 하며, 만약 제3 기관에 의하여 제공된다면 SM과 MNO 사이에는 상업적인 관계가 설정되어 있는 경우 등일 것이다.

[62] SM은 가입 관리를 위해서 MNO 가입자와 어떠한 직접적인 관련도 없다. MNO가 가입자와 관계를 가지며 고객 가입을 위한 진입 포인트가 되어야 하지만, 이는 M2M 서비스 제공자(M2M 서비스 제공자는 MNO 가입자 임)가 자신의 고객과 가질 수 있는 계약 관계에 편승할 의도는 아니다.

[63] MNO가 스왑(swap)되는 동안, 도너(Donor) 및 리시빙 MNO는 서로 사전 계약이 있을 수도 있고 없을 수도 있다. 사전 계약을 승인할 수 있는 메커니즘이 있어야 한다. 도너 오퍼레이터의 정책 제어(Policy Control) 기능은 자신의 크레덴셜의 제거 조건에 대하여 정의할 수 있으며, 정책 제어 기능(Policy Control Function; PCF)이 이러한 기능을 구현할 수 있다.

[64] 아키텍처는 SM이라고 정의되는 기능을 도입하며, SM의 주요한 역할은 MNO 크레덴셜을 포함하는 패키지 또는 프로파일을 준비해서 eUICC로 전달하는 것이다. SM 기능은 MNO에 의하여 직접적으로 제공될 수도 있고, MNO가 SM 서비스를 획득하기 위하여 제3 기관과 계약할 수도 있을 것이다.

[65] SM의 역할은 SM-SR, SM-DP와 같은 2개의 서브 기능으로 나뉘어 질 수 있다.

[66] 실제로, 이러한 SM-SR, SM-DP 기능들은 다른 엔터티에 의하여 제공될 수도 있고, 동일한 엔터티에 의해서 제공될 수도 있다. 따라서, SM-DP와 SM-SR의 기능을 명확하게 경계지을 필요가 있고, 이들 엔터티들 사이의 인터페이스를 정의할 필요가 있다.

[67] SM-DP는 eUICC로 전달될 패키지 또는 프로파일의 안전한 준비를 담당하며, 실제 전송을 위하여 SM-SR과 함께 동작한다. SM-DP의 핵심 기능은 1) eUICC의 기능적 특성 및 인증 레벨(Certification Level)을 관리하는 것과, 2) MNO 크레덴셜 또는 프로파일(예를 들면, IMSI, K, 부가 서비스 어플리케이션, 부가 서비스 데이터 중 하나 이상이며, 이들 중 일부는 잠재적으로 MNO에 의하여 암호화(Enciphered)되어 있을 수 있음)을 관리하는 것과, 3) SM-SR에 의한 다운로드를 위하여 OTA 패키지를 계산하는 기능 등이며, 추후 부가적인 기능이

Petitioner Samsung Ex-1038, 0322

추가될 수 있을 것이다.

[68] 만일, SM-DP 기능이 제3주체(Third party)에 의하여 제공되는 경우에는 보안과 신뢰 관계가 아주 중요해진다. SM-DP는 실시간 프로비저닝(Provisioning) 기능 이외에도 상당한 정도의 백그라운드 프로세싱 기능을 보유할 수 있으며, 퍼포먼스, 스케러빌러티(Scalability) 및 신뢰도에 대한 요구사항이 중요할 것으로 예상된다.

[69] SM-SR은 크레덴셜 패키지를 해당되는 eUICC로 안전하게 라우팅하고 전달하는 역할을 담당한다. SM-SR의 핵심 기능은 1) 사이퍼(Ciphered)된 VPN을 통한 eUICC와의 OTA 통신을 관리하는 것과, 2) eUICC까지 엔드-투-엔드(end-to-end)를 형성하기 위하여 다른 SM-SR과의 통신을 관리하는 기능과, 3) eUICC 공급자에 의하여 제공되는 SM-SR OTA 통신을 위해 사용되는 eUICC 데이터를 관리하는 기능과, 4) 오직 허용된 엔터티만을 필터링함으로써 eUICC와의 통신을 보호하는 기능(방화벽 기능) 등이다.

[70] SM-SR 데이터베이스는 eUICC 벤더와 장치(M2M 단말 등) 벤더 및 잠재적으로 MNO에 의하여 제공되며, SM-SR 메시 네트워크를 통해서 MNO에 의하여 사용될 수 있다.

[71] 신뢰 서클(Circle of trust)은 프로비저닝 프로파일 전달 동안 엔드-투-엔드 시큐리티 링크를 가능하게 하며, SM-SR은 프로비저닝 프로파일의 안전한 라우팅 및 eUICC 디스커버리를 위하여 신뢰 서클을 공유한다. MNO는 신뢰 써클내의 SM-SR 및 SM-DP 엔터티와 링크될 수 있으며, 자체적으로 이런 기능을 제공할 수도 있을 것이다. 고객과 관련된 MNO의 계약상 및 법률상 의무를 어기지 않고, eUICC의 불법적인 사용(클로닝, 크레덴셜의 불법 사용, 서비스 거부, 불법적인 MNO 컨텍스트 변경 등)을 방지하기 위하여, eUICC와 MNO 크레덴셜 사이의 안전한 엔드-투-엔드 링크가 필요하다.

[72] 즉, 도 1에서 110은 SM들끼리, 더 구체적으로는 SM-SR 멤버 사이에 형성되는 신뢰 서클을 나타내고, 120은 MNO 파트너들의 신뢰 서클이며, 130은 엔드투엔드 신뢰 링크를 도시한다.

[73] 도 2는 SM 분리 환경에서 SM-SR 및 SM-DP가 시스템에 위치하는 구성을 도시한다.

[74] 도 2와 같이, SM은 eUICC와 관련된 여러 프로파일(MNO의 오퍼레이션 프로파일, 프로비저닝 프로파일 등)을 안전하게 준비하는 SM-DP와, 그를 라우팅하기 위한 SM-SR로 구분되며, SM-SR은 다른 여러 SM-SR과 신뢰관계로 연동될 수 있고, SM-DP는 MNO 시스템에 연동되어 있다.

[75] 물론, SM-DP와 MNO 시스템의 배치는 도 2와 다르게 구현될 수 있다. (즉, SM-DP가 SM-SR과 연동되고, MNO 시스템이 SM-DP와 연동될 수 있다)

[76] 도 3은 본 발명이 적용되는 시스템에서 제1차 가입에 해당되는 프로비저닝 과정의 전체 흐름도이다.

[77] 프로비저닝 과정에서, eUICC는 기기 식별 정보 (IMEI 등)와 eUICC 식별 정보

Petitioner Samsung Ex-1038, 0323

(eICCid 등)를 포함하는 활성화 요청을 MNO로 전송한다.(Request activation; S310) 그런 다음, S320단계에서 MNO와 eUICC 사이에는 eUICC 상태 요청 및 기술적 능력 제어 요청/확인이 수행된다.(eUICC status request 및 technical capability control; S320)

[78] 또한, 도시하지는 않았지만, 상기 S320 단계에서는 아래에서 설명할 바와 같이, eUICC가 자신의 공개키(PK) 또는 프로파일 접근 크레덴셜 정보인 PKI 키정보(키 생성 알고리즘, 키 길이, 키 생성 방식 등)를 해당 MNO 시스템 또는 SM-SR로 제공하는 과정이 포함될 수 있다.

[79] S330단계에서 MNO는 SM-SR과 사이에서 eUICC 아이덴터티 검증과, 장치(eUICC)에 대한 정보를 수집한다(eUICC identity verification 및 collect information about device). S330단계에서, MNO는 본 발명의 일 실시예에 의하여 해당 eUICC에 대한 암호화 키, 구체적으로는 eUICC에 대응되는 공개키를 SM-SR로부터 획득할 수 있다.

[80] 이러한 공개키의 획득은 정적(static) 또는 동적(Dynamic)으로 이루어질 수 있는바, 정적으로 이루어지는 경우 eUICC 제조시에 이미 해당 eUICC 내부적으로, 세부적으로는 eUICC 내의 암호 연산 프로세서 (CCP 등)를 통해 공개키와 비밀키가 생성되어 eUICC에는 비밀키가 저장되고, 공개키는 모든 SM-SR이 공유함으로써 특정한 eUICC에 대한 공개키를 인식할 수 있도록 하고, MNO로부터 요청이 있는 경우 SM-SR은 해당되는 eUICC에 대한 공개키를 MNO로 전달하는 방식이다.

[81] 동적인 암호키 획득방법은 아래에서 도 8 및 도 9와 관련하여 설명할 바와 같이, MNO로부터 요청(특정 eUICC 식별정보 포함)이 있는 경우, SM-SR은 해당되는 eUICC에게 공개키 전송을 요청하고, 해당 eUICC는 eUICC 탑재 단말 내의 발급 처리 모듈(이 용어에 한정되지 않으며, 통신모듈, 프로비저닝 모듈, 발급 모듈, 개통 모듈 등으로 칭할 수 있으며, eUICC 프로비저닝을 위한 eUICC 탑재 단말 외부와의 통신 및 프로비저닝 관리의 역할을 수행함) 또는 eUICC 내의 보안모듈(암호키 생성 모듈, 암호키 처리 모듈, Security Policy 모듈, Credential Manager, Profile Manager 등 eUICC 내의 암호키 생성 및 암호키를 활용한 보안 연산을 수행하는 모듈)을 이용하여 공개키를 생성한 후 SM-SR로 전달하는 방식으로 수행될 수 있다. 이에 대해서는 아래에서 더 상세하게 설명한다.

[82] 여기서, eUICC 내에 탑재되는 보안모듈은 eUICC 제작 단계 또는 그 이후 eUICC 정책에 따라 eUICC 내에 공통적으로 1개가 설치될 수 있으며, eUICC 정책 및 각 MNO 정책에 따라 각 MNO 별로 여러 개가 설치될 수 있다.

[83] 해당 eUICC의 공개키(암호키)를 획득한 MNO는 SM-DP를 통해서 MNO에 맞는 새로운 eUICC 프로파일을 생성하고 그 프로파일을 획득한 eUICC 공개키(암호키)로 암호화한 후 MNO로 전달한다.(1차 암호화, S340 단계) 이때, 인증성(Authenticity)을 제공하기 위해 SM-DP는 자신의 개인키로 추가적인 전자서명을 생성할 수 있다. 즉, S340 단계에서 SM-DP는 인증을 위한 자신의

Petitioner Samsung Ex-1038, 0324

개인키 또는 비밀키로 프로파일을 전자서명(Sign)할 수 있다.

[84] 다음으로, MNO는 1차 암호화된 (eUICC) 프로파일을 SM-SR로 전달한 후 2차 암호화를 요청하면, SM-SR은 이미 저장하고 있는 eUICC 관리키(eUICC OTA 키, GP ISD 키 등)를 이용하여 eUICC 프로파일을 2차 암호화하여 MNO로 전달한다.(S350 단계)

[85] 그런 다음, MNO는 이중 암호화(Double Ciphered)된 eUICC 프로파일을 해당 eUICC로 전송한다.(S360 단계) 이때, 인증성을 제공하기 위해 SM-DP의 공개키 또는 인증서(Certification)를 함께 eUICC로 전송할 수 있다.

[86] eUICC는 이미 eUICC 관리키를 알고 있으므로 1차로 복호화한 후, 자신 공개키에 대응되는 비밀키(제조 또는 공개키 동적 생성 단계에서 이미 알고 있음)를 이용하여 2차 복호화함으로써 프로비저닝에 사용될 프로파일을 완전히 복호화 할 수 있다. 이때, eUICC는 인증서 확인 (MNO로부터 획득한 공개키에 해당되는 SM-DP로부터 생성된 eUICC 프로파일인지 확인하기 위해)을 위해 SM-DP의 공개키 (인증서의 경우, 신뢰할 수 있는 제 3의 개체로부터 해당 인증서의 유효성을 검증 받을 수 있음)로 서명 검증을 수행할 수 있다.

[87] S370 단계에서는 프로비저닝을 종료한 eUICC와 SM-SR 사이에서 상태 요청과 그에 대한 응답에 의하여 SM-SR 데이터베이스를 업데이트 한다.

[88] 이러한 각 단계에 대한 주요 구성을 추가로 설명하면 다음과 같다.

[89] S310단계에서, eUICC 식별 정보(eICCid 등)는 공개된 데이터이며 eUICC 내부에 통합 보호되어야 한다.

[90] S320, S330단계에서 상태 요청 및 기술적 가능성 제어는 eUICC 아이덴터티의 증명을 제공(신뢰할 수 있는 eUICC)하며, MNO 서비스를 위한 eUICC 특성의 적격성을 확인할 수 있어야 한다.

[91] S340~S360 단계에서는 eUICC 프로파일 생성 및 전송을 위하여 이중 암호화 메커니즘이 사용된다. 즉, SM-DP에 의하여 eUICC에 링크된 생성 프로파일은 오직 목표 eUICC에 의해서만 읽힐 수 있는 암호화 메커니즘에 의하여 암호화되며, 정당한 SM-DP로부터 생성된 프로파일임을 확인하기 위해 SM-DP에 의해 전자서명이 수행될 수 있고, SM-SR은 생성 프로파일을 eUICC 관리키로 암호화하여 전달 동안 eUICC를 인증하고 보호한다.

[92] S370 단계에서, SM-SR 데이터베이스는 가입 설치(Subscription installation)의 마무리 단계에서 업데이트 될 수 있다.

[93] 도 4는 본 발명이 적용되는 가입 변경 또는 MNO 변경 과정의 전체 흐름도이다.

[94] 전체적으로는 도 3의 프로비저닝 과정과 유사(즉, 변경 후 새로운 MNO가 도 3의 MNO에 해당)하며, 다만 새로운 MNO에 대한 프로파일 생성 전후에 새로운 MNO가 도너 MNO에게 협상 및 권리 전송 과정을 수행하는 점이 상이하다.(단계 S440')

[95] 즉, 도 4의 MNO 변경과정과 도 3의 프로비저닝 과정을 차이점은, 프로비저닝 또는 오퍼레이션 액티브 프로파일을 이용하여, 액티베이션 요청이 도너 MNO

Petitioner Samsung Ex-1038, 0325

OTA 베어러(Bearer)로 전송되고, 새로운 MNO는 OTA 또는 OTI 중 하나로 새로운 프로파일을 다운로드 하도록 SM-SR로부터 경로를 요청하는 것이다.

[96] 도 4에 의한 MNO 변경 과정을 구체적으로 설명하면 다음과 같다.

[97] MNO 변경을 위하여, eUICC는 기기 식별 정보 (IMEI 등)와 eUICC 식별 정보 (eICCid 등)를 포함하는 활성화 요청을 변경될 MNO(Receiving MNO)로 전송한다.(Request activation; S410) 그런 다음, S420단계에서 리시빙 MNO와 eUICC 사이에는 eUICC 상태 요청 및 기술적 능력 제어 요청/확인이 수행된다.(eUICC status request 및 technical capability control; S420)

[98] 또한, 도시하지는 않았지만, 상기 S420 단계에서는 아래에서 설명할 바와 같이, eUICC가 자신의 공개키(PK) 또는 프로파일 접근 크레덴셜 정보인 PKI 키정보(키 생성 알고리즘, 키 길이, 키 생성 방식 등)를 해당 MNO 시스템 또는 SM-SR로 제공하는 과정이 포함될 수 있음은 프로비저닝 과정인 S320과 동일하다.

[99] S430단계에서 리시빙 MNO는 SM-SR과 사이에서 eUICC 아이덴터티 검증과, 장치(eUICC)에 대한 정보를 수집한다(eUICC identity verification 및 collect information about device). S430단계에서, MNO는 본 발명의 일 실시예에 의하여 해당 eUICC에 대한 암호화 키, 구체적으로는 eUICC에 대응되는 공개키를 SM-SR로부터 획득할 수 있다.

[100] 이러한 공개키의 획득은 정적(static) 또는 동적(Dynamic)으로 이루어질 수 있는바, 정적으로 이루어지는 경우 eUICC 제조시에 이미 해당 eUICC 내부적으로, 세부적으로는 eUICC 내의 암호 연산 프로세서 (CCP 등)를 통해 공개키와 비밀키가 생성되어 eUICC에는 비밀키가 저장되고, 공개키는 모든 SM-SR이 공유함으로써 특정한 eUICC에 대한 공개키를 인식할 수 있도록 하고, MNO로부터 요청이 있는 경우 SM-SR은 해당되는 eUICC에 대한 공개키를 MNO로 전달하는 방식이다.

[101] 동적인 암호키 획득방법은 아래에서 도 8 및 도 9와 관련하여 설명할 바와 같이, MNO로부터 요청(특정 eUICC 식별정보 포함)이 있는 경우, SM-SR은 해당되는 eUICC에게 공개키 전송을 요청하고, 해당 eUICC는 eUICC 탑재 단말 내의 발급 처리 모듈(이 용어에 한정되지 않으며, 통신모듈, 프로비저닝 모듈, 발급 모듈, 개통 모듈 등으로 칭할 수 있으며, eUICC 프로비저닝을 위한 eUICC 탑재 단말 외부와의 통신 및 프로비저닝 관리의 역할을 수행함) 또는 eUICC 내의 보안모듈(암호키 생성 모듈, 암호키 처리 모듈, Security Policy 모듈, Credential Manager, Profile Manager 등 eUICC 내의 암호키 생성 및 암호키를 활용한 보안 연산을 수행하는 모듈)을 이용하여 공개키를 생성한 후 SM-SR로 전달하는 방식으로 수행될 수 있다. 이에 대해서는 아래에서 더 상세하게 설명한다.

[102] 여기서, eUICC 내에 탑재되는 보안모듈은 eUICC 제작 단계 또는 그 이후 eUICC 정책에 따라 eUICC 내에 공통적으로 1개가 설치될 수 있으며, eUICC 정책 및 각 MNO 정책에 따라 각 MNO 별로 여러 개가 설치될 수 있다.

[103] 해당 eUICC의 공개키(암호키)를 획득한 리시빙 MNO는 SM-DP를 통해서

Petitioner Samsung Ex-1038, 0326

MNO에 맞는 새로운 eUICC 프로파일을 생성하고 그 프로파일을 획득한 eUICC 공개키(암호키)로 암호화한 후 MNO로 전달한다.(1차 암호화, S440 단계) 이때, 인증성(Authenticity)을 제공하기 위해 SM-DP는 자신의 개인키로 추가적인 전자서명을 생성할 수 있다. 즉, S440 단계에서 SM-DP는 인증을 위한 자신의 개인키 또는 비밀키로 프로파일을 전자서명(Sign)할 수 있다.

[104] 또한, S440 단계 이전 또는 이후에 협상 및 권리 전송 단계(S440')가 수행될 수 있다. 이러한 협상 및 권리 전송 단계(S440')는 새로운 리시빙 MNO가 이전 MNO(도너 MNO)에게 해당 eUICC가 정당한지 여부와, MNO 변경에 따른 권리(정보)를 이전해 줄 것을 요청하는 등의 과정이다.

[105] 즉, S440' 단계에서는 새로운 MNO(Receiving MNO)가 가입 스위칭에 대해서 도너 MNO의 인증을 요청하며, 이러한 인증은 정책 제어 기능(Policy Control Function)에 의해서 제공될 수 있다.

[106] 다음으로, 리시빙 MNO는 1차 암호화된 (eUICC) 프로파일을 SM-SR로 전달한 후 2차 암호화를 요청하면, SM-SR은 이미 저장하고 있는 eUICC 관리키(eUICC OTA 키, GP ISD 키 등)를 이용하여 eUICC 프로파일을 2차 암호화하여 MNO로 전달한다.(S450 단계)

[107] 그런 다음, MNO는 이중 암호화(Double Ciphered)된 eUICC 프로파일을 해당 eUICC로 전송한다.(S460 단계) 이때, 인증성을 제공하기 위해 SM-DP의 공개키 또는 인증서(Certification)를 함께 eUICC로 전송할 수 있다.

[108] eUICC는 이미 eUICC 관리키를 알고 있으므로 1차로 복호화한 후, 자신 공개키에 대응되는 비밀키(제조 또는 공개키 동적 생성 단계에서 이미 알고 있음)를 이용하여 2차 복호화함으로써 MNO 변경에 사용될 프로파일을 완전히 복호화 할 수 있다. 이때, eUICC는 인증서 확인 (MNO로부터 획득한 공개키에 해당되는 SM-DP로부터 생성된 eUICC 프로파일인지 확인하기 위해)을 위해 SM-DP의 공개키 (인증서의 경우, 신뢰할 수 있는 제 3의 개체로부터 해당 인증서의 유효성을 검증 받을 수 있음)로 서명 검증을 수행할 수 있다.

[109] S470 단계에서는 프로비저닝을 종료한 eUICC와 SM-SR 사이에서 상태 요청과 그에 대한 응답에 의하여 SM-SR 데이터베이스를 업데이트 한다.

[110] 이상 도 1 내지 도 4의 방식에서는, eSIM은 단말 제조 단계에서 IC칩을 단말 회로판 상에 부착시킨 후, 소프트웨어 형태의 SIM 데이터 (개통 정보, 부가 서비스 정보 등)를 OTA (Over The Air) 또는 오프라인 (PC와의 USB 등의 기술 기반 연결)을 통해 발급하는 방식의 새로운 개념의 SIM 기술이다. eSIM에서 사용되는 IC칩은 일반적으로 하드웨어 기반의 CCP (Crypto Co-Processor)를 지원하여 하드웨어 기반의 공개키 생성을 제공하며, 이를 어플리케이션 (예, 애플릿) 기반에서 활용할 수 있는 API를 SIM 플랫폼 (예, Java Card Platform 등)에서 제공한다. Java Card Platform은 스마트카드 등에서 멀티 어플리케이션을 탑재하고 서비스를 제공할 수 있는 플랫폼 중 하나이다.

[111] SIM은 제한된 메모리 공간과 보안상의 이유로 누구나 SIM 내에

Petitioner Samsung Ex-1038, 0327

어플리케이션을 탑재해서는 안되며, 이로 인해 어플리케이션 탑재를 위한 플랫폼 이외에 SIM을 어플리케이션 탑재 및 관리를 담당하는 SIM 서비스 관리 플랫폼을 필요로 한다. SIM 서비스 관리 플랫폼은 관리키를 통한 인증 및 보안을 통해 SIM 메모리 영역에 데이터를 발급하며, GlobalPlatform과 ETSI TS 102.226의 RFM (Remote File Management) 및 RAM (Remote Application Management)은 이와 같은 SIM 서비스 관리 플랫폼의 표준 기술이다.

[112] eSIM 환경에서 중요한 요소 중의 하나인 SM은 eSIM은 원격으로 관리키를 통해 통신 및 부가 서비스 데이터를 발급하는 역할을 수행한다. GSMA에서는 SM의 역할을 SM-DP와 SM-SR로 분류하였다. SM-DP는 프로파일 (IMSI, K, OPc, 부가 서비스 데이터 등)를 안전하게 빌드하여 Credential Package 형태로 만드는 역할을 수행하며, SM-SR은 SM-DP가 생성한 Credential Package를 OTA 또는 GP SCP (Secure Communication Protocol)과 같은 SIM 원격 관리 기술을 통해 eSIM에 안전하게 다운로드하는 역할을 수행한다. 그리고 GSMA는 아래 그림의 "Circle of Trust"라는 구조를 제안하여 각 유사 개체들간 신뢰 관계의 중첩을 통해 MNO와 eSIM 간의 End-to-End 신뢰 관계를 구축한다는 개념을 제안하였다. 즉, MNO는 SM1과, SM1은 SM4, SM4는 eSIM과 신뢰관계를 형성하여, 이를 통해 MNO와 eSIM 간의 신뢰관계를 형성한다는 개념이다

[113] eSIM은 SM 등의 외부 개체로부터 프로파일을 소프트웨어적으로 발급함으로써 통신 및 부가 서비스를 제공한다. 하지만, 이 프로파일 종류 정보 (예, Operational Profile, Provisioning Profile, PCF (Policy Control Function, VAS (Value-Added Service) Profile 등), 현재 활성화 (Active) 된 프로파일의 종류 및 식별 정보 (예, 프로파일 ID 등), eSIM 내에 탑재된 프로파일 리스트 등의 관리 정보를 제공하고 활용하는 방식은 명확하지 않다.

[114] 따라서, 이하에서는, 본 발명의 실시예에 따른 eSIM 내 프로파일을 관리하는 방법과 그 활용 방안에 대하여 설명한다. 단, 이하에서는, 내장 SIM(eSIM) 또는 내장 UICC(eUICC)로 불릴 수 있는 내장형 타입의 스마트 카드를 eUICC로 통일하여 기재한다.

[115] 도 5는 본 발명의 실시예에 따른 프로파일 관리 방법을 위한 기본적인 구조를 나타낸 도면이다.

[116] 도 5를 참조하면, 본 발명의 실시예에 따른 프로파일 관리 방법은, MNO(Mobile Network Operator), SM(Subscription Manager)과 연동되는 eUICC(510) 내 프로파일 관리 방법에 관한 것으로서, eUICC(510)가 활성화된 프로파일의 종류에 대한 정보와 프로파일 리스트에 대한 정보 등 중 하나 이상을 프로파일 활용에 필요한 관리 정보로서 외부 엔티티(External Entity)로 제공하는 단계(S502) 등을 포함한다.

[117] 여기서, 외부 엔티티는, eUICC(510)를 탑재하는 eUICC 탑재 기기(500), MNO 및 SM 등 중 하나일 수 있으나, 도 5에서는 설명의 편의를 위해, eUICC(510)를 탑재하는 eUICC 탑재 기기(500)가 외부 엔티티인 것으로 가정하여

Petitioner Samsung Ex-1038, 0328

도시하였으며, 이하 설명에서도, eUICC(510)가 프로파일 활용에 필요한 관리 정보를 eUICC 탑재 기기(500)로 제공하는 것으로 설명한다.

[118] 본 명세서에서 "프로파일(Profile)"은 eUICC(510) 내에 파일 구조(File Structure), 데이터, 애플리케이션(예: 애플릿 등) 등의 조합을 의미할 수 있으며, 통신 및 부가 서비스 등을 위한 프로파일 또는 이와 유사한 형태의 정보들을 의미할 수 있다.

[119] 전술한 바와 같이, eUICC(510)는, 활성화된 프로파일의 종류에 대한 정보와 프로파일 리스트에 대한 정보 등 중 하나 이상을 프로파일 활용에 필요한 관리 정보로서 외부 엔티티(500)로 제공하는데, 프로파일 활용에 필요한 관리 정보로서, 프로파일 식별정보(예: 프로파일 ID 등) 및 프로파일 설명정보(예: 통신사 A의 LTE 프로파일, 통신사 A의 3G 프로파일 등) 등 중 하나 이상을 더 제공할 수 있다.

[120] 전술한 바와 같이, eUICC(510)가 외부 엔티티로 제공하는 "관리 정보"는, 활성화된 프로파일에 대한 종류정보, 식별정보, 리스트정보, 설명정보 등일 수 있는데, 활성화된 프로파일뿐만 아니라, eUICC(510)에 탑재된 모든 또는 일부 프로파일에 대한 종류정보, 식별정보, 리스트정보, 설명정보 등일 수도 있다.

[121] 위와 같은 관리 정보는, eUICC(510) 내에 프로파일 형태로 저장되며, 접근 제어에 따라 접근될 수 있다.

[122] 또한, 이러한 관리 정보는, 현재의 SIM 기술을 기준으로 TLV(Type Length Value) 형태로 된 파일 구조를 가질 수 있으며, 또는, EF 형태 및 애플릿 등의 애플리케이션 형태로 저장될 수 있다.

[123] 또한, 이러한 관리 정보는, 보안키 및 PIN(Personal Identification Number) 등 중 하나 이상을 통한 접근 제어에 의해 접근되어 관리될 수 있으며, 이에, SM(SM-SR, SM-DP 등), MNO 등 중 하나 이상을 포함하는 인가된 개체에 의해서만 수정(Update)되거나 활성화(Activate) 또는 비활성화(Deactivate) 될 수 있다. 단, 관리 정보는 외부 개체에 의해 자유롭게 읽힐 수는 있다. 물론, eUICC(510) 보안 정책에 따라서 접근 권한은 상이할 수 있다.

[124] 본 명세서에서 관리 정보는, eUICC(510) 내의 프로파일 정보를 관리하는 관리 프로파일(511)을 통해 관리될 수 있다. 여기서, 관리 프로파일(511)은, 일 예로, PCF(Policy Control Function)를 위한 프로파일, General Profile, Common Profile, Administration Profile, Administrative Profile, Information Profile 등일 수 있다.

[125] 도 5에 도시된 바와 같이, 본 발명의 실시예에 따른 프로파일 관리 방법을 위한 기본적인 구조는, eUICC(510) 내의 프로파일 정보를 관리하는 관리 프로파일(511)과, eUICC 탑재 기기(500)로 구성될 수 있다.

[126] S502 단계에서, eUICC(510)가 활성화된 프로파일의 종류에 대한 정보와 프로파일 리스트에 대한 정보 등 중 하나 이상을 프로파일 활용에 필요한 관리 정보로서 eUICC 탑재 기기(500)로 제공하기 위해서, eUICC(510)는, eUICC 탑재 기기(500)로부터의 어떠한 요청 수신 없이 관리 정보를 바로 제공할 수도 있고,

Petitioner Samsung Ex-1038, 0329

eUICC 탑재 기기(500)로부터 관리 정보 요청을 수신한 이후, 관리 정보 요청에 대한 응답으로서 관리 정보를 제공할 수도 있다.

[127] 도 5는 관리 정보의 제공이 요청-응답 과정을 통해 이루어지는 것에 대하여 도시한 것으로서, 도 5에 도시된 바와 같이, 관리 정보의 제공이 요청-응답 과정을 통해 이루어진다면, 관리 정보 제공이 이루어지는 S502 단계 이전에, eUICC(510) 내 관리 프로파일(511)이 외부 엔티티(예: eUICC 탑재 기기(500) 등)로부터 관리 정보 요청을 수신하는 단계(S500)가 수행될 수 있다.

[128] 이하에서는, 본 발명의 실시예에 따른 프로파일 관리 방법과 관련하여, eUICC 탑재 기기(500)에 대하여, 도 6을 참조하여, 더욱 상세하게 설명한다.

[129] 도 6은 본 발명의 실시예에 따른 eUICC 탑재 기기(500)에 대한 블록도이다.

[130] 도 6에 도시된 본 발명의 실시예에 따른 eUICC 탑재 기기(500)는, MNO(Mobile Network Operator), SM(Subscription Manager)과 연동하는 eUICC(510)를 포함하는 기기이다.

[131] 도 6을 참조하면, 본 발명의 실시예에 따른 eUICC 탑재 기기(500)는, 활성화된 프로파일의 종류에 대한 정보와 프로파일 리스트에 대한 정보 등 중 하나 이상을 프로파일 활용에 필요한 관리 정보로서 eUICC(510)로부터 획득하는 관리 정보 획득부(610) 등을 포함할 수 있다.

[132] 전술한 관리 정보 획득부(610)는, 프로파일 활용에 필요한 관리 정보로서, 활성화된 프로파일의 종류에 대한 정보와 프로파일 리스트에 대한 정보 등 중 하나 이상 이외에도, 활성화된 프로파일에 대한 프로파일 식별정보 및 프로파일 설명정보 등 중 하나 이상을 관리 정보로서 더 획득할 수 있다.

[133] 또한, 관리 정보 획득부(610)는, 프로파일 활용에 필요한 관리 정보로서, 활성화된 프로파일뿐 아니라, eUICC(510)에 탑재된 모든 또는 일부의 프로파일에 대한 종류, 리스트, 식별정보 및 설명정보 등을 획득할 수도 있다.

[134] 한편, 도 6에 도시된 바와 같이, 본 발명의 실시예에 따른 eUICC 탑재 기기(500)는, 프로파일 리스트를 표시하는 프로파일 리스트 표시부(620)와, 프로파일 리스트 중에서 사용자 등에 의해 선택된 프로파일을 토대로 MNO와 망 인증을 진행하는 망 인증부(630)와, 망 인증 완료 후, MNO와 연동하여 관리 프로파일(511)이 활성화된 프로파일을 기준으로 갱신되도록 하는 관리 프로파일 갱신부(640) 등을 더 포함할 수도 있다.

[135] 이하에서, 도 6에서와 같은 구성을 가질 수 있는 eUICC 탑재 기기(500) 내에 내장형으로 탑재되는 eUICC(510)에 대하여 도 7을 참조하여 더욱 상세하게 설명한다.

[136] 도 7은 본 발명의 실시예에 따른 eUICC(510)에 대한 블록도이다.

[137] 도 7을 참조하면, 본 발명의 실시예에 따른 eUICC(510)는, MNO(Mobile Network Operator), SM(Subscription Manager)와 연동하는 내장 UICC(eUICC: embedded Universal Integrated Circuit Card)로서, 활성화된 프로파일의 종류에 대한 정보와 프로파일 리스트에 대한 정보 등 중 하나 이상을 프로파일 활용에

Petitioner Samsung Ex-1038, 0330

필요한 관리 정보로서 외부 엔티티(External Entity)로 제공하는 관리 정보 제공 모듈(710) 등을 포함할 수 있다.

[138] 여기서, 외부 엔티티는, eUICC 탑재 기기(500), MNO 및 SM 등 중 하나일 수 있으나, 설명의 편의를 위해, eUICC 탑재 기기(500)가 외부 엔티티인 것으로 가정하여 설명한다.

[139] 전술한 관리 정보 제공 모듈(710)은, 일 예로, eUICC(510) 내 관리 프로파일(511)일 수 있으며, 경우에 따라서는, 관리 프로파일(511)과 같은 프로파일 형태가 아니라, 프로파일 형태와는 구별되는 eUICC(510) 내 논리적인 엔티티(Logical Entity)로서의 프로파일 매니저(Profile Manager)일 수도 있다.

[140] 한편, 도 7을 참조하면, 본 발명의 실시예에 따른 eUICC(510)는, 외부 엔티티로서 eUICC 탑재 기기(500)로 프로파일 활용에 필요한 관리 정보로서 프로파일 리스트를 제공한 이후, 프로파일 리스트에서 선택된 프로파일을 토대로 MNO와의 망 인증이 진행되도록 하는 망 인증 모듈(720)과, MNO와 연동하여 활성화된 프로파일을 기준으로 관리 프로파일(511)이 갱신되도록 하는 관리 프로파일 갱신 모듈(730) 등을 더 포함할 수도 있다.

[141] 위에서 언급한 관리 정보는, 전술한 바와 같이, eUICC(510) 내 탑재된 또는 활성화된 프로파일에 대한 종류정보, 식별정보, 리스트정보 및 설명정보 등 중 하나 이상을 포함할 수 있다.

[142] 이러한 관리 정보는, TLV(Type Length Value) 형태로 된 파일 구조를 갖거나, 애플리케이션 형태의 파일 구조를 가질 수 있다.

[143] 또한, 이러한 관리 정보는, 보안키 및 PIN(Personal Identification Number) 등 중 하나 이상을 통한 접근 제어에 의해 접근되어 관리될 수 있다. 이에, 관리 정보는 MNO 및 SM 등 중 하나 이상을 포함하는 인가된 개체에 의해서 수정되거나 활성화되거나 비활성화될 수 있다.

[144] 이하에서, 이상에서 설명한 프로파일 관리 방법의 활용 방안에 대한 예를 설명한다. 이러한 활용 방안의 예에서, eUICC(510)는 프로파일 리스트에 대한 정보를 eUICC 탑재 기기(500)로 제공하는 것으로 가정한다.

[145] 도 8은 본 발명의 실시예에 따른 프로파일 관리 방법의 활용 방안에 대한 흐름도이다.

[146] 도 8을 참조하면, 본 발명의 실시예에 따른 MNO(800)와 연동되는 내장 UICC(eUICC: embedded Universal Integrated Circuit Card) 내 프로파일 관리 방법은, 프로파일 리스트 제공 단계(S800), 프로파일 리스트의 표시 및 사용자 선택 단계(S802), 망 인증 진행 단계(S804) 및 관리 프로파일 갱신 단계(S806) 등을 포함한다.

[147] - 프로파일 리스트 제공 단계(S800): eUICC(510)가 프로파일 리스트를 eUICC 탑재 기기(500)로 제공한다. 이때, eUICC(510)는, 프로파일 활용에 필요한 관리 정보로서 프로파일 리스트에 대한 요청을 eUICC 탑재 기기(500)로부터 수신하고, 요청에 대한 응답으로서 프로파일 리스트를 eUICC 탑재 기기(500)로

Petitioner Samsung Ex-1038, 0331

송신할 수 있다.

[148] - 프로파일 리스트의 표시 및 사용자 선택 단계(S802): eUICC 탑재 기기(500)는, eUICC(510)로부터 프로파일 리스트를 수신하여, 수신한 프로파일 리스트를 표시하고, 표시된 프로파일 리스트에서 사용자에 의해 선택된 하나의 프로파일에 대한 선택 정보를 입력받을 수 있다.

[149] 이때, eUICC 탑재 기기(500)는, 사용자가 선택한 프로파일에 대한 선택 정보를 MNO(800) 또는 eUICC(510)로 제공해줄 수 있다.

[150] - 망 인증 진행 단계(S804): NNO(800)는, eUICC(510)에서 제공된 프로파일 리스트에서 사용자 등에 의해 선택된 프로파일을 토대로 eUICC 탑재 기기(500)와 망 인증을 진행한다.

[151] - 관리 프로파일 갱신 단계(S806): NNO(800)는, 망 인증 완료 후, eUICC(510) 내에서 프로파일 리스트를 관리하는 관리 프로파일(511)을 활성화된 프로파일을 기준으로 갱신한다.

[152] 이때, NNO(800)는, SM(SM-SR 등)과 연동하여 eUICC(510) 내에서 프로파일 리스트를 관리하는 관리 프로파일(511)을 활성화된 프로파일을 기준으로 갱신할 수 있다.

[153] 한편, MNO(800)가 eUICC(510) 내 신규 프로파일이 생기거나 기존 프로파일이 삭제되면, 관리 프로파일을 eUICC 내 프로파일 현황에 맞게 갱신할 수도 있다.

[154] 이상에서 설명한 바와 같은 본 발명을 이용하면, eUICC 탑재 기기(500)는, eUICC(510) 내에 활성화된 프로파일 종류와 식별정보 그리고 탑재된 프로파일 리스트를 알 수 있다.

[155] 이를 통해, eUICC(510) 내의 복수 개의 프로파일이 탑재되거나 활성화되었을 때, 본 발명의 관리 프로파일을 통해 eUICC 탑재 기기(500)의 동작 및 외부 시스템과의 연동을 효율적이고 편리하게 구체화할 수는 기본 정보 활용이 쉽고 편리해지는 효과가 있다.

[156] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 발명에 개시된 실시 예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시 예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

[157] **CROSS-REFERENCE TO RELATED APPLICATION**

[158] 본 특허출원은 2011년 9월 28일 한국에 출원한 특허출원번호 제 10-2011-0097901 호에 대해 미국 특허법 119(a)조 (35 U.S.C § 119(a))에 따라 우선권을 주장하며, 그 모든 내용은 참고문헌으로 본 특허출원에 병합된다. 아울러, 본 특허출원은 미국 이외에 국가에 대해서도 위와 동일한 이유로

Petitioner Samsung Ex-1038, 0332

우선권을 주장하면 그 모든 내용은 참고문헌으로 본 특허출원에 병합된다.

청구범위

[청구항 1] MNO(Mobile Network Operator), SM(Subscription Manager)과 연동되는 내장 UICC(eUICC: embedded Universal Integrated Circuit Card) 내 프로파일 관리 방법으로서,
상기 eUICC가 활성화된 프로파일의 종류에 대한 정보와 프로파일 리스트에 대한 정보 중 하나 이상을 외부 엔티티(External Entity)로 제공하는 단계를 포함하는 프로파일 관리 방법.

[청구항 2] 제1항에 있어서,
상기 제공하는 단계에서, 상기 eUICC는,
상기 활성화된 프로파일의 종류에 대한 정보와 상기 프로파일 리스트에 대한 정보 중 하나 이상을 프로파일 활용에 필요한 관리 정보로서 상기 외부 엔티티로 제공하되, 프로파일 식별정보 및 프로파일 설명정보 중 하나 이상을 상기 관리 정보로서 더 제공하는 것을 특징으로 하는 프로파일 관리 방법.

[청구항 3] 제2항에 있어서,
상기 관리 정보는,
상기 MNO 및 상기 SM 중 하나 이상을 포함하는 인가된 개체에 의해서 수정되거나 활성화되거나 비활성화되는 것을 특징으로 하는 프로파일 관리 방법.

[청구항 4] 제2항에 있어서,
상기 관리 정보는,
상기 eUICC 내 관리 프로파일을 통해 관리되는 것을 특징으로 하는 프로파일 관리 방법.

[청구항 5] 제4항에 있어서,
상기 제공하는 단계 이전에,
상기 관리 프로파일이 상기 외부 엔티티로부터 관리 정보 요청을 수신하는 단계를 더 포함하는 프로파일 관리 방법.

[청구항 6] 제1항에 있어서,
상기 외부 엔티티는,
상기 eUICC를 탑재하는 eUICC 탑재 기기, 상기 MNO 및 상기 SM 중 하나인 것을 특징으로 하는 프로파일 관리 방법.

[청구항 7] MNO(Mobile Network Operator), SM(Subscription Manager)와 연동하는 내장 UICC(eUICC: embedded Universal Integrated Circuit Card)로서,
상기 eUICC는 활성화된 프로파일의 종류에 대한 정보와 프로파일 리스트에 대한 정보 중 하나 이상을 외부 엔티티(External Entity)로 제공하는 관리 정보 제공 모듈을 포함하는 eUICC.

Petitioner Samsung Ex-1038, 0334

[청구항 8] 제7항에 있어서,
상기 관리 정보 제공 모듈은 상기 eUICC 내 관리 프로파일인 것을 특징으로 하는 eUICC.

[청구항 9] 제8항에 있어서,
상기 외부 엔티티로서 eUICC 탑재 기기로 상기 프로파일 리스트를 제공한 이후, 상기 프로파일 리스트에서 선택된 프로파일을 토대로 상기 MNO와의 망 인증이 진행되도록 하는 망 인증 모듈; 및
상기 MNO와 연동하여 활성화된 프로파일을 기준으로 상기 관리 프로파일이 갱신되도록 하는 관리 프로파일 갱신 모듈을 더 포함하는 eUICC.

[청구항 10] 제7항에 있어서,
상기 관리 정보 제공 모듈은,
상기 활성화된 프로파일의 종류에 대한 정보와 프로파일 리스트에 대한 정보 중 하나 이상을 프로파일 활용에 필요한 관리 정보로서 상기 외부 엔티티로 제공하되, 프로파일 식별정보 및 프로파일 설명정보 중 하나 이상을 상기 관리 정보로서 더 제공하는 것을 특징으로 하는 eUICC.

[청구항 11] MNO(Mobile Network Operator), SM(Subscription Manager)과 연동하는 내장 UICC(eUICC: embedded Universal Integrated Circuit Card)를 탑재하는 기기로서,
활성화된 프로파일의 종류에 대한 정보와 프로파일 리스트에 대한 정보 중 하나 이상을 상기 eUICC로부터 획득하는 관리 정보 획득부를 포함하는 eUICC 내 프로파일을 관리하는 eUICC 탑재 기기.

[청구항 12] 제11항에 있어서,
상기 관리 정보 획득부는,
상기 활성화된 프로파일의 종류에 대한 정보와 프로파일 리스트에 대한 정보 중 하나 이상을 프로파일 활용에 필요한 관리 정보로서 획득하되,
상기 관리 정보는 상기 eUICC 내 관리 프로파일을 통해 관리되는 것을 특징으로 하는 eUICC 탑재 기기.

[청구항 13] 제12항에 있어서,
상기 프로파일 리스트를 표시하는 프로파일 리스트 표시부;
상기 프로파일 리스트 중에서 선택된 프로파일을 토대로 상기 MNO와 망 인증을 진행하는 망 인증부; 및
상기 MNO와 연동하여 상기 관리 프로파일이 활성화된 프로파일을 기준으로 갱신되도록 하는 관리 프로파일 갱신부을 더

Petitioner Samsung Ex-1038, 0335

포함하는 eUICC 탑재 기기.

[청구항 14] MNO(Mobile Network Operator)와 연동되는 내장 UICC(eUICC: embedded Universal Integrated Circuit Card) 내 프로파일 관리 방법으로서,

상기 NNO가 상기 eUICC에서 제공된 프로파일 리스트에서 선택된 프로파일을 토대로 eUICC 탑재 기기와 망 인증을 진행하는 단계; 및

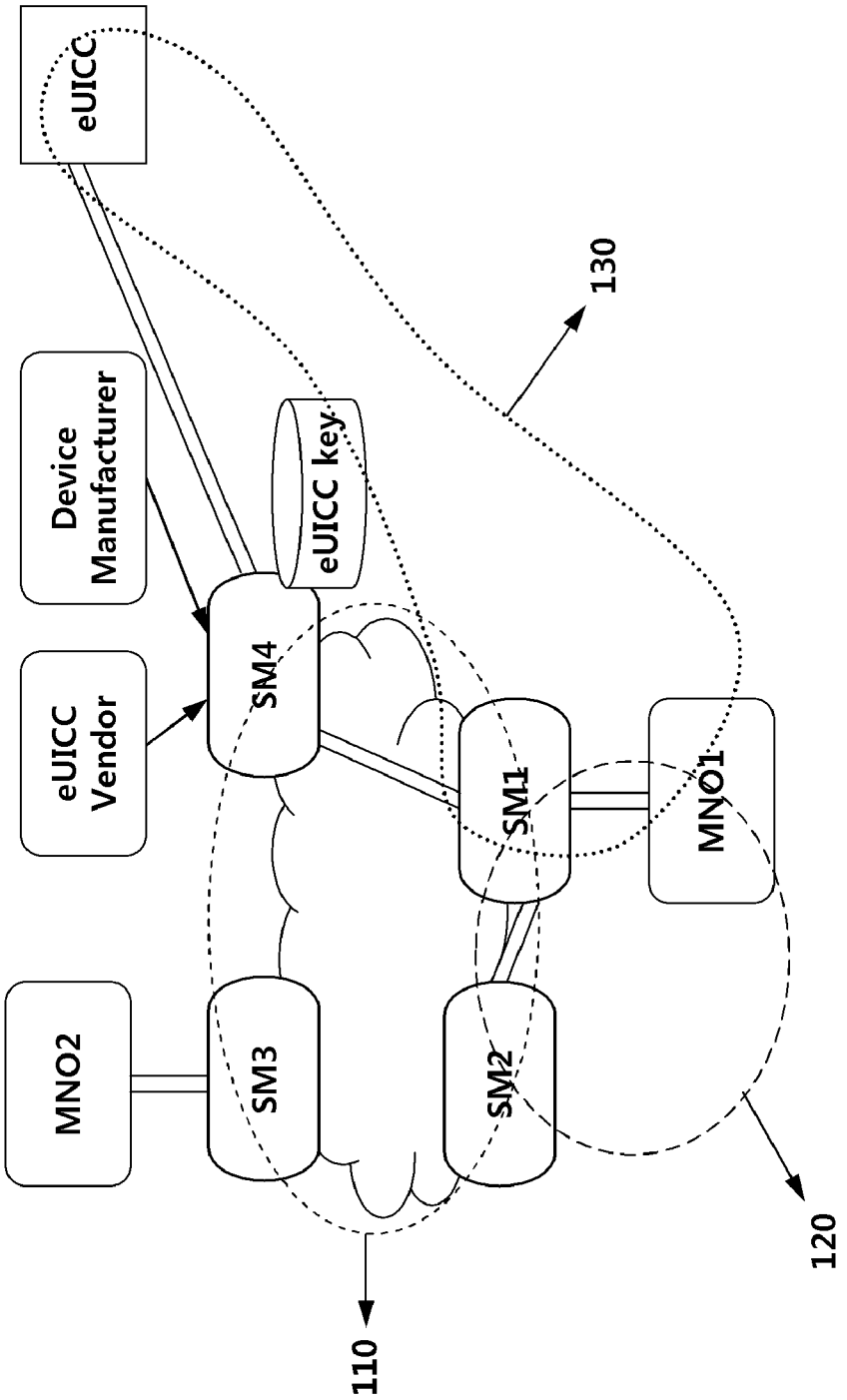
상기 MNO가 상기 eUICC 내에서 상기 프로파일 리스트를 관리하는 관리 프로파일을 활성화된 프로파일을 기준으로 갱신하는 단계를 포함하는 프로파일 관리 방법.

[청구항 15] 제14항에 있어서,

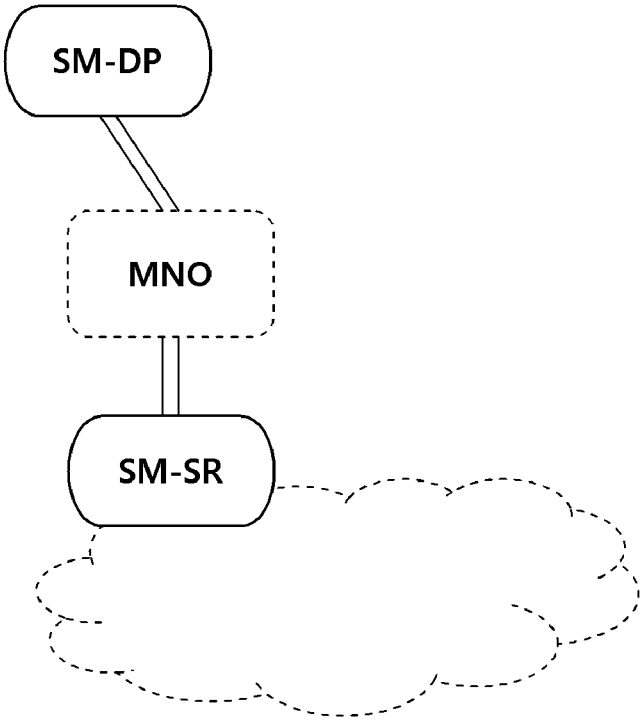
상기 MNO가 상기 eUICC 내 신규 프로파일이 생기거나 기존 프로파일이 삭제되면, 상기 관리 프로파일을 상기 eUICC 내 프로파일 현황에 맞게 갱신하는 것을 특징으로 하는 프로파일 관리 방법.

Petitioner Samsung Ex-1038, 0336

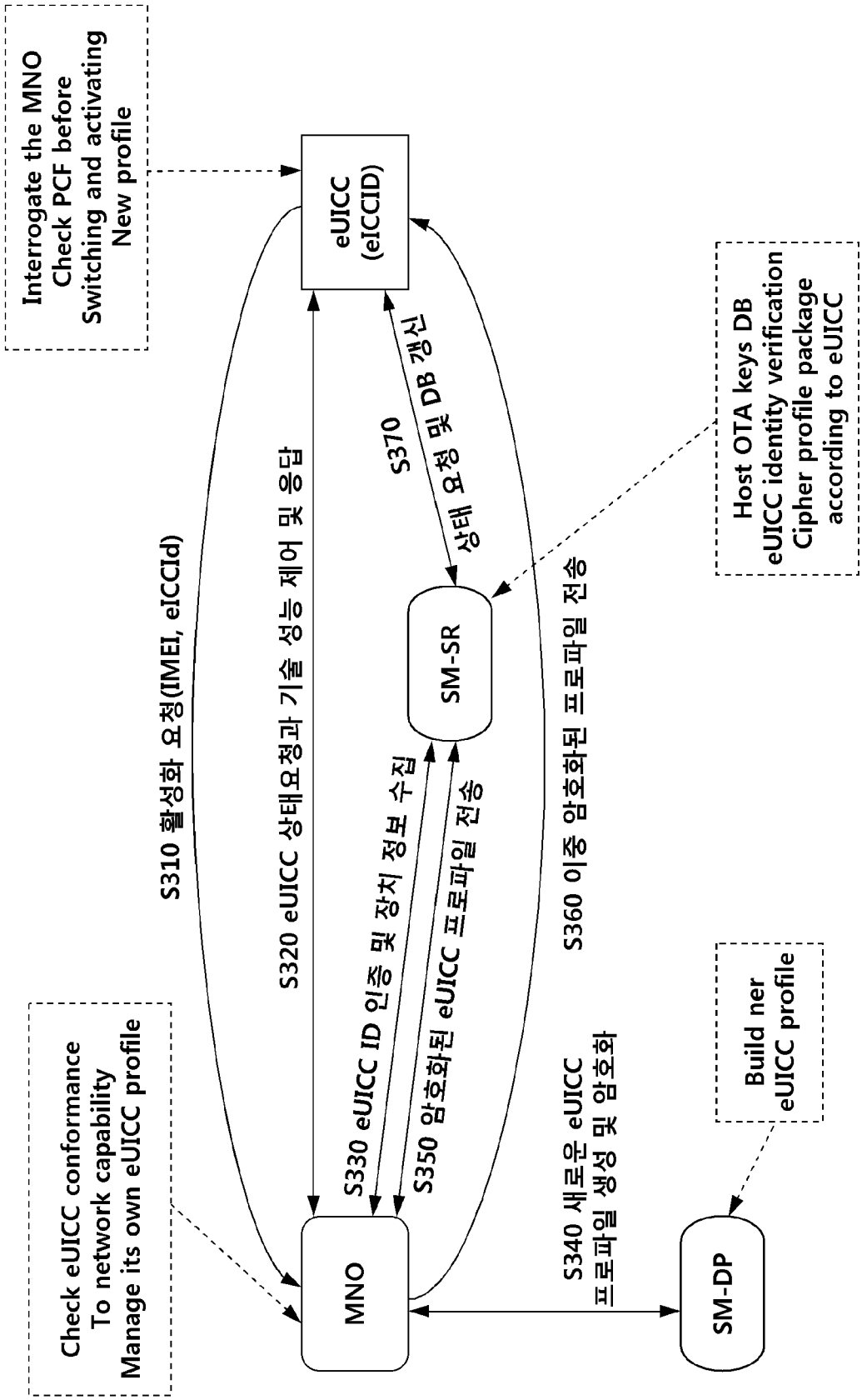
[Fig. 1]


eUICC
130
Device Manufacturer
eUICC key
eUICC Vendor
SM4
SM1
MNO1
MNO2
SM3
SM2
120
110

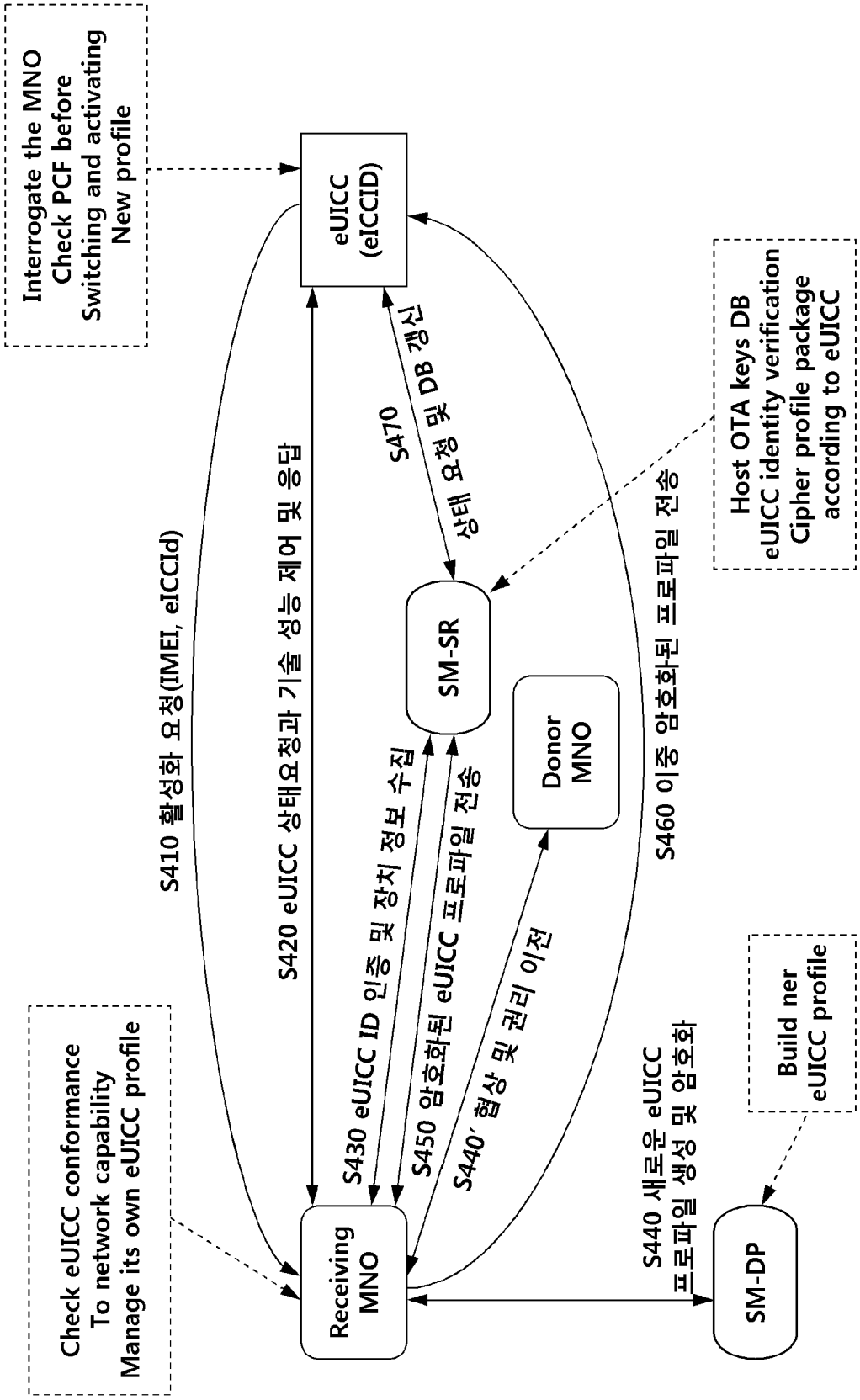
[Fig. 2]



[Fig. 3]

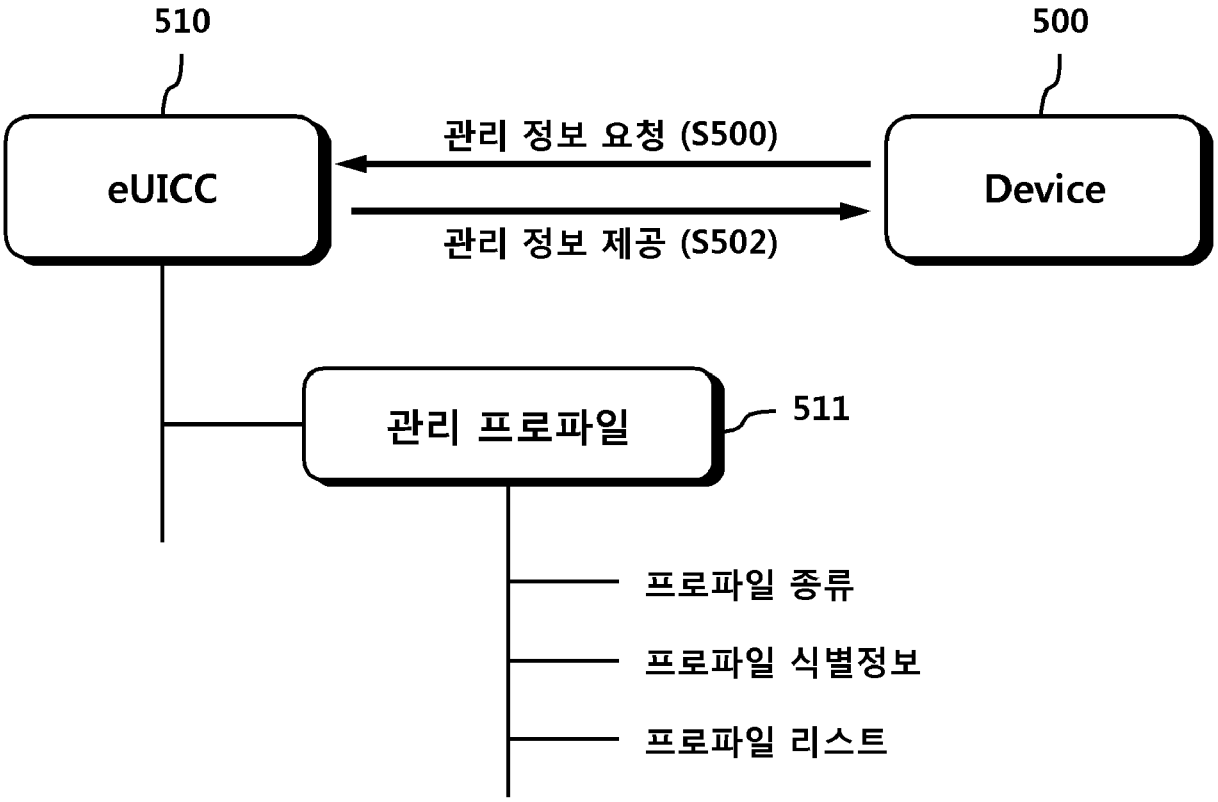

Interrogate the MNO
Check PCF before
Switching and activating
New profile
eUICC
(eICCID)
Host OTA keys DB
eUICC identity verification
Cipher profile package
according to eUICC
S310 활성화 요청(IMEI, eICCId)
S320 eUICC 상태요청과 기술 성능 제어 및 응답
S370
상태 요청 및 DB 갱신
SM-SR
S330 eUICC ID 인증 및 장치 정보 수집
S350 암호화된 eUICC 프로파일 전송
S360 이중 암호화된 프로파일 전송
Check eUICC conformance
To network capability
Manage its own eUICC profile
MNO
S340 새로운 eUICC
프로파일 생성 및 암호화
Build ner
eUICC profile
SM-DP

[Fig. 4]

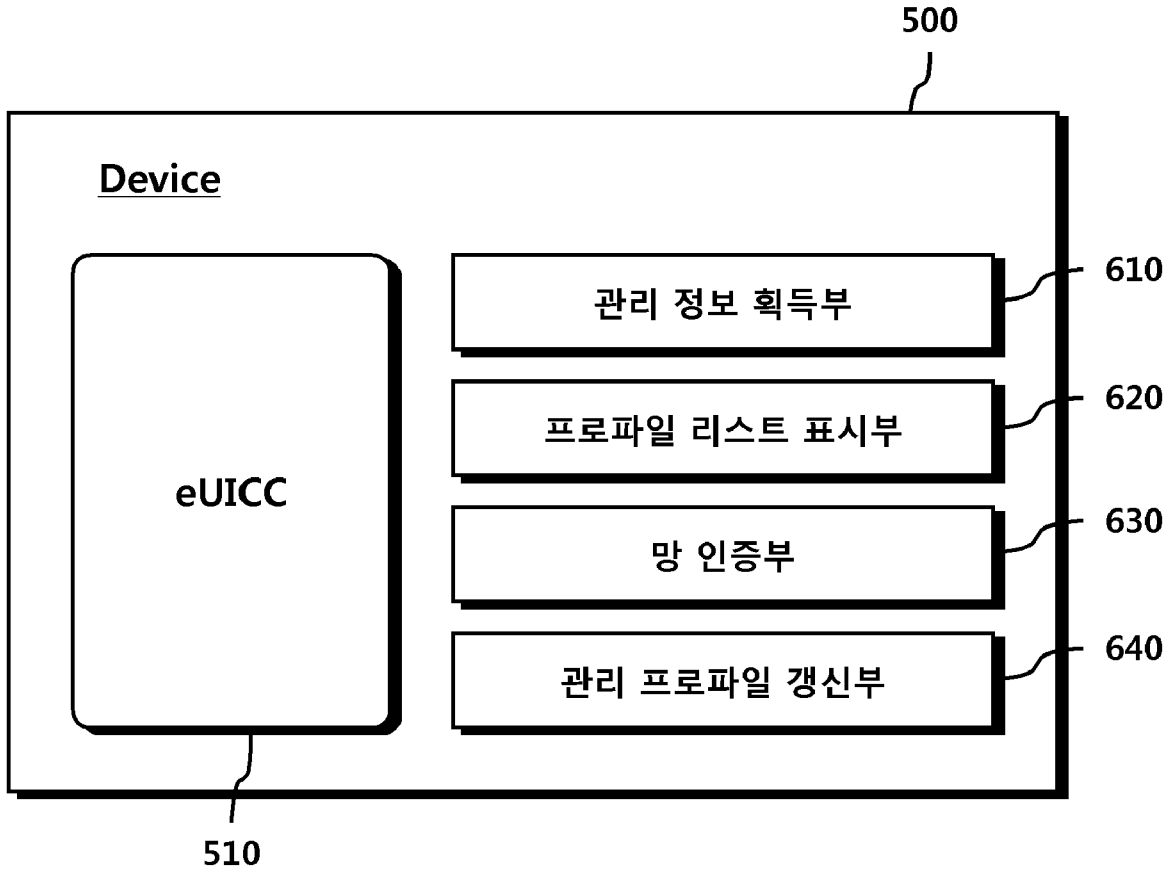


Petitioner Samsung Ex-1038, 0340

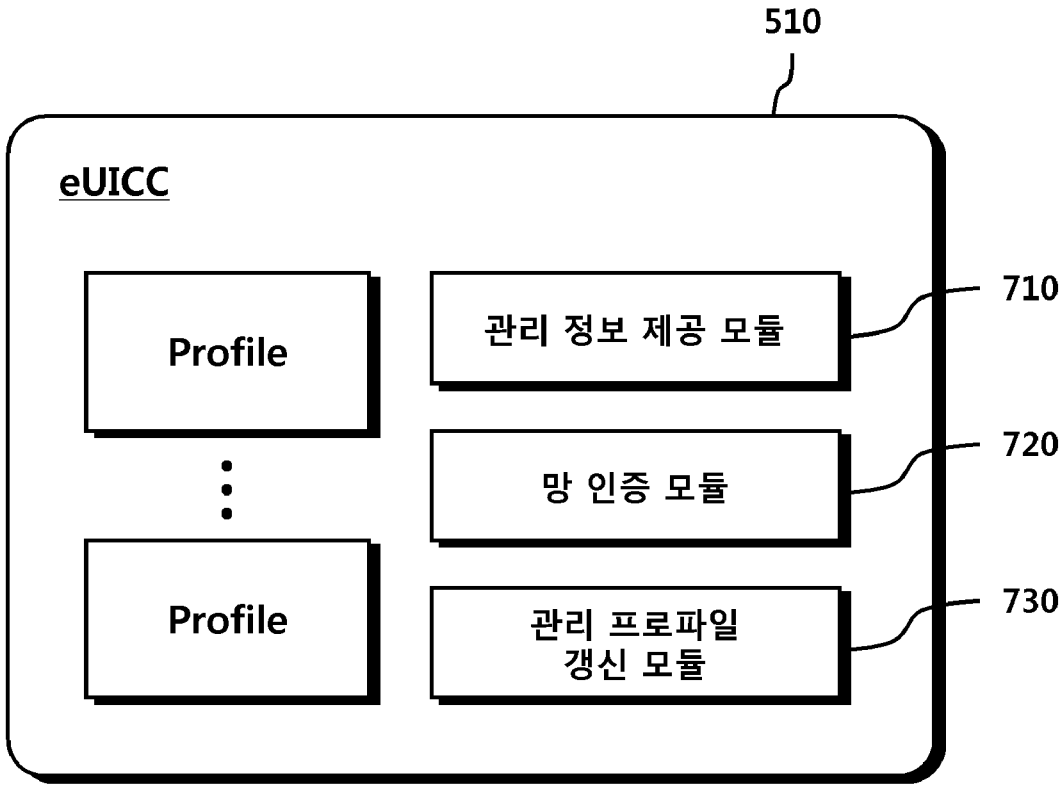
[Fig. 5]


510
500
eUICC
관리 정보 요청 (S500)
관리 정보 제공 (S502)
Device
관리 프로파일
511
프로파일 종류
프로파일 식별정보
프로파일 리스트

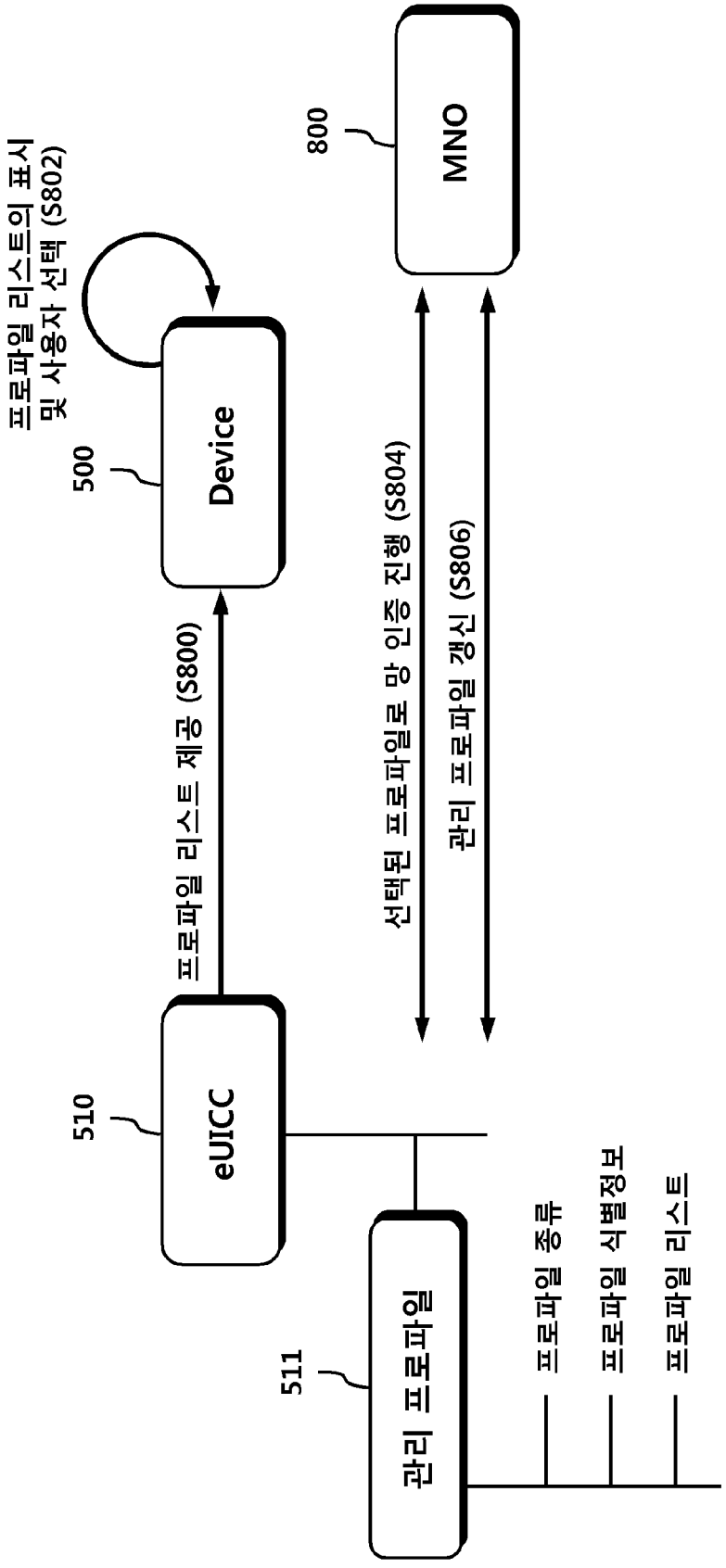
[Fig. 6]


500
Device
eUICC
관리 정보 획득부
610
프로파일 리스트 표시부
620
망 인증부
630
관리 프로파일 갱신부
640
510

[Fig. 7]


510
eUICC
Profile
Profile
관리 정보 제공 모듈
망 인증 모듈
관리 프로파일
갱신 모듈
710
720
730

[Fig. 8]


800
MNO
프로파일 리스트의 표시
및 사용자 선택 (S802)
500
Device
프로파일 리스트 제공 (S800)
선택된 프로파일로 망 인증 진행 (S804)
관리 프로파일 갱신 (S806)
510
eUICC
511
관리 프로파일
프로파일 종류
프로파일 식별정보
프로파일 리스트

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20130149996	A1	2013-06-13	King et al.	
	2	20130166915	A1	2013-06-27	Desai et al.	
	3	20130173747	A1	2013-07-04	Kim et al.	
	4	20130212637	A1	2013-08-15	Guccione et al.	
	5	20130227646	A1	2013-08-29	Haggerty et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	6	20130305345	A1	2013-11-14	Bugenhagen	
	7	20130322621	A1	2013-12-05	Yoon et al.	
	8	20130331063	A1	2013-12-12	Cormier et al.	
	9	20140003604	A1	2014-01-02	Campagna et al.	
	10	20140053241	A1	2014-02-20	Norman et al.	
	11	20140073375	A1	2014-03-13	Li et al.	
	12	20140082538	A1	2014-03-20	Nakhjiri et al.	
	13	20140082539	A1	2014-03-20	Nakhjiri et al.	
	14	20140087790	A1	2014-03-27	Babbage et al.	
	15	20140101444	A1	2014-04-10	Lee et al.	
	16	20140108801	A1	2014-04-17	McBride et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	17	20140140507	A1	2014-05-22	Park et al.	
	18	20140143826	A1	2014-05-22	Sharp et al.	
	19	20140161113	A1	2014-06-12	Cui et al.	
	20	20140165155	A1	2014-06-12	Zhang	
	21	20140192976	A1	2014-07-10	Yoon et al.	
	22	20140219447	A1	2014-08-07	Park et al.	
	23	20140219448	A1	2014-08-07	Froels et al.	
	24	20140244994	A1	2014-08-28	Yu	
	25	20140273913	A1	2014-09-18	Michel et al.	
	26	20140287725	A1	2014-09-25	Lee	
	27	20140337937	A1	2014-11-13	Truskovsky et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	28	20140351403	A1	2014-11-27	Lin et al.	
	29	20150012743	A1	2015-01-08	Holtmanns et al.	
	30	20150017910	A1	2015-01-15	Li et al.	
	31	20150071139	A1	2015-03-12	Nix	
	32	20150092590	A1	2015-04-02	Zhu et al.	
	33	20150095514	A1	2015-04-02	Yu	
	34	20150095648	A1	2015-04-02	Nix	
	35	20150113275	A1	2015-04-23	Kim et al.	
	36	20150121495	A1	2015-04-30	Gao et al.	
	37	20130231087	A1	2013-09-05	O'Leary	
	38	20130165073	A1	2013-06-27	Madsen	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	39	20130007442	A1	2013-01-03	Yinian Mao et al.	
	40	20120170451	A1	2012-07-05	Harish Viswanathan et al.	
	41	20120084568	A1	2012-04-05	Bellcet Sarikaya et al.	
	42	20120030461	A1	2012-02-02	William Daniel Willey et al.	
	43	20080307218	A1	2008-12-11	Oleg Logvinov	
	44	20110035584	A1	2011-02-10	Meyerstein et al.	
	45	20090060197	A1	2009-03-05	Taylor et al.	
	46	20150089214	A1	2015-03-26	Dupre	
	47	20140122878	A1	2014-05-01	Cho et al.	
	48	20140115335	A1	2014-04-24	Jorden et al.	
	49	20130173926	A1	2013-07-04	Morese et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

	50	20130012168	A1	2013-01-10	Rajadurai et al.	
	51	20120331298	A1	2012-12-27	Xu et al.	
	52	20120190354	A1	2012-07-26	Merrien et al.	
	53	20040221163	A1	2004-11-04	Jorgensen et al.	
	54	20090113203	A1	2009-04-30	Tsuge et al.	
	55	20150163056	A1	2015-06-11	Nix	
	56	20090217348	A1	2009-08-27	Salmela et al.	
	57	20080130879	A1	2008-06-05	Heinonen et al.	
	58	20130122864	A1	2013-05-16	Haggerty et al.	
	59	20150071139	A1	2015-03-12	Nix	
	60	20150095648	A1	2015-04-02	Nix	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Albert J. Boardman/	Date (YYYY-MM-DD)	2022-04-05
Name/Print	Albert J. Boardman	Registration Number	70,601

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

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	45395286
Application Number:	17647812
International Application Number:	
Confirmation Number:	6784
Title of Invention:	Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)
First Named Inventor/Applicant Name:	John A. Nix
Customer Number:	1912
Filer:	Albert J. Boardman/Miki Ueki
Filer Authorized By:	Albert J. Boardman
Attorney Docket Number:	63121/0213
Receipt Date:	05-APR-2022
Filing Date:	12-JAN-2022
Time Stamp:	16:06:47
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	1-IDS_Transmittal_Letter.pdf	179296 b12e40ee1c2c63e4045a1b8ab3a31580687ed7da	no	4

Warnings:

Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	2-IDS1.pdf	1174363 62a3d73fca4277e9ce06179aa69d6d9e66b1de40	no	14
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	3-IDS2.pdf	1060755 0d44ed466064be4353f88ad9c4d0d47fbfc82ea7	no	9
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Form (SB08)	4-IDS3.pdf	1075690 e8ba078cee63969cde4c2fcf64d3e45fc63afde9	no	9
Warnings:					
Information:					
5	Information Disclosure Statement (IDS) Form (SB08)	5-IDS4.pdf	1016974 3a653017e8187cd331c693753a9918677a1bd85c	no	9
Warnings:					
Information:					
6	Information Disclosure Statement (IDS) Form (SB08)	7-IDS6.pdf	1014798 6fb0b13021ac30d6150e38a872601e89504b071d	no	7
Warnings:					
Information:					
7	Information Disclosure Statement (IDS) Form (SB08)	8-IDS7.pdf	1061234 4197721a4516bc71106d39d32ddd88ea1690fb79	no	10
Warnings:					
Information:					
8	Information Disclosure Statement (IDS) Form (SB08)	9-IDS8.pdf	1091159 58f8ff02c256180549750c4a31a768b833fe65d2	no	7
Warnings:					
Information:					

9	Foreign Reference	10-FR1-KR1020130026351AI.pdf	2226973 dd48ed12997a4f7e6f308919bf08aca0c9a82ef5	no	44
Warnings:					
Information:					
10	Foreign Reference	11-FR2-WO2013048084A2.pdf	1735016 aea95ca16416aa5ec05164e0970a83ae49ba7743	no	44
Warnings:					
Information:					
11	Other reference-Patent/Application/ Search Documents	12-NPL1-21182424-EESR.pdf	129706 380c6c6d48d6cd47594cb156f03edaeaf8dedb48	no	5
Warnings:					
Information:					
12	Other reference-Patent/Application/ Search Documents	13-NPL2-21182451-EESR.pdf	130587 0534df7a3fd03d4b0069a497584b2f61521435dd	no	5
Warnings:					
Information:					
13	Other reference-Patent/Application/ Search Documents	14-NPL3-21182432-EESR.pdf	130631 ea3d255dedc0f430b65072e23ac722abdda35573	no	5
Warnings:					
Information:					
14	Non Patent Literature	15-Bender_Article.pdf	597724 c200d29e860481b29ca8fa5e4a898e1a1721c3df	no	6
Warnings:					
Information:					
15	Information Disclosure Statement (IDS) Form (SB08)	6-IDS5.pdf	1037202 e8c983ef120f7ef845299cb4530dd39ba3cf00cf	no	9
Warnings:					
Information:					
		Total Files Size (in bytes):	13662108		

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Network-1 Technologies, Inc.	Confirmation No.: 6784
Title:	Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)	
Appl. No.:	17/647,812	
Filing Date:	January 12, 2022	
Examiner:	PEARSON, David J.	
Art Unit:	2438	
Docket No.:	63121/0213	
Customer No.:	01912	

INFORMATION DISCLOSURE STATEMENT LETTER
UNDER 37 C.F.R. § 1.56

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

Sir:

In accordance with the duty of disclosure under 37 C.F.R. §1.56, the attention of the Patent and Trademark Office is hereby directed to the information item(s) listed on the attached Form PTO-SB08. Unless otherwise indicated herein, one copy of each item(s) is attached. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the item(s) be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

Reference to Related Patents and Co-Pending Applications

The below chart provides information regarding related issued patents and co-pending applications filed by the present Applicant:

Petitioner Samsung Ex-1038, 0357

Serial No.	Attorney Docket No.	Filing Date	Status
17/647,812	**63121/0213**	**2022-01-12**	**(Present Application) Pending - Case Docketed to Examiner in GAU 2022-03-19**
17/547,990	63121/0212	2021-12-10	Pending - Ready for Examination
17/304,922	63121/0209	2021-06-28	Pending - Ready for Examination
17/249,242	63121/0202	2021-02-24	Pending – Ready for Examination
16/879,325	63121/0198	2020-05-20	USP 11,082,218
16/843,107	63121/0197	2020-04-08	USP 11,283,603
16/721,153	63121/0195	2019-12-19	Non-Final Action issued on January 21, 2022
16/593,561	63121/0190	2019-10-04	USP 11,258,595
16/453,682	63121/0184	2019-06-26	USP 11,233,780
16/271,455	63121/0181	2019-02-08	USP 10,594,679
16/271,428	63121/0180	2019-02-08	USP 10,523,432
16/201,401	63121/0179	2018-11-27	USP 10,700,856
16/200,118	63121/0178	2018-11-26	USP 10,498,530
16/110,804	63121/0168	2018-08-23	USP 10,382,422
16/036,506	63121/0167	2018-07-16	USP 10,530,575
15/983,957	63121/0163	2018-05-18	USP 10,177,911
15/973,012	63121/0162	2018-05-07	USP 10,250,386
15/972,914	63121/0161	2018-05-07	USP 10,652,017
15/928,848	63121/0160	2018-03-22	USP 10,084,768
15/010,905	63121/0157	2016-01-29	USP 9,641,327
15/680,758	63121/0147	2017-08-18	USP 10,187,206
15/162,292	63121/0146	2016-05-23	USP 10,362,012
14/751,119	63121/0145	2015-06-25	USP 9,961,060
15/457,700	63121/0144	2017-03-13	USP 9,998,281
15/583,968	63121/0143	2017-05-01	USP 10,057,059
15/043,293	63121/0142	2016-02-12	USP 9,998,280
15/642,088	63121/0141	2017-07-05	USP 10,003,461
15/130,146	63121/0140	2016-04-15	USP 9,742,562
15/162,302	63121/0139	2016-05-23	USP 9,698,981
14/789,255	63121/0138	2015-07-01	USP 9,596,078
14/139,419	63121/0137	2013-12-23	USP 9,351,162
14/136,711	63121/0136	2013-12-20	USP 9,300,473
14/099,329	63121/0135	2013-12-06	USP 9,100,175

Petitioner Samsung Ex-1038, 0358

14/084,141	63121/0134	2013-11-19	USP 9,319,223
14/064,618	63121/0133	2013-10-28	USP 9,118,464
14/055,606	63121/0132	2013-10-16	USP 9,276,740
14/039,401	63121/0131	2013-09-27	USP 9,288,059
14/023,181	63121/0130	2013-09-10	USP 9,350,550
AU 2019246774	63121-0199	2019-10-08	Published on 2021-09-23
GB 1608573	63121-0151	2014-10-27	Published on 2016-08-03
GB 2100530	63121-0201	2014-10-27	Published on 2021-05-12
CA 2,965,119	63121-0152	2014-10-27	Published on 2015-05-07
HK 17101082.8	63121-0153	2014-10-27	Published on 2017-10-20
EU 14868381.6	63121-0154	2014-12-04	Published on 2017-01-04
CA 2,969,829	63121-0155	2014-12-04	Published on 2015-06-11
HK 17106540.3	63121-0156	2014-12-04	Published on 2018-01-19

The Examiner is invited to review the prosecution history of each of these applications, including the cited references of record and related office actions, as the Examiner deems appropriate.

* * * * *

This Information Disclosure Statement is being filed within three months of the filing date and before the mailing date of a first Office Action on the merits in the present application. No certification or fee is required. Applicant(s) hereby petition(s) that the Information Disclosure Statement be considered. Please charge any fee deficiency or credit any overpayment to Deposit Account No. 01-1785, under Docket No. 63121/0213.

Petitioner Samsung Ex-1038, 0359

Respectfully submitted,

AMSTER, ROTHSTEIN & EBENSTEIN LLP
Attorneys for Applicant
90 Park Avenue
New York, NY 10016
(212) 336-8000

Dated: April 5, 2022
New York, NY

By: /Albert J. Boardman/
Albert J. Boardman, Reg. No. 70,601

4876-7247-0281 v.1

Petitioner Samsung Ex-1038, 0360

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.
17/647,812	01/12/2022	John A. Nix	63121/0213	6784

1912 7590 04/14/2022

AMSTER, ROTHSTEIN & EBENSTEIN LLP
90 PARK AVENUE
NEW YORK, NY 10016

EXAMINER	
PEARSON, DAVID J	

ART UNIT	PAPER NUMBER
2438	

MAIL DATE	DELIVERY MODE
04/14/2022	PAPER

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

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

Petitioner Samsung Ex-1038, 0361

Office Action Summary	Application No. 17/647,812	Applicant(s) Nix, John A.	
	Examiner DAVID J PEARSON	Art Unit 2438	AIA (FITF) Status Yes

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 12 January 2022.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ 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.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-20 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-20 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, 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.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 12 January 2022 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ 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)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

Petitioner Samsung Ex-1038, 0362

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.

1. Instant application is a continuation of 16/593561, now U.S. Patent 11258595, which is a continuation of 16/036506, now U.S. Patent 10530575; which is a continuation of 15/583968, now U.S. Patent 10057059; which is a continuation of 15/010905, now U.S. Patent 9641327; which is a continuation of 14/055606, now U.S. Patent 9276740. Claims 1-20 have been examined.

Information Disclosure Statement

2. The information disclosure statements (IDS) submitted on 04/05/2022 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statements are being considered by the examiner.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46

USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on nonstatutory double patenting provided the reference application or patent either is shown to be commonly owned with the examined application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. See MPEP § 717.02 for applications subject to examination under the first inventor to file provisions of the AIA as explained in MPEP § 2159. See MPEP § 2146 *et seq.* for applications not subject to examination under the first inventor to file provisions of the AIA. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO Internet website contains terminal disclaimer forms which may be used. Please visit www.uspto.gov/patent/patents-forms. The filing date of the application in which the form is filed determines what form (e.g., PTO/SB/25, PTO/SB/26, PTO/AIA/25, or PTO/AIA/26) should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

3. Claims 1-2, 4-7, 9, 11, 14 and 20 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-18 of U.S. Patent No. 11258595. Although the claims at issue are not identical, they are not patentably distinct from each other because:

See chart below.

Claims 1-18 of U.S. Patent No. 11258595 contain every element of claims 1-2, 4-7, 9, 11, 14 and 20 of the instant application and as such anticipate claim of the instant application.

"A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or **anticipated by**, the earlier claim. In re Longi, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); In re Berg, 140 F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness-type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species within that genus). " ELI LILLY AND COMPANY v BARR LABORATORIES, INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001).

4. Claims 1-2 and 6-7 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-9 of U.S. Patent No. 10530575. Although the

claims at issue are not identical, they are not patentably distinct from each other because:

See chart below.

Claims 1-2 and 6-7 of U.S. Patent No. 10530575 contain every element of claims 1-7, 15 and 18 of the instant application and as such anticipate claim of the instant application.

"A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or **anticipated by**, the earlier claim. In re Longi, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); In re Berg, 140 F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness-type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species within that genus). " ELI LILLY AND COMPANY v BARR LABORATORIES, INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001).

5. Claims 1-2 and 6-7 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-9 of U.S. Patent No. 10057059. Although the claims at issue are not identical, they are not patentably distinct from each other because:

See chart below.

Claims 1-2 and 6-7 of U.S. Patent No. 10057059 contain every element of claims 1-7, 15 and 18 of the instant application and as such anticipate claim of the instant application.

"A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or **anticipated by**, the earlier claim. In re Longi, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); In re Berg, 140 F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness-type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species within that genus). " ELI LILLY AND COMPANY v BARR LABORATORIES, INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001).

Instant Application	11258595	10530575	10057059
1. A mobile device comprising: (a) at least one	Claim 1	Claim 1 (2)…memory…	Claim 1

processor; and (b) at least one computer-readable medium operatively connected to the at least one processor and having stored thereon instructions that, when executed by the at least one processor, cause the mobile device to perform a method of authentication with a wireless			(a)…module identity…

network, the method comprising:(1) storing a server public key, a module identity, cryptographic algorithms, and a pre-shared secret key, wherein the module identity comprises a permanent identifier for the mobile device and the cryptographic algorithms includes a	(a) storing...	(b) server private key... derived shared secret key...module identity (a) receiving...	(b) server public key... (c) derived shared secret key...

symmetric ciphering algorithm; (2) deriving a module private key and a corresponding module public key using the cryptographic algorithms; (3) deriving a symmetric ciphering key using (i) an elliptic curve integrated encryption scheme with the server public key and the module	(b) receiving...	(a) (ii) ...temporary module private key	(a) receiving...
	(c) deriving...	(b) generating...	(a) (ii) ...temporary module private key
			(c) generating derived secret key...

private key and (ii) an American National Standards Institute standard X-9.63 key derivation function; (4) generating a module encrypted data using the symmetric ciphering key and the symmetric ciphering algorithm, wherein the module	(d) decrypting, ...	(c) receiving....	. (c) receiving....

encrypted data includes the module identity; (5) sending a message to a server for the wireless network, the message comprising the module encrypted data and the module public key, wherein the server mutually derives the symmetric ciphering key using at least	(d) decrypting, ...	(c) receiving...	(c) receiving....

the module public key, and wherein the wireless network selects the pre-shared secret key for the mobile device using the module identity; and (6) authenticating with the wireless network using a message digest with the pre-shared secret key.	(e) authenticating...	(d) authenticating...	(e) authenticating...

Claim 2	Claim 2	Claim 1 (a) (i) module identity…	Claim 1 (a) (ii) module identity…
Claim 4	Claim 8		
Claim 5	Claim 4		
Claim 6	Claim 5	Claim 3	Claim 3
Claim 7	Claim 1 (b)	Claim 3	Claim 3
Claim 9	Claim 15		
Claim 11	Claim 16		
Claim 14	Claim 1		
Claim 20	Claim 11		

6. Claims 3, 8, 10, 12-13 and 15-19 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-18 of U.S. Patent No. 11258595 in view of Official Notice.

Examiner takes Official Notice it would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to combine the secure machine to machine communication method of 11258595 and the various device types of claims 3, 8, 10, 12-13 and 15-19 of the instant application. It would have been obvious because combining the secure machine to machine communication of 11258595 and known devices and standards (e.g. 802.11, UDP packets, IMSI) would yield the predictable results of using a secure communication method (11258595) with well-known technologies in the art.

7. Claims 3-5 and 8-20 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-9 of U.S. Patent No. 10530575 in view of Official Notice.

Examiner takes Official Notice it would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to combine the secure machine to machine communication method of 10530575 and the various device types of claims 3, 8, 10, 12-13 and 15-19 of the instant application. It would have been obvious because combining the secure machine to machine communication of 10530575 and known devices and standards (e.g. 802.11, UDP packets, IMSI) would yield the predictable results of using a secure communication method (10530575) with well-known technologies in the art.

8. Claims 3-5 and 8-20 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-9 of U.S. Patent No. 10057059 in view of Official Notice.

Examiner takes Official Notice it would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention to combine the secure machine to machine communication method of 10057059 and the various device types of claims 3, 8, 10, 12-13 and 15-19 of the instant application. It would have been obvious because combining the secure machine to machine communication of 10057059 and known devices and standards (e.g. 802.11, UDP packets, IMSI) would

yield the predictable results of using a secure communication method (10057059) with well-known technologies in the art.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Nakhjiri et al. (U.S. Patent Application Publication 2014/0082359) teaches a mobile device generating a public private key pair from a seed (note paragraph [0026]) and then using the key pair in an ECDH key agreement with a server (note paragraph [0032]).

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAVID J PEARSON whose telephone number is (571)272-0711. The examiner can normally be reached 6:00 - 5:30 pm; Monday through Thursday.

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

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/David J Pearson/
Primary Examiner, Art Unit 2438

Notice of References Cited	Application/Control No. 17/647,812	Applicant(s)/Patent Under Reexamination Nix, John A.	
	Examiner DAVID J PEARSON	Art Unit 2438	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-20140082359-A1	03-2014	Nakhjiri; Madjid	H04L63/0435	713/168
	B					
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/647,812	Nix, John A.
	Examiner	Art Unit
	DAVID J PEARSON	2438

CPC - Searched*		
Symbol	**Date**	**Examiner**
H04W12/40, 069	04/11/2022	DP
G06F21/445	04/11/2022	DP
H04L9/0841, 0816, 32	04/11/2022	DP
H04L63/0272, 045, 061	04/11/2022	DP
G06F2221/2115	04/11/2022	DP

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

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

Search Notes		
Search Notes	**Date**	**Examiner**
Inventor name search	04/11/2022	DP
CPC class and keyword search	04/11/2022	DP
See attached NPL searches - IP.com; Google Scholar; Dialog	04/11/2022	DP
See attached SEARCH report	04/12/2022	DP

Petitioner Samsung Ex-1038, 0379

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/647,812	Nix, John A.
	Examiner	Art Unit
	DAVID J PEARSON	2438

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

Petitioner Samsung Ex-1038, 0380

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/647,812	Nix, John A.
	Examiner	**Art Unit**
	DAVID J PEARSON	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/12/2022								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								

Petitioner Samsung Ex-1038, 0381

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L237	141	(nix-john$).in.	(US-PGPUB; USPAT)	OR	OFF	OFF	2022/04/11 08:42 AM
L238	23646	(H04W12/40 OR G06F21/445 OR H04L9/0841 OR H04L9/0816 OR H04L9/32 OR H04L63/0272 OR H04L63/045 OR G06F2221/2115).cpc.	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM
L239	452	L151 AND (PSK (preshared pre-shared) near2 (secret key)) AND (ECDH DH diffie)	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM
L240	408	L151 AND (PSK (preshared pre-shared) near2 (secret key)) same3 (challenge authenticat$3 hash$3 signature digest) AND (ECDH DH diffie)	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM
L241	355	L151 AND (PSK (preshared pre-shared) near2 (secret key)) SAME (challenge authenticat$3 hash$3 signature digest) AND (ECDH DH diffie)	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM
L242	299	L151 AND (PSK (preshared pre-shared) near2 (secret key)) AND (challenge authenticat$3) SAME (hash$3 signature digest) AND (ECDH DH diffie)	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM
L243	106	(L154 L155) AND @ad<"20131016"	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM
L244	340	L151 AND (challenge authenticat$3) SAME (hash$3 signature digest) SAME (secret key) same4 (ECDH elliptic$2 near2(DH diffie diffie-hellman))	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM
L245	20	L2 and ((ID identity identif$4) with ((private public) adj key) with (server) with (authenticat$3)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM

Petitioner Samsung Ex-1038, 0382

L246	67	("20050058294" OR "20060129848" OR "20080044032" OR "20080107083" OR "20110035604" OR "20110213959" OR "20110268022" OR "20110269422" OR "20110269461" OR "20110269472" OR "20110270747" OR "20120011362" OR "20120087493" OR "20120190354" OR "20120263298" OR "20130012168" OR "20130122864" OR "20130157673" OR "20130165075" OR "20130227646" OR "20130283047" OR "20130294602" OR "20130340040" OR "20130344864" OR "20140003604" OR "20140082358" OR "20140082359" OR "20140120874" OR "20140140507" OR "20140219447" OR "20140235210" OR "20140237101" OR "20140287725" OR "20140308991" OR "20140329502" OR "20140357229" OR "20150121495" OR "20150281964" OR "20150350881" OR "20160057725" OR "20160088096" OR "20160127132" OR "20160149903" OR "5216715" OR "5642420" OR "5664017" OR "5852665" OR "5995625" OR "6256733" OR "6721886" OR "6804357" OR "6842628" OR "7957532" OR "8352739" OR "8452017" OR "8577337" OR "8965366" OR "9020479" OR	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM

Petitioner Samsung Ex-1038, 0383

		"9270653" OR "9332129" OR "9572016" OR "9628981" OR "9674690" OR "9794775" OR "9800993" OR "9807605" OR "9923724").pn.					
L247	7	L167 AND (PSK (preshared pre-shared shared) near2 (secret key)) SAME (challenge authenticat$3 hash$3 signature digest identi$7) AND (ECDH DH diffie)	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM
L248	0	L167 AND (PSK (preshared pre-shared shared) near2 (secret key)) WITH (challenge authenticat$3 hash$3 signature digest) SAME (identi$7) AND (server) near3 (public private) ADJ (key) SAME (client user device) near3 (public private) ADJ (key) SAME (generat$3 deriv$5 diffie DH ECDH elliptic$2) WITH (key)	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM
L249	6	L167 AND (PSK (preshared pre-shared shared) near2 (secret key)) WITH (challenge authenticat$3 hash$3 signature digest) SAME (identi$7)	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM
L250	1	L167 AND (server) near3 (public private) ADJ (key) SAME (client user device) near3 (public private) ADJ (key) SAME (generat$3 deriv$5 diffie DH ECDH elliptic$2) WITH (key)	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM
L251	50462	(H04W12/40 OR G06F21/445 OR H04L9/0841 OR H04L9/0816 OR H04L9/32 OR H04L63/0272 OR H04L63/045 OR H04L63/0442 OR H04L63/123 OR H04W52/0216 OR	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM

		H04L63/061 OR G06F2221/2115).cpc.					
L252	1107	L172 AND (PSK (preshared pre-shared shared) near2 (secret key)) SAME (challenge authenticat$3 hash$3 signature digest) SAME (ID identi$7) AND (ECDH DH diffie)	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM
L253	39	L172 AND (PSK (preshared pre-shared shared) near2 (secret key)) SAME (challenge hash$3 signature digest) SAME (ID identi$7) near4 (client EUICC user SIM UICC device) SAME (server) WITH (authenticat$3 verif$7 validat$3 compar$3 confirm$5) same4 (ECDH DH diffie)	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM
L254	79	L172 AND (PSK (preshared pre-shared shared) near2 (secret key)) SAME (challenge hash$3 signature digest) SAME (ID identi$7) near4 (client EUICC user SIM UICC device) SAME (server) WITH (authenticat$3 verif$7 validat$3 compar$3 confirm$5) AND (ECDH DH diffie)	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM
L255	101	L172 AND (PSK (preshared pre-shared shared) near2 (secret key)) SAME (challenge hash$3 signature digest) SAME (ID identi$7) SAME (server) SAME (authenticat$3 verif$7 validat$3 compar$3 confirm$5) same4 (ECDH DH diffie)	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM
L256	79	L172 AND (PSK (preshared pre-shared shared) near2 (secret key)) WITH (challenge authenticat$3 hash$3 signature digest) SAME (identi$7) AND (server)	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM

Petitioner Samsung Ex-1038, 0385

		near3 (public private) ADJ (key) SAME (client user device) near3 (public private) ADJ (key) SAME (generat$3 deriv$5 diffie DH ECDH elliptic$2) WITH (key)					
L257	24	L172 AND (ECDH diffie near4 elliptic$2) SAME (decrypt$3) WITH (respon$4 challenge reply digest hash) WITH (server client SIM EUICC UICC token)	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM
L258	103	L172 AND (ECDH diffie near4 elliptic$2) same3 (decrypt$3) WITH (respon$4 challenge reply digest hash) WITH (server client SIM EUICC UICC token)	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM
L259	210	L172 AND (ECDH diffie near4 elliptic$2) same3 (decrypt$3) SAME (respon$4 challenge reply digest hash) SAME (server client SIM EUICC UICC token) SAME (PSK (pre-shared shared stored) near2 (key secret))	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM
L260	188	L172 AND (ECDH diffie near4 elliptic$2) same3 (decrypt$3) SAME (respon$4 challenge reply digest hash token) SAME (server client SIM EUICC UICC) SAME (PSK (pre-shared shared stored) near2 (key secret))	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM
L261	53	(L174 L175 L176 L177 L178 L179 L180 L181) AND @ad<"20131016"	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 08:42 AM
L262	3	("20110158411" "20130145151" "20140068252").pn.	(US-PGPUB; USPAT)	OR	OFF	OFF	2022/04/11 10:44 AM
L263	241	("10169587" OR "10621352" OR "20010029581" OR "20020018569" OR "20030003895" OR "20030211842" OR "20040162472" OR "20040179684" OR	(US-PGPUB; USPAT)	OR	OFF	OFF	2022/04/11 11:40 AM

Petitioner Samsung Ex-1038, 0386

		"20040221163" OR "20050008159" OR "20050021875" OR "20050050323" OR "20050058294" OR "20050120202" OR "20050138353" OR "20050193199" OR "20050246282" OR "20050278787" OR "20060021063" OR "20060056355" OR "20060059344" OR "20060095771" OR "20060129848" OR "20060206710" OR "20060281442" OR "20070101400" OR "20070158439" OR "20070206799" OR "20080016230" OR "20080022089" OR "20080031204" OR "20080044032" OR "20080107083" OR "20080114978" OR "20080130879" OR "20080165698" OR "20080307218" OR "20090028341" OR "20090041110" OR "20090060197" OR "20090077643" OR "20090113203" OR "20090116642" OR "20090125996" OR "20090132806" OR "20090183541" OR "20090191857" OR "20090209232" OR "20090217348" OR "20090268909" OR "20090274306" OR "20090282246" OR "20090313472" OR "20100031042" OR "20100062808" OR "20100093347" OR "20100098253" OR "20100166167" OR "20100195833" OR "20100199334" OR "20100223461" OR "20100275028" OR "20100291907" OR "20110016321" OR "20110035584" OR "20110035604" OR				

Petitioner Samsung Ex-1038, 0387

		"20110055553" OR "20110158411" OR "20110167272" OR "20110213959" OR "20110237281" OR "20110268022" OR "20110269422" OR "20110269461" OR "20110269472" OR "20110270747" OR "20110291803" OR "20110314287" OR "20120011360" OR "20120011362" OR "20120023336" OR "20120030461" OR "20120033613" OR "20120072732" OR "20120084568" OR "20120087493" OR "20120089568" OR "20120108205" OR "20120117635" OR "20120159153" OR "20120170451" OR "20120190354" OR "20120214444" OR "20120260086" OR "20120260090" OR "20120260095" OR "20120263298" OR "20120278490" OR "20120300932" OR "20120331292" OR "20120331298" OR "20130007442" OR "20130012168" OR "20130028184" OR "20130091556" OR "20130114810" OR "20130117824" OR "20130122864" OR "20130149996" OR "20130157673" OR "20130165073" OR "20130165075" OR "20130166915" OR "20130173747" OR "20130173926" OR "20130179962" OR "20130182586" OR "20130183932" OR "20130212637" OR "20130227646" OR "20130231087" OR "20130283047" OR "20130294602" OR "20130305345" OR					

Petitioner Samsung Ex-1038, 0388

		"20130322621" OR "20130331063" OR "20130340040" OR "20130344864" OR "20140003604" OR "20140040628" OR "20140049653" OR "20140053241" OR "20140073375" OR "20140082358" OR "20140082359" OR "20140082538" OR "20140082539" OR "20140087790" OR "20140101444" OR "20140108801" OR "20140115335" OR "20140120874" OR "20140122878" OR "20140140507" OR "20140140509" OR "20140143534" OR "20140143826" OR "20140161113" OR "20140165155" OR "20140192976" OR "20140219447" OR "20140219448" OR "20140235210" OR "20140237101" OR "20140244994" OR "20140273913" OR "20140281483" OR "20140287725" OR "20140308991" OR "20140329502" OR "20140337937" OR "20140351403" OR "20140357229" OR "20150012743" OR "20150017910" OR "20150071139" OR "20150089214" OR "20150092590" OR "20150095514" OR "20150095648" OR "20150106616" OR "20150113275" OR "20150121066" OR "20150121495" OR "20150143125" OR "20150163056" OR "20150215126" OR "20150222604" OR "20150222619" OR "20150281964" OR "20150350881" OR "20160014112" OR					

Petitioner Samsung Ex-1038, 0389

		"20160057725" OR "20160088096" OR "20160127132" OR "20160149903" OR "20160294829" OR "20170206532" OR "20190313246" OR "20190332774" OR "20190356482" OR "20200162247" OR "20200162269" OR "20200226258" OR "20200280436" OR "20210126801" OR "20210184842" OR "20210194681" OR "20210211279" OR "20210218560" OR "5216715" OR "5642420" OR "5664017" OR "5852665" OR "5995625" OR "6038322" OR "6256733" OR "6721886" OR "6804357" OR "6842628" OR "7921292" OR "7957532" OR "8127142" OR "8352739" OR "8434139" OR "8452017" OR "8522013" OR "8526606" OR "8555067" OR "8577337" OR "8590028" OR "8782774" OR "8843179" OR "8924715" OR "8948386" OR "8965366" OR "9002018" OR "9020479" OR "9253643" OR "9270653" OR "9332129" OR "9408012" OR "9572016" OR "9596078" OR "9628981" OR "9674690" OR "9698981" OR "9794775" OR "9800993" OR "9807605" OR					

Petitioner Samsung Ex-1038, 0390

		"9923724").pn.					
L264	30	L263 AND (challenge authenticat$3) SAME (hash$3 signature digest) SAME (secret key) AND (ECDH elliptic$2 near2(DH diffie diffie-hellman))	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 11:59 AM
L265	93	L263 AND (challenge authenticat$3) SAME (hash$3 signature digest) SAME (secret key) AND (generat$3 determin$5 deriv$5) WITH (key) SAME (public ADJ key) SAME (private ADJ key)	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 12:00 PM
L266	34	L263 AND (challenge authenticat$3) SAME (hash$3 signature digest) SAME (secret key) AND (generat$3 determin$5 deriv$5) WITH (key) SAME (public ADJ key) SAME (private ADJ key) SAME (server network) SAME (mobile client module)	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 12:01 PM
L267	46	(L264 L266)	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 12:02 PM
L268	30	L263 AND (challenge authenticat$3 validat$3 verif$7) WITH (mobile client module SIM) SAME (hash$3 signature digest) WITH (seed secret key) AND (generat$3 determin$5 deriv$5) WITH (key) SAME (public ADJ key) SAME (private ADJ key) SAME (server network) SAME (mobile client module)	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 04:00 PM
L269	16414	(H04L63/045 OR H04L63/061 OR H04W12/069 OR H04W12/40).cpc.	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 04:20 PM
L270	597	L269 AND (challenge authenticat$3 validat$3 verif$7) WITH (mobile client module SIM) SAME (hash$3 signature digest) WITH (seed secret key) AND	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 04:20 PM

Petitioner Samsung Ex-1038, 0391

		(generat$3 determin$5 deriv$5) WITH (key) SAME (public ADJ key) SAME (private ADJ key) SAME (server network) SAME (mobile client module)					
L271	240	L269 AND (challenge authenticat$3 validat$3 verif$7) WITH (mobile client module SIM) SAME (hash$3 signature digest) WITH (seed secret key) AND (ECDH elliptic$2 near2(DH diffie diffie-hellman))	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 04:21 PM
L272	177	(L270 L271) AND @ad<"20131016"	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 04:21 PM
L273	82	(seed shared near2 (secret key)) SAME (generat$3) WITH ((private public) ADJ key) AND (challenge authenticat$3 validat$3 verif$7) WITH (mobile client module SIM) SAME (hash$3 signature digest) WITH (seed (shared) near2 (secret key)) AND (ECDH elliptic$2 near2(DH diffie diffie-hellman))	(US-PGPUB; USPAT)	OR	ON	ON	2022/04/11 05:03 PM
L274	4	("20140082358" "20140235210" "20150350881" "20100291907").pn.	(US-PGPUB; USPAT)	OR	OFF	OFF	2022/04/11 05:27 PM
L275	137	(seed shared near2 (secret key)) SAME (generat$3) WITH ((private public) ADJ key) AND (challenge authenticat$3 validat$3 verif$7) WITH (mobile client module SIM) SAME (hash$3 signature digest) WITH (seed (shared) near2 (secret key)) AND (ECDH elliptic$2 near2(DH diffie diffie-hellman))	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/04/12 11:46 AM
L276	3	(L275) AND @ad<"20131016"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	ON	2022/04/12 11:46 AM

Petitioner Samsung Ex-1038, 0392

			IBM_TDB)				
L277	580	(seed shared secret) SAME (generat$3) WITH ((private public) ADJ key) AND (challenge authenticat$3 validat$3 verif$7) WITH (mobile client module SIM) SAME (hash$3 signature digest) WITH (seed shared secret key) AND (ECDH elliptic$2 near2(DH diffie diffie-hellman))	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/04/12 11:56 AM
L278	42	(L277) AND @ad<"20131016"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/04/12 11:56 AM
L279	134	(seed shared secret) SAME (generat$3) WITH ((private public) ADJ key) AND (challenge authenticat$3 validat$3 verif$7) WITH (mobile client module SIM) SAME (hash$3 signature digest) WITH (seed shared secret key) AND (generat$3 creat$3 calculat$3 deriv$5) WITH (shared symmetric) near3 (key) SAME (server) near2 ((private public) ADJ key) SAME (client mobile SIM) near2 ((private public) ADJ key)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/04/12 12:07 PM
L280	510	(seed shared secret) SAME (generat$3) WITH ((private public) ADJ key) AND (challenge authenticat$3 validat$3 verif$7) WITH (mobile client module SIM) SAME (hash$3 signature digest) WITH (seed shared secret key) AND (generat$3 creat$3 calculat$3 deriv$5) near5 (shared symmetric key) SAME (server) near2 ((private public) ADJ key) SAME	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/04/12 12:07 PM

Petitioner Samsung Ex-1038, 0393

		(client mobile SIM) near2 ((private public) ADJ key)					
L281	117	(L280 L279) AND @ad<"20131016"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/04/12 12:07 PM
L282	155	(L278 L281)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/04/12 12:08 PM

PE2E SEARCH - Search History (Interference)

There are no Interference searches to show.

Petitioner Samsung Ex-1038, 0394

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Network-1 Technologies, Inc.	Confirmation No.: 6784
Title:	Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)	
Appl. No.:	17/647,812	
Filing Date:	January 12, 2022	
Examiner:	PEARSON, David J.	
Art Unit:	2438	
Docket No.:	63121/0213	
Customer No.:	01912	

INFORMATION DISCLOSURE STATEMENT LETTER
UNDER 37 C.F.R. § 1.56

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

Sir:

In accordance with the duty of disclosure under 37 C.F.R. §1.56, the attention of the Patent and Trademark Office is hereby directed to the information item(s) listed on the attached Form PTO-SB08. Unless otherwise indicated herein, one copy of each item(s) is attached. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the item(s) be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

Reference to Related Patents and Co-Pending Applications

The below chart provides information regarding related issued patents and co-pending applications filed by the present Applicant:

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

Petitioner Samsung Ex-1038, 0395

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

Serial No.	Attorney Docket No.	Filing Date	Status
17/647,812	**63121/0213**	**2022-01-12**	**(Present Application) Pending - Case Docketed to Examiner in GAU 2022-03-19**
17/547,990	63121/0212	2021-12-10	Pending - Ready for Examination
17/304,922	63121/0209	2021-06-28	Pending - Ready for Examination
17/249,242	63121/0202	2021-02-24	Pending – Ready for Examination
16/879,325	63121/0198	2020-05-20	USP 11,082,218
16/843,107	63121/0197	2020-04-08	USP 11,283,603
16/721,153	63121/0195	2019-12-19	Non-Final Action issued on January 21, 2022
16/593,561	63121/0190	2019-10-04	USP 11,258,595
16/453,682	63121/0184	2019-06-26	USP 11,233,780
16/271,455	63121/0181	2019-02-08	USP 10,594,679
16/271,428	63121/0180	2019-02-08	USP 10,523,432
16/201,401	63121/0179	2018-11-27	USP 10,700,856
16/200,118	63121/0178	2018-11-26	USP 10,498,530
16/110,804	63121/0168	2018-08-23	USP 10,382,422
16/036,506	63121/0167	2018-07-16	USP 10,530,575
15/983,957	63121/0163	2018-05-18	USP 10,177,911
15/973,012	63121/0162	2018-05-07	USP 10,250,386
15/972,914	63121/0161	2018-05-07	USP 10,652,017
15/928,848	63121/0160	2018-03-22	USP 10,084,768
15/010,905	63121/0157	2016-01-29	USP 9,641,327
15/680,758	63121/0147	2017-08-18	USP 10,187,206
15/162,292	63121/0146	2016-05-23	USP 10,362,012
14/751,119	63121/0145	2015-06-25	USP 9,961,060
15/457,700	63121/0144	2017-03-13	USP 9,998,281
15/583,968	63121/0143	2017-05-01	USP 10,057,059
15/043,293	63121/0142	2016-02-12	USP 9,998,280
15/642,088	63121/0141	2017-07-05	USP 10,003,461
15/130,146	63121/0140	2016-04-15	USP 9,742,562
15/162,302	63121/0139	2016-05-23	USP 9,698,981
14/789,255	63121/0138	2015-07-01	USP 9,596,078
14/139,419	63121/0137	2013-12-23	USP 9,351,162
14/136,711	63121/0136	2013-12-20	USP 9,300,473
14/099,329	63121/0135	2013-12-06	USP 9,100,175

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

Petitioner Samsung Ex-1038, 0396

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

14/084,141	63121/0134	2013-11-19	USP 9,319,223
14/064,618	63121/0133	2013-10-28	USP 9,118,464
14/055,606	63121/0132	2013-10-16	USP 9,276,740
14/039,401	63121/0131	2013-09-27	USP 9,288,059
14/023,181	63121/0130	2013-09-10	USP 9,350,550
AU 2019246774	63121-0199	2019-10-08	Published on 2021-09-23
GB 1608573	63121-0151	2014-10-27	Published on 2016-08-03
GB 2100530	63121-0201	2014-10-27	Published on 2021-05-12
CA 2,965,119	63121-0152	2014-10-27	Published on 2015-05-07
HK 17101082.8	63121-0153	2014-10-27	Published on 2017-10-20
EU 14868381.6	63121-0154	2014-12-04	Published on 2017-01-04
CA 2,969,829	63121-0155	2014-12-04	Published on 2015-06-11
HK 17106540.3	63121-0156	2014-12-04	Published on 2018-01-19

The Examiner is invited to review the prosecution history of each of these applications, including the cited references of record and related office actions, as the Examiner deems appropriate.

* * * * *

This Information Disclosure Statement is being filed within three months of the filing date and before the mailing date of a first Office Action on the merits in the present application. No certification or fee is required. Applicant(s) hereby petition(s) that the Information Disclosure Statement be considered. Please charge any fee deficiency or credit any overpayment to Deposit Account No. 01-1785, under Docket No. 63121/0213.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

Petitioner Samsung Ex-1038, 0397

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

Respectfully submitted,

AMSTER, ROTHSTEIN & EBENSTEIN LLP
Attorneys for Applicant
90 Park Avenue
New York, NY 10016
(212) 336-8000

Dated: April 5, 2022
New York, NY

By: /Albert J. Boardman/
Albert J. Boardman, Reg. No. 70,601

04/11/2022

/David J Pearson/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

Petitioner Samsung Ex-1038, 0398

Bibliographic Data

Application No: 17/647,812

Foreign Priority claimed: ○ Yes ◉ No

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

Verified and Acknowledged: /David J Pearson/ (Examiner's Signature) | DJP (Initials)

Title: Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
01/12/2022	713	2438	63121/0213
RULE			

APPLICANTS

Network-1 Technologies, Inc., New York, NY, UNITED STATES

INVENTORS

John A. Nix, Evanston, IL, UNITED STATES

CONTINUING DATA

This application is a CON of 16593561 10/04/2019 PAT 11258595

16593561 is a CON of 16036506 07/16/2018 PAT 10530575

16036506 is a CON of 15583968 05/01/2017 PAT 10057059

15583968 is a CON of 15010905 01/29/2016 PAT 9641327

15010905 is a CON of 14055606 10/16/2013 PAT 9276740

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

01/24/2022

**** SMALL ENTITY ****

STATE OR COUNTRY

UNITED STATES

ADDRESS

AMSTER, ROTHSTEIN & EBENSTEIN LLP
90 PARK AVENUE
NEW YORK, NY 10016
UNITED STATES

FILING FEE RECEIVED

$3,000

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	10169587	B1	2019-01-01	Nix	
	2	10621352	B2	2020-04-14	Nix	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060021063	A1	2006-01-26	Hori	
	2	20100093347	A1	2010-04-15	Hahn et al.	
	3	20110158411	A1	2011-06-30	Medvinsky et al.	
	4	20210126801	A1	2021-04-29	Nix	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	5	20200280436	A1	2020-09-03	Nix	
	6	20210218560	A1	2021-07-15	Nix	
	7	20210184842	A1	2021-06-17	Nix	
	8	20210194681	A1	2021-06-24	Nix	
	9	20190356482	A1	2019-11-21	Nix	
	10	20200226258	A1	2020-07-16	Nix	
	11	20190313246	A1	2019-10-10	Nix	
	12	20210211279	A1	2021-07-08	Nix	
	13	20200162269	A1	2020-05-21	Nix	
	14	20200162247	A1	2020-05-21	Nix	
	15	20190332774	A1	2019-10-31	Nix	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	16	20100291907	A1	2010-11-18	Malcolm David MacNaughtan et al.	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2518976	GB	A	2015-04-08	Vodafone IP Licensing Ltd		
	2	2021007235	WO	A1	2021-01-14	Nix		
	3	2021007235	WO	A1	2021-01-14	Nix		
	4	2021087221	WO	A1	2021-05-06	Nix		
	5	2020223319	WO	A1	2020-11-05	Nix		
	6	2020006162	WO	A1	2020-01-02	Nix		
	7	2019246206	WO	A1	2019-12-26	Nix		
	8	2019222319	WO	A1	2019-11-21	Nix		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	9	2019209598	WO	A1	2019-10-31	Nix		
	10	2019178312	WO	A1	2019-09-19	Nix		
	11	2020123959	WO	A1	2020-06-18	Nix		
	12	2020061023	WO	A1	2020-03-26	Nix		
	13	3110641	CA	A1	2019-10-31	Nix		
	14	3110468	CA	A1	2019-11-21	Nix		
	15	19803936	DE	A1	1999-08-05	Osram GmbH Siemens AG		
	16	3766222	EP	A1	2021-01-20	Nix		
	17	20130026351	KR	A	2013-03-13	KT CORPORATION		☒
	18	2013/048084	WO	A2	2013-04-04	KT CORPORATION		☒

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

NON-PATENT LITERATURE DOCUMENTS Remove

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Search Report issued in UK Application No. GB2108534.5 dated July 7, 2021.	
	2	ANSI X9.63 Overview, Key Agreement and Key Transport Using Elliptic Curve Cryptography, Simon Blake-Wilson, Certicom (2000)	
	3	TLS 1.3 Wish List Presentation, IETF 87 (Eric Rescorla), dated August 1, 2013.	
	4	European Patent Office Communication with European Search Report and European Search Opinion issued in EP 21182424.8 dated October 12, 2021.	
	5	European Patent Office Communication with European Search Report and European Search Opinion issued in EP 21182451.1 dated October 12, 2021.	
	6	European Patent Office Communication with European Search Report and European Search Opinion issued in EP 21182432.1 dated October 12, 2021.	
	7	Harald Bender et al., "Business transformation of the provisioning process for Machine-to-Machine," 2011 15th International Conference on Intelligence in Next Generation Networks, IEEE, 2011. (Year: 2011).	

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

EXAMINER SIGNATURE

Examiner Signature	/David J Pearson/	Date Considered	04/11/2022

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20120033613	A1	2012-02-09	Lin et al.	
	2	20130028184	A1	2013-01-31	Lee et al.	
	3	20130182586	A1	2013-07-18	Paladugu et al.	
	4	20020018569	A1	2002-02-14	Panjwani et al.	
	5	20030003895	A1	2003-01-02	Wallentin et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	6	20030211842	A1	2003-11-13	Kempf et al.	
	7	20040179684	A1	2004-09-16	Appenzeller et al.	
	8	20050008159	A1	2005-01-13	Grilli et al.	
	9	20050021875	A1	2005-01-27	Bouthemy et al.	
	10	20050120202	A1	2005-06-02	Cuellar et al.	
	11	20050138353	A1	2005-06-23	Spies et al.	
	12	20050193199	A1	2005-09-01	Asokan et al.	
	13	20050246282	A1	2005-11-03	Naslund et al.	
	14	20050278787	A1	2005-12-15	Naslund et al.	
	15	20060021063	A1	2006-01-26	Hori	
	16	20060056355	A1	2006-03-16	Love et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	17	20060059344	A1	2006-03-16	Mononen	
	18	20060206710	A1	2006-09-14	Gehrmann	
	19	20060281442	A1	2006-12-14	Lee et al.	
	20	20070206799	A1	2007-09-06	Wingert et al.	
	21	20080016230	A1	2008-01-17	Holtmanns et al.	
	22	20080022089	A1	2008-01-24	Leedom	
	23	20080114978	A1	2008-05-15	Lehtovirta et al.	
	24	20080165698	A1	2008-07-10	Dalsgaard et al.	
	25	20090116642	A1	2009-05-07	Yang et al.	
	26	20090028341	A1	2009-01-29	Hamachi	
	27	20090077643	A1	2009-03-19	Schmidt et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	28	20090125996	A1	2009-05-14	Guccione et al.	
	29	20090132806	A1	2009-05-21	Blommaert et al.	
	30	20090191857	A1	2009-07-30	Horn et al.	
	31	20090209232	A1	2009-08-20	Cha et al.	
	32	20090268909	A1	2009-10-29	Girao et al.	
	33	20090282246	A1	2009-11-12	Gunther	
	34	20090313472	A1	2009-12-17	Guccione et al.	
	35	20100166167	A1	2010-07-01	Karimi-Cherkandi et al.	
	36	20100031042	A1	2010-02-04	Di Crescenzo et al.	
	37	20100062808	A1	2010-03-11	Cha et al.	
	38	20100098253	A1	2010-04-22	Delerablee	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	39	20100275028	A1	2010-10-28	Takashima	
	40	20110016321	A1	2011-01-20	Sundaram et al.	
	41	20110055553	A1	2011-03-03	Lee et al.	
	42	20110237281	A1	2011-09-29	Busropan et al.	
	43	20110291803	A1	2011-12-01	Bajic et al.	
	44	20110314287	A1	2011-12-22	Escott et al.	
	45	20120011360	A1	2012-01-12	Engels et al.	
	46	20120023336	A1	2012-01-26	Natarajan	
	47	20120072732	A1	2012-03-22	Canard et al.	
	48	20120089568	A1	2012-04-12	Manley et al.	
	49	20120108205	A1	2012-05-03	Schell et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	50	20120117635	A1	2012-05-10	Schell et al.	
	51	20120159153	A1	2012-06-21	Shim et al.	
	52	20120260086	A1	2012-10-11	Haggerty et al.	
	53	20120260090	A1	2012-10-11	Hauck et al.	
	54	20120260095	A1	2012-10-11	Von Hauck et al.	
	55	20120278490	A1	2012-11-01	Sennett et al.	
	56	20120300932	A1	2012-11-29	Cambridge et al.	
	57	20120331292	A1	2012-12-27	Haggerty et al.	
	58	20130091556	A1	2013-04-11	Horn et al.	
	59	20130114810	A1	2013-05-09	Kobayashi et al.	
	60	20130117824	A1	2013-05-09	Naslund et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

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

EXAMINER SIGNATURE

Examiner Signature	/David J Pearson/	Date Considered	04/11/2022

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20140143826	A1	2014-05-22	Sharp et al.	
	2	20140161113	A1	2014-06-12	Cui et al.	
	3	20140165155	A1	2014-06-12	Zhang	
	4	20140192976	A1	2014-07-10	Yoon et al.	
	5	20140219447	A1	2014-08-07	Park et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	6	20140219448	A1	2014-08-07	Froels et al.	
	7	20140244994	A1	2014-08-28	Yu	
	8	20140273913	A1	2014-09-18	Michel et al.	
	9	20140287725	A1	2014-09-25	Lee	
	10	20140337937	A1	2014-11-13	Truskovsky et al.	
	11	20140351403	A1	2014-11-27	Lein et al.	
	12	20150012743	A1	2015-01-08	Holtmanns et al.	
	13	20150017910	A1	2015-01-15	Li et al.	
	14	20150071139	A1	2015-03-12	Nix	
	15	20150092590	A1	2015-04-02	Zhu et al.	
	16	20150095514	A1	2015-04-02	Yu	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	17	20150095648	A1	2015-04-02	Nix	
	18	20150113275	A1	2015-04-23	Kim et al.	
	19	20150121495	A1	2015-04-03	Gao et al.	
	20	20130231087	A1	2013-09-05	O'Leary	
	21	20130165073	A1	2013-06-27	Madsen	
	22	20130007442	A1	2013-01-03	Mao et aL	
	23	20120170451	A1	2012-07-05	Viswanathan et aL	
	24	20120084568	A1	2012-08-05	Sarikaya et al.	
	25	20120030461	A1	2012-02-02	Willey et al.	
	26	20080307218	A1	2008-12-11	Logvinov	
	27	20110035584	A1	2011-02-10	Meyerstein et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	28	20090060197	A1	2009-03-05	Taylor et al.	
	29	20150089214	A1	2015-03-26	Dupre	
	30	20140122878	A1	2014-05-01	Cho et al.	
	31	20140115335	A1	2014-04-24	Jorden et al.	
	32	20130173926	A1	2013-07-04	Morese et al.	
	33	20130012168	A1	2013-01-10	Rajadurai et al.	
	34	20120331298	A1	2012-12-27	Xu et al.	
	35	20120190354	A1	2012-07-26	Merrien et al.	
	36	20040221163	A1	2004-11-04	Jorgensen et al.	
	37	20090113203	A1	2009-04-30	Tsuge et al.	
	38	20150163056	A1	2015-06-11	Nix	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	39	20090217348	A1	2009-08-27	Salmela et al.	
	40	20080130879	A1	2008-06-05	Heinonen et al.	
	41	20130122864	A1	2013-05-16	Haggerty et al.	
	42	20150071139	A1	2015-03-12	Nix	
	43	20150095648	A1	2015-04-02	Nix	
	44	20150106616	A1	2015-04-16	Nix	
	45	20150121066	A1	2015-04-30	Nix	
	46	20150143125	A1	2015-05-21	Nix	
	47	20040162472	A1	2004-08-19	Berson et al.	
	48	20150215126	A1	2015-07-30	Ashdown	
	49	20160294829	A1	2016-10-06	Angus	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	50	20110269422	A1	2011-11-03	Xu et al.	
	51	20110269461	A1	2011-11-03	Xu et al.	
	52	20110269472	A1	2011-11-03	Xu et al.	
	53	20110270747	A1	2011-11-03	Xu et al.	
	54	20130294602	A1	2013-11-07	Huxham et al.	
	55	20130340040	A1	2013-12-19	Park et al.	
	56	20140308991	A1	2014-10-16	Lee et al.	
	57	20140329502	A1	2014-11-06	Lee et al.	
	58	20150281964	A1	2015-10-01	Seo et al.	
	59	20070158439	A1	2007-07-12	Conner et al.	
	60	20130183932	A1	2013-07-18	Lemilainen et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

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

EXAMINER SIGNATURE

Examiner Signature	/David J Pearson/	Date Considered	04/11/2022

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20120033613	A1	2012-02-09	Lin et al.	
	2	20130028184	A1	2013-01-31	Lee et al.	
	3	20130182586	A1	2013-07-18	Paladugu et al.	
	4	20020018569	A1	2002-02-14	Panjwani et al.	
	5	20030003895	A1	2003-01-02	Wallentin et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	6	20030211842	A1	2003-11-13	Kempf et al.	
	7	20040179684	A1	2004-09-16	Appenzeller et al.	
	8	20050008159	A1	2005-01-13	Grilli et al.	
	9	20050021875	A1	2005-01-27	Bouthemy et al.	
	10	20050120202	A1	2005-06-02	Cuellar et al.	
	11	20050138353	A1	2005-06-23	Spies et al.	
	12	20050193199	A1	2005-09-01	Asokan et al.	
	13	20050246282	A1	2005-11-03	Naslund et al.	
	14	20050278787	A1	2005-12-15	Naslund et al.	
	15	20060021063	A1	2006-01-26	Hori	
	16	20060056355	A1	2006-03-16	Love et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	17	20060059344	A1	2006-03-16	Mononen	
	18	20060206710	A1	2006-09-14	Gehrmann	
	19	20060281442	A1	2006-12-14	Lee et al.	
	20	20070206799	A1	2007-09-06	Wingert et al.	
	21	20080016230	A1	2008-01-17	Holtmanns et al.	
	22	20080022089	A1	2008-01-24	Leedom	
	23	20080114978	A1	2008-05-15	Lehtovirta et al.	
	24	20080165698	A1	2008-07-10	Dalsgaard et al.	
	25	20090116642	A1	2009-05-07	Yang et al.	
	26	20090028341	A1	2009-01-29	Hamachi	
	27	20090077643	A1	2009-03-19	Schmidt et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	28	20090125996	A1	2009-05-14	Guccione et al.	
	29	20090132806	A1	2009-05-21	Blommaert et al.	
	30	20090191857	A1	2009-07-30	Horn et al.	
	31	20090209232	A1	2009-08-20	Cha et al.	
	32	20090268909	A1	2009-10-29	Girao et al.	
	33	20090282246	A1	2009-11-12	Gunther	
	34	20090313472	A1	2009-12-17	Guccione et al.	
	35	20100166167	A1	2010-07-01	Karimi-Cherkandi et al.	
	36	20100031042	A1	2010-02-04	Di Crescenzo et al.	
	37	20100062808	A1	2010-03-11	Cha et al.	
	38	20100098253	A1	2010-04-22	Delerablee	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	39	20100275028	A1	2010-10-28	Takashima	
	40	20110016321	A1	2011-01-20	Sundaram et al.	
	41	20110055553	A1	2011-03-03	Lee et al.	
	42	20110237281	A1	2011-09-29	Busropan et al.	
	43	20110291803	A1	2011-12-01	Bajic et al.	
	44	20110314287	A1	2011-12-22	Escott et al.	
	45	20120011360	A1	2012-01-12	Engels et al.	
	46	20120023336	A1	2012-01-26	Natarajan	
	47	20120072732	A1	2012-03-22	Canard et al.	
	48	20120089568	A1	2012-04-12	Manley et al.	
	49	20120108205	A1	2012-05-03	Schell et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	50	20120117635	A1	2012-05-10	Schell et al.	
	51	20120159153	A1	2012-06-21	Shim et al.	
	52	20120260086	A1	2012-10-11	Haggerty et al.	
	53	20120260090	A1	2012-10-11	Hauck et al.	
	54	20120260095	A1	2012-10-11	Von Hauck et al.	
	55	20120278490	A1	2012-11-01	Sennett et al.	
	56	20120300932	A1	2012-11-29	Cambridge et al.	
	57	20120331292	A1	2012-12-27	Haggerty et al.	
	58	20130091556	A1	2013-04-11	Horn et al.	
	59	20130114810	A1	2013-05-09	Kobayashi et al.	
	60	20130117824	A1	2013-05-09	Naslund et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

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

EXAMINER SIGNATURE

Examiner Signature	/David J Pearson/	Date Considered	04/11/2022

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

Main Concept Document
==========
US20200036521
Title: Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)
Abstract: Methods and systems are provided for supporting efficient and secure “Machine-to-Machine” (M2M) communications using a module, a server, and an application. A module can communicate with the server by accessing the Internet, and the module can include a sensor and/or an actuator. The module, server, and application can utilize public key infrastructure (PKI) such as public keys and private keys. The module can internally derive pairs of private/public keys using cryptographic algorithms and a first set of parameters. A server can authenticate the submission of derived public keys and an associated module identity. The server can use a first server private key and a second set of parameters to (i) send module data to the application and (ii) receive module instructions from the application. The server can use a second server private key and the first set of parameters to communicate with the module.

(No Concept Modifiers)
==========

Filters (3)
==========
Earliest Priority Date: To 2013-10-16

Inventors excluded: Nix

Assignees/Applicants excluded: "M2M & IOT TECH LLC"

Options
==========
De-dup: Extended Family Numbers
Cut-off: None
Sort: Relevance

Content: Patent Publications (164)
==========
US Patents
US Designs
US Applications
EPO Patents
EPO Applications
China Patents

Petitioner Samsung Ex-1038, 0426

China Applications
Japan Patents
Japan Applications
Korea Patents
Korea Applications
WIPO Applications
Argentina Patents
Argentina Applications
Brazil Patents
Brazil Applications
Canada Patents
Canada Applications
Chile Patents
Chile Applications
Colombia Applications
Costa Rica Applications
Cuba Patents
Cuba Applications
Dominican Republic Applications
Ecuador Patents
Ecuador Applications
El Salvador Applications
Guatemala Applications
Honduras Applications
Mexico Patents
Mexico Applications
Nicaragua Patents
Panama Applications
Peru Applications
Trinidad & Tobago Patents
Uruguay Applications
Austria Patents
Austria Applications
Belarus Patents
Belgium Patents
Belgium Applications
Bosnia & Herzegovina Patents
Bosnia & Herzegovina Applications
Bulgaria Patents
Bulgaria Applications
Croatia Patents
Croatia Applications
Czech Republic Patents
Czech Republic Applications
Czechoslovakia Patents
Czechoslovakia Applications
Denmark Patents
Denmark Applications

Petitioner Samsung Ex-1038, 0427

Estonia Patents
Estonia Applications
EUIPO Patents
Finland Patents
Finland Applications
France Patents
France Applications
Germany Patents
Germany Applications
Great Britain Patents
Great Britain Applications
Greece Patents
Greece Applications
Hungary Patents
Hungary Applications
Iceland Patents
Iceland Applications
Ireland Patents
Ireland Applications
Italy Patents
Italy Applications
Latvia Patents
Latvia Applications
Lithuania Patents
Lithuania Applications
Luxembourg Patents
Malta Patents
Monaco Patents
Montenegro Patents
Montenegro Applications
Netherlands Patents
Netherlands Applications
Norway Patents
Norway Applications
Poland Patents
Poland Applications
Portugal Patents
Portugal Applications
Republic of Moldova Patents
Republic of Moldova Applications
Romania Patents
Romania Applications
San Marino Patents
San Marino Applications
Serbia Patents
Serbia Applications
Slovakia Patents
Slovakia Applications

Petitioner Samsung Ex-1038, 0428

Slovenia Patents
Spain Patents
Spain Applications
Sweden Patents
Sweden Applications
Switzerland Patents
Switzerland Applications
Ukraine Patents
Yugoslavia/Serbia and Montenegro Patents
Yugoslavia/Serbia and Montenegro Applications
Armenia Patents
Australia Patents
Australia Applications
Cyprus Patents
Gulf Cooperation Council Patents
Hong Kong Patents
India Patents
India Applications
Indonesia Patents
Indonesia Applications
Israel Applications
Jordan Patents
Kyrgyzstan Patents
Macao Applications
Malaysia Patents
Mongolia Patents
New Zealand Patents
Philippines Patents
Philippines Applications
Saudi Arabia Patents
Singapore Patents
Singapore Applications
Taiwan Patents
Taiwan Applications
Tajikistan Patents
Tajikistan Applications
Thailand Applications
Uzbekistan Patents
Vietnam Patents
Algeria Patents
ARIPO Patents
ARIPO Applications
Egypt Patents
Kenya Patents
Malawi Patents
Morocco Patents
Morocco Applications
OAPI Patents

Petitioner Samsung Ex-1038, 0429

South Africa Patents
Tunisia Applications
Zambia Patents
Zimbabwe Patents
EAPO Patents
EAPO Applications
Georgia Patents
Georgia Applications
Kazakhstan Patents
Kazakhstan Applications
Russia Patents
Russia Applications
Turkey Patents
Turkey Applications

Petitioner Samsung Ex-1038, 0430

Main Concept Document
==========
US20200036521
Title: Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)
Abstract: Methods and systems are provided for supporting efficient and secure “Machine-to-Machine” (M2M) communications using a module, a server, and an application. A module can communicate with the server by accessing the Internet, and the module can include a sensor and/or an actuator. The module, server, and application can utilize public key infrastructure (PKI) such as public keys and private keys. The module can internally derive pairs of private/public keys using cryptographic algorithms and a first set of parameters. A server can authenticate the submission of derived public keys and an associated module identity. The server can use a first server private key and a second set of parameters to (i) send module data to the application and (ii) receive module instructions from the application. The server can use a second server private key and the first set of parameters to communicate with the module.

(No Concept Modifiers)
==========

Filters (1)
==========
Publication Date: To 2013-10-16

Options
==========
De-dup: None
Cut-off: None
Sort: Relevance

Content: Non-Patent Literature (23)
==========
IEEE Xplore Publications: IEEE Periodicals
IEEE Xplore Publications: IEEE Conferences
IEEE Xplore Publications: IEEE Standards
IEEE Xplore Publications: IEEE Early Access
IEEE Xplore Publications: SMPTE Periodicals
IEEE Xplore Publications: SMPTE Conferences
IEEE Xplore Publications: SMPTE Standards
IEEE Xplore Publications: MIT Press eBooks
IEEE Xplore Publications: Wiley-IEEE eBooks
IEEE Xplore Publications: IBM Periodicals

Petitioner Samsung Ex-1038, 0431

IEEE Xplore Publications: URSI Periodicals
IEEE Xplore Publications: VDE Conferences
IEEE Xplore Publications: Periodicals from China
IP.com Prior Art Database: The IP.com Journal
IP.com Prior Art Database: Internet Society RFC
IP.com Prior Art Database: IBM TDB Archive
IP.com Prior Art Database: Legacy Journals
IP.com Prior Art Database: Software Patent Institute
OnePetro.org: Periodicals at OnePetro.org
OnePetro.org: Conferences at OnePetro.org
Other Literature: IBM Redbooks
Other Literature: PubMed Central
Other Literature: arXiv.org

Petitioner Samsung Ex-1038, 0432

Main Concept Text
==========
server authenticating mobile identity using pre-shared key encrypted hash challenge elliptical curve diffie-hellman ECDH

(No Concept Modifiers)
==========

Filters (1)
==========
Publication Date: To 2013-10-16

Options
=======
De-dup: None
Cut-off: None
Sort: Relevance

Content: Non-Patent Literature (23)
==========
IEEE Xplore Publications: IEEE Periodicals
IEEE Xplore Publications: IEEE Conferences
IEEE Xplore Publications: IEEE Standards
IEEE Xplore Publications: IEEE Early Access
IEEE Xplore Publications: SMPTE Periodicals
IEEE Xplore Publications: SMPTE Conferences
IEEE Xplore Publications: SMPTE Standards
IEEE Xplore Publications: MIT Press eBooks
IEEE Xplore Publications: Wiley-IEEE eBooks
IEEE Xplore Publications: IBM Periodicals
IEEE Xplore Publications: URSI Periodicals
IEEE Xplore Publications: VDE Conferences
IEEE Xplore Publications: Periodicals from China
IP.com Prior Art Database: The IP.com Journal
IP.com Prior Art Database: Internet Society RFC
IP.com Prior Art Database: IBM TDB Archive
IP.com Prior Art Database: Legacy Journals
IP.com Prior Art Database: Software Patent Institute
OnePetro.org: Periodicals at OnePetro.org
OnePetro.org: Conferences at OnePetro.org
Other Literature: IBM Redbooks
Other Literature: PubMed Central
Other Literature: arXiv.org

Petitioner Samsung Ex-1038, 0433

Dialog®

STIC
Scientific and Technical Information Center

Report Information from Dialog

July 02 2021 16:12

Petitioner Samsung Ex-1038, 0434

Table of contents

Search Strategy iv

1. A security architecture for IPv6 enabled wireless medical sensor networks 1

2. Security Analysis and Improvements on WLANs 1

3. Energy efficient security framework for wireless local area networks 1

4. A study on wireless network security 1

5. Security Mechanisms for Protecting Foundational Services in Wireless Sensor Networks 1

6. Authentication and key exchange in mobile ad hoc networks 2

7. New Authentication and Key Agreement Protocol for LTE-WLAN Interworking 2

8. Enabling end-to-end secure communication between wireless sensor networks and the Internet 2

9. Energy efficiency and security for multihop wireless networks 2

10. Performance evaluation of security implementation in IEEE 802.15.4 beacon enabled networks 3

11. Secure communication using elliptic curve cryptosystem in ad hoc network 3

12. A Family of Key Agreement Mechanisms for Mission Critical Communications for Secure Mobile Ad Hoc and Wireless Mesh Internetworking 3

13. Key management protocols in hybrid wireless sensor networks 3

14. Performance analysis of elliptic curve cryptography in the IP security protocol 3

15. A Secure TCP Connection Migration Protocol to Enable the Survivability of Client-Server Applications Under Malicious Attack 4

16. Cross-Enterprise Access Control Security for Electronic Health Records: Technical, Practical and Legislation Impact 4

17. Combating dos attacks in wireless networks using lightweight key management schemes 4

18. Cryptanalysis of Arshad et al.'s ECC-based mutual authentication scheme for session initiation protocol 4

19. Compact integrity-aware architectures 5

20. Design and analysis of self-secured, scalable, distributed authentication services for ad hoc networks ... 5

21. Mobile certifying cryptographic file system 5

22. Low overhead bilateral authentication for cellular digital packet data networks 5

23. Elliptic curve cryptography based mutual authentication scheme for session initiation protocol 5

24. Performance evaluation of an authentication solution for IMS services access 6

25. Mitigating botnet-based DDoS attacks against web servers 6

26. Secured Public key Authentication and Energy Efficient MAC Implementation in Wireless Sensor Networks 6

27. A lightweight payment scheme for real-time services based on SIP 6

28. Design and Implementation of a SecureWireless Mote-Based Medical Sensor Network 7

29. SMS Security in Mobile Devices: A Survey 7

30. Flexible Architectures for Enhanced Security 7

31. Efficient, Compromise Resilient and Compact Cryptographic Constructions for Digital Forensics 7

Petitioner Samsung Ex-1038, 0435

Table of contents

32. Broadcast Secrecy via Key-Chain-Based Encryption in Single-Hop Wireless Sensor Networks..... 8

33. Easing PAIN with Digital Signatures..... 8

34. Efficient wireless security protocols based on elliptic curve cryptography..... 8

Petitioner Samsung Ex-1038, 0436

Search Strategy

Databases: ABI/INFORM® Professional Advanced, Abstracts in New Technology & Engineering, AdisInsight: Drugs, AdisInsight: Trials, Adis Pharmacoeconomics & Outcomes News, AGRICOLA, AGRIS, Allied & Complementary Medicine™, Analytical Abstracts, APA PsycInfo®, Aqualine, Aquatic Science & Fisheries Abstracts (ASFA), Australian Education Index, BIOSIS® Toxicology, BIOSIS Previews®, British Library Inside Conferences, British Nursing Index, Business & Industry, CAB ABSTRACTS, Chemical Business Newsbase, Chemical Engineering & Biotechnology Abstracts, Chemical Safety Newsbase, Civil Engineering Abstracts, Current Contents® Search, Derwent Drug File, Derwent Drug Registry, DH-DATA: Health Administration, Medical Toxicology & Environmental Health, DIOGENES® FDA Regulatory Updates, Drug Information Fulltext, Earthquake Engineering Abstracts, EconLit, Ei Compendex®, Ei EnCompassLIT, Embase®, EMCare®, ERIC, ESPICOM Pharmaceutical & Medical Device News, FDAnews, FLUIDEX (Fluid Engineering Abstracts), Foodline®: MARKET, Foodline®: PRODUCT, Foodline®: SCIENCE, FSTA®, Gale Group Computer Database™, Gale Group Health Periodicals Database, Gale Group New Product Announcements / Plus®, Gale Group Newsletter Database™, Gale Group PharmaBiomed Business Journals, Gale Group PROMT®, Gale Group Trade & Industry Database™, GEOBASE, GeoRef, Global Health, HSELINE: Health and Safety, ICONDA - International Construction Database, IMS Company Profiles, IMS New Product Focus, IMS Pharma Trademarks, IMS R&D Focus, IMS R&D Focus Drug News, Inspec®, International Pharmaceutical Abstracts, Jane's Defense & Aerospace News, King's Fund, KOSMET: Cosmetic Science, Lancet Titles, Material Safety Datasheets -OHS™, Mechanical & Transportation Engineering Abstracts, MEDLINE®, Meteorological & Geoastrophysical Abstracts, Morressier Life Science Conference Abstracts and Posters, New England Journal of Medicine, Northern Light Life Sciences Conference Abstracts, NTIS: National Technical Information Service, Oceanic Abstracts, PAIS International, Paperbase, PAPERCHEM, ProQuest Advanced Tech & Aerospace Professional, ProQuest Biological & Health Science Professional, ProQuest Dissertations and Theses Professional, ProQuest Environmental Science Professional, ProQuest Materials Research Professional, ProQuest Newsstand Professional, ProQuest Technology Research Professional, Prous Science Daily Essentials, Prous Science Drug Data Report, Prous Science Drugs Of The Future™, Publicly Available Content, Registry of Toxic Effects of Chemical Substances (RTECS®), SciSearch®: a Cited Reference Science Database, Social SciSearch®, ToxFile®, Transport Research International Documentation, TULSA™ (Petroleum Abstracts), UBM Computer Full Text, Weldasearch®, Zoological Record

Set#	Searched for	Results
S8	(s5 OR s6) and (pd(20010101-20131016))	34°
S7	s5 OR s6	92°
S6	s3 AND ((SIM OR EUICC OR ESIM OR UICC OR module) near/5 (ID or identity OR identifier))	17°
S5	s3 AND ((authenticate OR validate OR verify OR decrypt) near/6 (token OR digest OR hash OR challenge OR nonce))	80°
S4	s3 AND ((authenticate OR validate OR verify) near/6 (decrypt) near/6 (token OR digest OR hash OR challenge OR nonce))	2°
S3	s1 AND s2	402°
S2	(PSK) OR ("pre-shared key") OR (shared near/2 (key OR secret))	185160*
S1	(ECDH) OR (elliptical near/4 diffie)	1478°

Petitioner Samsung Ex-1038, 0437

* Duplicates are removed from the search, but included in the result count.
° Duplicates are removed from the search and from the result count.

Petitioner Samsung Ex-1038, 0438

Document 1 of 34

A security architecture for IPv6 enabled wireless medical sensor networks

Author: Alim, M. Abdul

Publication info: University of Northern British Columbia (Canada). ProQuest Dissertations Publishing, 2008. MR48828.

ProQuest document link

Databases: ProQuest Dissertations and Theses Professional

Document 2 of 34

Security Analysis and Improvements on WLANs

Author: Wang, Li; Srinivasan, Bala; Bhattacharjee, Nandita

Publication info: Journal of Networks, suppl. Special Issue: Recent Network Technologies and its.. 6.3: 470-481. Academy Publisher. (Mar 2011)

ProQuest document link

Databases: ABI/INFORM® Professional Advanced, ProQuest Advanced Tech & Aerospace Professional, ProQuest Technology Research Professional

---

Document 3 of 34

Energy efficient security framework for wireless local area networks

Author: Kiratiwintakorn, Phongsak

Publication info: University of Pittsburgh. ProQuest Dissertations Publishing, 2005. 3188963.

ProQuest document link

Databases: ProQuest Dissertations and Theses Professional

Document 4 of 34

A study on wireless network security

Author: Du, Chunyan

Publication info: University of Massachusetts Lowell. ProQuest Dissertations Publishing, 2007. 1448841.

ProQuest document link

Databases: ProQuest Dissertations and Theses Professional

Document 5 of 34

Security Mechanisms for Protecting Foundational Services in Wireless Sensor Networks

Petitioner Samsung Ex-1038, 0439

Author: Liu, An
Publication info: North Carolina State University. ProQuest Dissertations Publishing, 2010. 3442667.
ProQuest document link

Databases: ProQuest Dissertations and Theses Professional

Document 6 of 34

Authentication and key exchange in mobile ad hoc networks

Author: Hoeper, Katrin
Publication info: University of Waterloo (Canada). ProQuest Dissertations Publishing, 2007. NR36440.
ProQuest document link

Databases: ProQuest Dissertations and Theses Professional

Document 7 of 34

New Authentication and Key Agreement Protocol for LTE-WLAN Interworking

Author: Hassanein, Ahmed H; Abdel Hafez, Ahmed A; A Gaafar, Abd El-hamid
Publication info: International Journal of Computer Applications 61.19 Foundation of Computer Science. (2013)
ProQuest document link

Databases: ProQuest Advanced Tech & Aerospace Professional, ProQuest Technology Research Professional

Document 8 of 34

Enabling end-to-end secure communication between wireless sensor networks and the Internet

Author: Yu, Hong; He, Jingsha; Zhang, Ting; Xiao, Peng; Zhang, Yuqiang
Publication info: World Wide Web 16.4: 515-540. Springer Nature B.V. (Jul 2013)
ProQuest document link

Databases: ProQuest Advanced Tech & Aerospace Professional, ProQuest Technology Research Professional

Document 9 of 34

Energy efficiency and security for multihop wireless networks

Author: Miller, Matthew Jefferson
Publication info: University of Illinois at Urbana-Champaign. ProQuest Dissertations Publishing, 2006. 3250293.
ProQuest document link

Databases: ProQuest Dissertations and Theses Professional

Petitioner Samsung Ex-1038, 0440

Document 10 of 34

Performance evaluation of security implementation in IEEE 802.15.4 beacon enabled networks

Author: Khan, Moazzam
Publication info: University of Manitoba (Canada). ProQuest Dissertations Publishing, 2009. MR63891.
ProQuest document link

Databases: ProQuest Dissertations and Theses Professional

Document 11 of 34

Secure communication using elliptic curve cryptosystem in ad hoc network

Author: Singh, Namita
Publication info: University of Ottawa (Canada). ProQuest Dissertations Publishing, 2008. MR48508.
ProQuest document link

Databases: ProQuest Dissertations and Theses Professional

Document 12 of 34

A Family of Key Agreement Mechanisms for Mission Critical Communications for Secure Mobile Ad Hoc and Wireless Mesh Internetworking

Author: Askoxylakis, Ioannis G; Tryfonas, Theo; May, John; Siris, Vasilios; Traganitis, Apostolos
Publication info: EURASIP Journal on Wireless Communications and Networking Springer Nature B.V. (2011)
ProQuest document link

Databases: ProQuest Advanced Tech & Aerospace Professional, ProQuest Technology Research Professional, Publicly Available Content

Document 13 of 34

Key management protocols in hybrid wireless sensor networks

Author: Wang, Yong
Publication info: The University of Nebraska - Lincoln. ProQuest Dissertations Publishing, 2007. 3277703.
ProQuest document link

Databases: ProQuest Dissertations and Theses Professional

Document 14 of 34

Performance analysis of elliptic curve cryptography in the IP security protocol

Author: Nair, Sreeja S.

Petitioner Samsung Ex-1038, 0441

Publication info: Dalhousie University (Canada). ProQuest Dissertations Publishing, 2003. MQ79518.
ProQuest document link

Databases: ProQuest Dissertations and Theses Professional

Document 15 of 34

A Secure TCP Connection Migration Protocol to Enable the Survivability of Client-Server Applications Under Malicious Attack

Author: Ray, Indrajit; Tideman, Sonja
Publication info: Journal of Network and Systems Management 12.2: 251-276. Springer Nature B.V. (Jun 2004)
ProQuest document link

Databases: ABI/INFORM® Professional Advanced, ProQuest Advanced Tech & Aerospace Professional, ProQuest Technology Research Professional

Document 16 of 34

Cross-Enterprise Access Control Security for Electronic Health Records: Technical, Practical and Legislation Impact

Author: Rodzinka, Mark
Publication info: Rochester Institute of Technology. ProQuest Dissertations Publishing, 2012. 1530829.
ProQuest document link

Databases: ProQuest Dissertations and Theses Professional

Document 17 of 34

Combating dos attacks in wireless networks using lightweight key management schemes

Author: Dong, Qi
Publication info: The University of Texas at Arlington. ProQuest Dissertations Publishing, 2010. 3419457.
ProQuest document link

Databases: ProQuest Dissertations and Theses Professional

Document 18 of 34

Cryptanalysis of Arshad et al.'s ECC-based mutual authentication scheme for session initiation protocol

Author: Tang, Hongbin; Liu, Xinsong
Publication info: Multimedia Tools and Applications 65.3: 321-333. Springer Nature B.V. (Aug 2013)
ProQuest document link

Petitioner Samsung Ex-1038, 0442

Databases: ABI/INFORM® Professional Advanced, ProQuest Advanced Tech & Aerospace Professional, ProQuest Technology Research Professional

Document 19 of 34

Compact integrity-aware architectures

Author: LeMay, Michael D.
Publication info: University of Illinois at Urbana-Champaign. ProQuest Dissertations Publishing, 2011. 3496699.
ProQuest document link

Databases: ProQuest Dissertations and Theses Professional

Document 20 of 34

Design and analysis of self-secured, scalable, distributed authentication services for ad hoc networks

Author: Ghorpade, Vijay R.
Publication info: Swami Ramanand Teerth Marathwada University (India). ProQuest Dissertations Publishing, 2007. 13848566.
ProQuest document link

Databases: ProQuest Dissertations and Theses Professional

Document 21 of 34

Mobile certifying cryptographic file system

Author: Guo, Hong
Publication info: University of Ottawa (Canada). ProQuest Dissertations Publishing, 2006. MR18422.
ProQuest document link

Databases: ProQuest Dissertations and Theses Professional

Document 22 of 34

Low overhead bilateral authentication for cellular digital packet data networks

Author: Hatefi, Farid G.
Publication info: Arizona State University. ProQuest Dissertations Publishing, 2003. 3112563.
ProQuest document link

Databases: ProQuest Dissertations and Theses Professional

Document 23 of 34

Petitioner Samsung Ex-1038, 0443

Elliptic curve cryptography based mutual authentication scheme for session initiation protocol

Author: Arshad, R; Ikram, N

Publication info: Multimedia Tools and Applications 66.2: 165-178. Springer Nature B.V. (Sep 2013)

ProQuest document link

Databases: ABI/INFORM® Professional Advanced, ProQuest Advanced Tech & Aerospace Professional, ProQuest Technology Research Professional

Document 24 of 34

Performance evaluation of an authentication solution for IMS services access

Author: Song, Songbo; Abid, Mohamed; Moustafa, Hassnaa; Afifi, Hossam

Publication info: Telecommunication Systems 52.4: 2205-2218. Springer Nature B.V. (Apr 2013)

ProQuest document link

Databases: ABI/INFORM® Professional Advanced, ProQuest Advanced Tech & Aerospace Professional, ProQuest Technology Research Professional

Document 25 of 34

Mitigating botnet-based DDoS attacks against web servers

Author: Djalaliev, Peter L.

Publication info: University of Pittsburgh. ProQuest Dissertations Publishing, 2013. 3577083.

ProQuest document link

Databases: ProQuest Dissertations and Theses Professional

Document 26 of 34

Secured Public key Authentication and Energy Efficient MAC Implementation in Wireless Sensor Networks

Author: Challa, Manoj; Reddy, P Venkata Subba; Reddy, M Damodar; Mungara, Jitendra Nath

Publication info: International Journal of Computer Science and Network Security (IJCSNS) 12.8: 84-89. International Journal of Computer Science and Network Security. (Aug 2012)

ProQuest document link

Databases: ProQuest Advanced Tech & Aerospace Professional, ProQuest Technology Research Professional

Document 27 of 34

A lightweight payment scheme for real-time services based on SIP

Author: Ruiz-martínez, Antonio; Marín-lópez, C Inmaculada

Petitioner Samsung Ex-1038, 0444

Publication info: EURASIP Journal on Wireless Communications and Networking 2012 : 1-25. Springer Nature B.V. (May 2012)
ProQuest document link

Databases: ProQuest Advanced Tech & Aerospace Professional, ProQuest Technology Research Professional, Publicly Available Content

Document 28 of 34

Design and Implementation of a SecureWireless Mote-Based Medical Sensor Network

Author: Malasri, Kriangsiri; Wang, Lan
Publication info: Sensors 9.8: 6273-6297. MDPI AG. (2009)
ProQuest document link

Databases: ProQuest Advanced Tech & Aerospace Professional, Mechanical & Transportation Engineering Abstracts, ProQuest Technology Research Professional, Publicly Available Content

Document 29 of 34

SMS Security in Mobile Devices: A Survey

Author: Khan, Muhammad Waseem
Publication info: International Journal of Advanced Networking and Applications 5.2: 1873-1882. Eswar Publications. (Sep/Oct 2013)
ProQuest document link

Databases: ProQuest Advanced Tech & Aerospace Professional, ProQuest Technology Research Professional, Publicly Available Content

Document 30 of 34

Flexible Architectures for Enhanced Security

Author: Chang, Jed Kao-Tung
Publication info: University of California, Irvine. ProQuest Dissertations Publishing, 2012. 3518799.
ProQuest document link

Databases: ProQuest Dissertations and Theses Professional

Document 31 of 34

Efficient, Compromise Resilient and Compact Cryptographic Constructions for Digital Forensics

Author: Yavuz, Attila Altay
Publication info: North Carolina State University. ProQuest Dissertations Publishing, 2011. 3479590.

Petitioner Samsung Ex-1038, 0445

ProQuest document link

Databases: ProQuest Dissertations and Theses Professional

Document 32 of 34

Broadcast Secrecy via Key-Chain-Based Encryption in Single-Hop Wireless Sensor Networks

Author: Sivaraman, Vijay; Ostry, Diethelm; Shaheen, Jaleel; Antoni Junior Hianto; Jha, Sanjay
Publication info: EURASIP Journal on Wireless Communications and Networking Springer Nature B.V. (2011)
ProQuest document link

Databases: ProQuest Advanced Tech & Aerospace Professional, ProQuest Technology Research Professional, Publicly Available Content

Document 33 of 34

Easing PAIN with Digital Signatures

Author: Banday, M Tariq
Publication info: International Journal of Computer Applications 29.2 Foundation of Computer Science. (2011)
ProQuest document link

Databases: ProQuest Advanced Tech & Aerospace Professional, ProQuest Technology Research Professional

Document 34 of 34

Efficient wireless security protocols based on elliptic curve cryptography

Author: Aydos, Murat
Publication info: Oregon State University. ProQuest Dissertations Publishing, 2001. 3005501.
ProQuest document link

Databases: ProQuest Dissertations and Theses Professional

Contact ProQuest
Copyright © 2021 ProQuest LLC. All rights reserved. - **Terms and Conditions**

Petitioner Samsung Ex-1038, 0446

Google Scholar | server authenticating mobile identity pre-shared key encrypted hash elliptical curve diffie-hellman ECDH | SIGN IN

Articles | About 81 results (0.07 sec) | My profile | My library

Any time
Since 2021
Since 2020
Since 2017
Custom range...
— 2013

Sort by relevance
Sort by date

include patents
include citations

Create alert

[HTML] A new provably **secure authentication** and **key** agreement protocol for SIP using ECC — [HTML] sciencedirect.com

L Wu, Y Zhang, F Wang - Computer Standards & Interfaces, 2009 - Elsevier

... The other is the requirement of pre-existing user configuration on **servers** ... Fig. 2 is a message flow describing a Digest AKE process of **authenticating** a SIP REGISTER request ... 7. **Server** responds with appropriate error message or grants access ...

Cited by 132 Related articles All 10 versions

[HTML] SE-AKA: A **secure** and efficient group **authentication** and **key** agreement protocol for LTE networks — [HTML] sciencedirect.com

C Lai, H Li, R Lu, XS Shen - Computer Networks, 2013 - Elsevier

... MAC MME ' is not the same MAC MME , the HSS or the MME **server** is not ... the length of AV is 640 bits, therefore occupied storage space for **authenticating** n ME ... and KFS/KBS, but also provide a group **authentication** mechanism which can effectively **authenticate** group devices ...

Cited by 163 Related articles All 6 versions

An ECC based public **key** infrastructure usable for **mobile** applications — [PDF] acm.org

S Ray, GP Biswas - Proceedings of the second international conference ..., 2012 - dl.acm.org

... To copy otherwise, or republish, to post on **servers** or to redistribute to lists, requires prior ... to generate a public **key** certificate for a user containing a valid and **authenticate** public **key** with ... RA and used by the **mobile** phone user, the mutual **authentication** of both **server** and **mobile** ...

Cited by 13 Related articles All 2 versions

Multilayer consensus ECC-based password **authenticated** **key**-exchange (MCEPAK) protocol for smart grid system — [PDF] ieee.org

H Nicanfar, VCM Leung - IEEE Transactions on Smart Grid, 2013 - ieeexplore.ieee.org

... to keep the password table in **server** side in order to reduce the side effect of compro- mising the **server** ... To perform the **key** validation using AVISPA and evaluate it by the back-end **servers**, the protocol and mechanisms are ... [18] "Password-**Authenticated Key** Exchange (PAK ...

Cited by 70 Related articles All 3 versions

[HTML] Cryptanalysis of Arshad et al.'s ECC-based mutual **authentication** scheme for session initiation protocol — [HTML] springer.com Full View

H Tang, X Liu - Multimedia tools and applications, 2013 - Springer

... Proof: Mutual **authentication** means that both the user and the **server** are **authenticated** to each other within ... **server** can make a correct response to the user's challenge R 1 . **Server** can **authenticate** the user ... Computation cost of the user and the **server** are 2 PM + 1 HP + 1 PA + 3 ...

Cited by 47 Related articles All 10 versions

[PDF] Design of **mobile** public **key** infrastructure (M-PKI) using **elliptic curve cryptography** — [PDF] academia.edu

S Ray, GP Biswas - International Journal on Cryptography and ..., 2013 - academia.edu

... to generate a public **key** certificate for a user containing a valid and **authenticate** public **key** ... In our proposed ECC-based M-PKI, initially, MHA should be **authenticated** to RA to ensure ... RA and used by the **mobile** phone user, the mutual **authentication** of both **server** and **mobile** ...

Cited by 8 Related articles All 3 versions

A survey of SIP **authentication** and **key** agreement schemes — [PDF] ieee.org

HH Kilinc, T Yanik - IEEE Communications Surveys & Tutorials, 2013 - ieeexplore.ieee.org

... The proposed scheme is based on **authenticating** the client with the outbound proxy **server** ... Besides, these **servers** have the required public-**key** certificates which are given by domain authorities ... Then, the registrar **server** computes a **hash** value r using the large number N and its ...

Cited by 197 Related articles All 2 versions

A Trustable **Key** Exchange Protocol for **Mobile** Oriented VoIP Devices via **ECDH** and Synchronous **Key** Update Mechanism — [PDF] sciencedirect.com

Petitioner Samsung Ex-1038, 0447

D Chandirasekaran, G Achila, P Thivagaraian - Procedia engineering, 2012 - Elsevier
... Typically the User Agent **Servers** register themselves with a registrar, this registration information is required by the ... **Key** Continuity A "baby duck security" model is used by ZRTP to **authenticate** the **Diffie** ... to exploit vulnerability and to take over an existing SIP proxy **server** [4]. Now ...
Cited by 1 Related articles All 2 versions

[HTML] A **secure** and efficient SIP **authentication** scheme for converged VoIP networks [HTML] sciencedirect.com

EJ Yoon, KY Yoo, C Kim, YS Hong, M Jo... - Computer ..., 2010 - Elsevier
... The illegal attacker Eve cannot pretend to be U or S to **authenticate** since she does not own the mutual password ... **Servers** are always the target of attacks ... If the client's password pw and the **server's secret key** x are compromised, it does not allow an attacker Eve to determine the ...
Cited by 104 Related articles All 9 versions

[PDF] Enabling end-to-end **secure** communication between wireless sensor networks and the Internet [PDF] springer.com Full View

H Yu, J He, T Zhang, P Xiao, Y Zhang - World Wide Web, 2013 - Springer
... 1) During **authentication**, the fact that **servers** are always ... If an attacker injects fake request messages with an invalid **identity**, the sensor node cannot **authenticate** the validity of the certificate as well as the ... Hoa, NT, Naoe, K., Takefuji, Y.: Micro **secure** socket layer for micro **server** ...
Cited by 46 Related articles All 5 versions

Petitioner Samsung Ex-1038, 0448

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20140143826	A1	2014-05-22	Sharp et al.	
	2	20140161113	A1	2014-06-12	Cui et al.	
	3	20140165155	A1	2014-06-12	Zhang	
	4	20140192976	A1	2014-07-10	Yoon et al.	
	5	20140219447	A1	2014-08-07	Park et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	6	20140219448	A1	2014-08-07	Froels et al.	
	7	20140244994	A1	2014-08-28	Yu	
	8	20140273913	A1	2014-09-18	Michel et al.	
	9	20140287725	A1	2014-09-25	Lee	
	10	20140337937	A1	2014-11-13	Truskovsky et al.	
	11	20140351403	A1	2014-11-27	Lein et al.	
	12	20150012743	A1	2015-01-08	Holtmanns et al.	
	13	20150017910	A1	2015-01-15	Li et al.	
	14	20150071139	A1	2015-03-12	Nix	
	15	20150092590	A1	2015-04-02	Zhu et al.	
	16	20150095514	A1	2015-04-02	Yu	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	17	20150095648	A1	2015-04-02	Nix	
	18	20150113275	A1	2015-04-23	Kim et al.	
	19	20150121495	A1	2015-04-03	Gao et al.	
	20	20130231087	A1	2013-09-05	O'Leary	
	21	20130165073	A1	2013-06-27	Madsen	
	22	20130007442	A1	2013-01-03	Mao et aL	
	23	20120170451	A1	2012-07-05	Viswanathan et aL	
	24	20120084568	A1	2012-08-05	Sarikaya et al.	
	25	20120030461	A1	2012-02-02	Willey et al.	
	26	20080307218	A1	2008-12-11	Logvinov	
	27	20110035584	A1	2011-02-10	Meyerstein et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	28	20090060197	A1	2009-03-05	Taylor et al.	
	29	20150089214	A1	2015-03-26	Dupre	
	30	20140122878	A1	2014-05-01	Cho et al.	
	31	20140115335	A1	2014-04-24	Jorden et al.	
	32	20130173926	A1	2013-07-04	Morese et al.	
	33	20130012168	A1	2013-01-10	Rajadurai et al.	
	34	20120331298	A1	2012-12-27	Xu et al.	
	35	20120190354	A1	2012-07-26	Merrien et al.	
	36	20040221163	A1	2004-11-04	Jorgensen et al.	
	37	20090113203	A1	2009-04-30	Tsuge et al.	
	38	20150163056	A1	2015-06-11	Nix	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	39	20090217348	A1	2009-08-27	Salmela et al.	
	40	20080130879	A1	2008-06-05	Heinonen et al.	
	41	20130122864	A1	2013-05-16	Haggerty et al.	
	42	20150071139	A1	2015-03-12	Nix	
	43	20150095648	A1	2015-04-02	Nix	
	44	20150106616	A1	2015-04-16	Nix	
	45	20150121066	A1	2015-04-30	Nix	
	46	20150143125	A1	2015-05-21	Nix	
	47	20040162472	A1	2004-08-19	Berson et al.	
	48	20150215126	A1	2015-07-30	Ashdown	
	49	20160294829	A1	2016-10-06	Angus	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	50	20110269422	A1	2011-11-03	Xu et al.	
	51	20110269461	A1	2011-11-03	Xu et al.	
	52	20110269472	A1	2011-11-03	Xu et al.	
	53	20110270747	A1	2011-11-03	Xu et al.	
	54	20130294602	A1	2013-11-07	Huxham et al.	
	55	20130340040	A1	2013-12-19	Park et al.	
	56	20140308991	A1	2014-10-16	Lee et al.	
	57	20140329502	A1	2014-11-06	Lee et al.	
	58	20150281964	A1	2015-10-01	Seo et al.	
	59	20070158439	A1	2007-07-12	Conner et al.	
	60	20130183932	A1	2013-07-18	Lemilainen et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

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

EXAMINER SIGNATURE

Examiner Signature	/David J Pearson/	Date Considered	04/11/2022

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20150106616	A1	2015-04-16	Nix	
	2	20150121066	A1	2015-04-30	Nix	
	3	20150143125	A1	2015-05-21	Nix	
	4	20040162472	A1	2004-08-19	Berson et al.	
	5	20150215126	A1	2015-07-30	Ashdown	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	6	20160294829	A1	2016-10-06	Angus	
	7	20120108205	A1	2012-05-03	Schell et al.	
	8	20130012168	A1	2013-01-10	Rajadurai et al.	
	9	20140219447	A1	2014-08-07	Park et al.	
	10	20140161113	A1	2014-06-12	Cui et al.	
	11	20150113275	A1	2015-04-23	Kim et al.	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	10-2013-0026352	KR	A	2013-03-13	KT CORPORATION		
	2	10-2013-0026958	KR	A	2013-03-14	KT CORPORATION		
	3	19 81 224	EP	A1	2008-10-15	Samsung Electronics Co., Ltd.		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	4	2013027085	WO	A1	2013-02-28	Nokia Corporation et al.		
	5	2013066077	WO	A1	2013-05-10	KT CORPORATION		
	6	2775853	CA	A1	2012-12-01	BlackBerry Ltd.		
	7	2011138238	WO	A1	2011-11-10	Alcatel Lucent		

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	International Search Report for PCT/US2014/068544 dated February 13, 2015.	
	2	T. Pornin, Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm ECDSA), Internet Engineering Task Force RFC 6979, August 2013, pp.I-79.	
	3	GSMA, Fast Dormancy Best Practices Version 1.0,27 July 2011, TS.18, pp. 1-23.	
	4	N. CHU et al, EXALTED: Expanding LTE for Devices, European Commission for Information Society and Media, 31 October 2012, pp. 1-141.	
	5	J. HUANG et al, A Close Examination of Performance and Power Characteristics of 4G LTE Networks, Mobisys' 12, 25-29 June 2012, pp. 1-14.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	6	F. QIAN et al, TOP: Tail Optimization Protocol for Cellular Resource Allocation, 18th IEEE International Conference on Network Protocols (ICNP), 2010, 5-8 Oct. 2010, pp. 285-298.
	7	ETSI, Machine-to-Machine communications (M2M), mia, dla, and mid interfaces, TS 102.921 v1.1.1, Feb 2012, pp. 1-538.
	8	C. DOWNEY, Migrating Legacy M2M Systems to the Cloud, http://www.ecnmag.com/articles/2013/02/migrating-legacy-m2m-systems-cloud, Feb 2013, pp. 1-2.
	9	A. Wander et al, Energy Analysis of Public-Key Cryptography on Small Wireless Devices, Sun Microsystems Laboratories, pp.1-16. 2005
	10	V. Martinez et al, A Survey of the Elliptic Curve Integrated Encryption Scheme, Journal of Computer Science and Engineering, Volume 2, August 2010, pp.7-13.
	11	ETSI, UMTS;LTE; SIM/USIM Internal and External Interworking Aspects, TR 131900 v.10.0.0, May 2011, pp.1-41.
	12	International Search Report and Written Opinion for PCT/US2014/062435 mailed February 6, 2015.
	13	Wikipedia, RSA (algorithm), http://en.wikipedia.org/wiki/RSA_(algorithm), 9 Sept. 2013, pp. 1-12.
	14	Wikipedia, Elliptic Curve Cryptography, http://en.wikipedia.org/wiki/Elliptic_curve_cryptography, 9 Sept. 2013, pp. 1-8 .
	15	L. LARZON, The Lightweight User Datagram Protocol (UDP-Lite), Internet Engineering Task Force RFC 3828, July 2004, pp. 1-12.
	16	Wikipedia, Digital Signature, http://en.wikipedia.orglwiki/Digital_signature, 9 Sept. 2013, pp. 1-10.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	17	D. Cooper, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Internet Engineering Task Force RFC 5280, pp. 1-133. 2008
	18	J. Jonsson et al, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, Internet Engineering Task Force RFC 3447, February 2003, pp.1-72.
	19	D. McGrew et al, Fundamental Elliptic Curve Cryptography Algorithms, Internet Engineering Task Force RFC 6090, February 2011, pp. 1-34.
	20	Wikipedia, Elliptic Curve Diffie-Hellman, http://en.wikipedia.org/wiki/Elliptic_curve_Diffie%E2%80%93Hellman, 24 Sept. 2013, pp. 1-2.
	21	ETSI, Smart Cards; Embedded UICC; Requirements Specification, TS 103 383 v12.1.0, June 2013, pp. 1-20.
	22	3GPP, 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture, 3GPP TS 33.401 V12.9.0 (2013-09) pp. 1-75.
	23	3GPP, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3, 3GPP TS 24.301 v12.2.0, Sept. 2013 pp. 1-6, 63-100.
	24	ETSI, Smart Cards; UICC-Terminal Interfaces; Physical and Logical Characteristics, TS 102 221 v11.0.0, June 2012, pp. 1-181.

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

EXAMINER SIGNATURE

Examiner Signature	/David J Pearson/	Date Considered	04/11/2022

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	9807605	B2	2017-10-31	Gao et al.	
	2	8577337	B2	2013-11-05	O'Leary	
	3	9800993	B2	2013-11-05	Lee et al.	
	4	9794775	B2	2017-10-17	Huber et al.	
	5	9674690	B2	2017-06-06	Lee et al.	
	6	9628981	B2	2017-04-18	Park et al.	
	7	9572016	B2	2017-02-14	Cormier et al.	
	8	9332129	B2	2016-05-03	Li et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	9	9270653	B2	2016-02-23	Maria	
	10	6804357	B1	2004-10-12	Ikonen et al.	
	11	9923724	B2	2018-03-20	Lee et al.	
	12	6842628	B1	2005-01-11	Arnold et al.	
	13	8352739	B2	2013-01-08	Park et al.	
	14	6721886	B1	2004-04-13	Uskela	
	15	5995625	A	1999-11-30	Sudia et al.	
	16	5852665	A	1998-12-22	Gressel et al.	
	17	5664017	A	1997-09-02	Gressel et al.	
	18	5642420	A	1997-06-24	Kuroda et al.	
	19	5216715	A	1993-06-01	Markwitz	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	20	6256733	B1	2001-07-03	Thakkar et al.	
	21	9020479	B1	2015-04-28	Somayajula et al.	
	22	8965366	B1	2015-02-24	Somayajula et al.	
	23	8452017	B2	2013-05-28	Sherkin	
	24	7957532	B2	2011-06-07	Chen et al.	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20110213959	A1	2011-09-01	Bodi et al.	
	2	20130344864	A1	2013-12-26	Park et al.	
	3	20140082359	A1	2014-03-20	Nakhjiri et al.	
	4	20140120874	A1	2014-05-01	Kang et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	5	20140329502	A1	2014-11-06	Lee et al.	
	6	20150350881	A1	2015-12-03	Weiss et al.	
	7	20130283047	A1	2013-10-24	Merrien et al.	
	8	20120263298	A1	2012-10-18	Suh et al.	
	9	20080044032	A1	2008-02-21	Lou et al.	
	10	20050058294	A1	2005-03-17	Chen et al.	
	11	20160088096	A1	2016-03-24	Quiriconi et al.	
	12	20120190354	A1	2012-07-23	Merrien et al.	
	13	20110035604	A1	2011-02-10	Habraken	
	14	20140237101	A1	2014-08-21	Park	
	15	20140235210	A1	2014-08-21	Park et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	16	20140219447	A1	2014-08-07	Park et al.	
	17	20140140507	A1	2014-05-22	Park et al.	
	18	20140082358	A1	2014-03-20	Nakhjiri et al.	
	19	20150281964	A1	2015-10-01	Seo et al.	
	20	20150121495	A1	2015-04-30	Gao et al.	
	21	20140308991	A1	2014-10-16	LEE et al.	
	22	20130340040	A1	2013-12-19	Park et al.	
	23	20130122864	A1	2013-05-16	Haggerty et al.	
	24	20110270747	A1	2011-11-03	Xu	
	25	20160057725	A1	2016-02-25	Suh	
	26	20160149903	A1	2016-05-26	Suh	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	27	20130157673	A1	2013-06-20	Brusilovsky	
	28	20110268022	A1	2011-11-03	Xu	
	29	20160127132	A1	2016-05-05	Lee et al.	
	30	20140357229	A1	2014-12-04	Lee et al.	
	31	20130227646	A1	2013-08-29	Haggerty et al.	
	32	20130012168	A1	2013-01-10	Rajadurai et al.	
	33	20130294602	A1	2013-11-07	Huxham et al.	
	34	20140003604	A1	2014-01-02	Campagna et al.	
	35	20110269461	A1	2011-11-03	Xu et al.	
	36	20110269472	A1	2011-11-03	Xu et al.	
	37	20110269422	A1	2011-11-03	Xu et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	38	20120011362	A1	2012-01-12	Lambert	
	39	20060129848	A1	2006-06-15	Paksoy et al.	
	40	20120087493	A1	2012-04-12	Chidambaram et al.	
	41	20080107083	A1	2008-05-08	Shirota et al.	
	42	20130165075	A1	2013-06-27	Rishy-Maharaj et al.	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	ANSI X9.63 Overview, Key Agreement and Key Transport Using Elliptic Curve Cryptography, Simon Blake-Wilson, Certicom (2000)	

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

EXAMINER SIGNATURE

Examiner Signature	/David J Pearson/	Date Considered	04/11/2022

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20060206710	A1	2006-09-14	Gehrmann	
	2	20060281442	A1	2006-12-14	Lee et al.	
	3	20070206799	A1	2007-09-06	Wingert et al.	
	4	20080016230	A1	2008-01-17	Hollmanns et al.	
	5	20080022089	A1	2008-01-24	Leedom	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	6	20080114978	A1	2008-05-15	Lehtoviorta et al.	
	7	20080165698	A1	2008-07-10	Dalsgard et al.	
	8	20090116642	A1	2009-05-07	Yang et al.	
	9	20090028341	A1	2009-01-29	Hamachi	
	10	20090077643	A1	2009-03-19	Schmidt et al.	
	11	20090125996	A1	2009-05-14	Guccione et al.	
	12	20090132806	A1	2009-05-21	Blommaert et al.	
	13	20090191857	A1	2009-07-30	Horn et al.	
	14	20090209232	A1	2009-08-20	Cha et al.	
	15	20090268909	A1	2009-10-29	Girao et al.	
	16	20090282246	A1	2009-11-12	Gunther	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	17	20090313472	A1	2009-12-17	Guccione et al.	
	18	20100166167	A1	2010-07-01	Karimi-Cherkandi et al.	
	19	20100031042	A1	2010-02-04	Di Crescenzo et al.	
	20	20100062808	A1	2010-03-11	Cha et al.	
	21	20100098253	A1	2010-04-22	Delerablee	
	22	20100275028	A1	2010-10-28	Takashima	
	23	20110016321	A1	2011-01-20	Sundaram et al.	
	24	20110055553	A1	2011-03-03	Lee et al.	
	25	20110237281	A1	2011-09-20	Busropan et al.	
	26	20110291803	A1	2011-12-01	Bajic et al.	
	27	20110314287	A1	2011-12-22	Escott et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	28	20120011360	A1	2012-01-12	Engels et al.	
	29	20120023336	A1	2012-01-26	Natarajan	
	30	20120072732	A1	2012-03-22	Canard et al.	
	31	20120089568	A1	2012-04-12	Manley et al.	
	32	20120108205	A1	2012-05-03	Schell et al.	
	33	20120117635	A1	2012-05-10	Schell et al.	
	34	20120159153	A1	2012-06-21	Shim et al.	
	35	20120260086	A1	2012-10-11	Haggerty et al.	
	36	20120260090	A1	2012-10-11	Hauck et al.	
	37	20120260095	A1	2012-10-11	Von Hauck et al.	
	38	20120278490	A1	2012-11-01	Sennett et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	39	20120300932	A1	2012-11-29	Cambridge et al.	
	40	20120331292	A1	2012-12-27	Haggerty et al.	
	41	20130091556	A1	2013-04-11	Horn et al.	
	42	20130114810	A1	2013-05-09	Kobayashi et al.	
	43	20130117824	A1	2013-05-09	Naslund et al.	
	44	20130149996	A1	2013-06-13	King et al.	
	45	20130166915	A1	2013-06-27	desai et al.	
	46	20130173747	A1	2013-07-04	Kim et al.	
	47	20130212637	A1	2013-08-15	Guccione et al.	
	48	20130227646	A1	2013-08-29	Haggerty et al.	
	49	20130305345	A1	2013-11-14	Bugenhagen	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	50	20130322621	A1	2013-12-05	Yoon et al.	
	51	20130331063	A1	2013-12-12	Cormier et al.	
	52	20140003604	A1	2014-01-02	Campagna et al.	
	53	20140053241	A1	2014-02-20	Norman et al.	
	54	20140073375	A1	2014-03-13	Li et al.	
	55	20140082358	A1	2014-03-20	Nakhjiri et al.	
	56	20140082359	A1	2014-03-20	Nakhjiri et al.	
	57	20140087790	A1	2014-03-27	Babbage et al.	
	58	20140101444	A1	2014-04-10	Lee et al.	
	59	20140108801	A1	2014-04-17	McBride et al.	
	60	20140140507	A1	2014-05-22	Park et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

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

EXAMINER SIGNATURE

Examiner Signature	/David J Pearson/	Date Considered	04/11/2022

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8127142	B2	2012-02-28	Cuppett	
	2	8522013	B2	2013-08-27	Zhang et al.	
	3	8843179	B2	2014-09-23	Li et al.	
	4	9408012	B2	2016-08-02	Li et al.	
	5	8924715	B2	2014-12-30	Schell et al.	
	6	9698981	B2	2017-07-04	Nix	
	7	9596078	B2	2017-03-14	Nix	
	8	8434139	B1	2013-04-30	Ortiz, Jr.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	9	8965366	B1	2015-02-24	Somayajula et al.	
	10	9020479	B1	2015-04-28	Somayajula et al.	
	11	9253643	B2	2016-02-02	Pattar et al.	
	12	6038322		2000-03-14	Harkins	
	13	7921292	B1	2011-04-05	Pauker et al.	
	14	8526606	B2	2013-09-03	Muthaiah	
	15	8555067	B2	2013-10-08	Schell et al.	
	16	8590028	B2	2013-11-19	Saxena et al.	
	17	8782774	B1	2014-07-15	Pahl et al.	
	18	8948386	B2	2015-02-03	Campagna et al.	
	19	9002018	B2	2015-04-07	Wilkins et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	20	9253643	B2	2016-02-02	Pattar et al.	
	21	8434139	B1	2013-04-30	Ortiz, Jr.	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20140281483	A1	2014-09-18	Vigliaturo et al.	
	2	20130179962	A1	2013-07-11	Arial et al.	
	3	20080031204	A1	2008-02-07	Sood	
	4	20090041110	A1	2009-02-12	Malladi	
	5	20090282246	A1	2009-11-12	Gunther	
	6	20090274306	A1	2009-11-05	Nolte	
	7	20140140509	A1	2014-05-22	Chastain et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	8	20140143534	A1	2014-05-22	Chastain et al.	
	9	20140237101	A1	2014-08-21	Park	
	10	20140235210	A1	2014-08-21	Park et al.	
	11	20060095771	A1	2006-05-04	Appenzeller et al.	
	12	20100223461	A1	2010-09-02	Drader et al.	
	13	20100199334	A1	2010-08-05	Ehrensvard et al.	
	14	20140040628	A1	2014-02-06	Fort et al.	
	15	20070101400	A1	2007-05-03	Freeman et al.	
	16	20160014112	A1	2016-01-14	Gunning et al.	
	17	20150222619	A1	2015-08-06	Hughes et al.	
	18	20010029581	A1	2001-10-11	Knauft	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	19	20140049653	A1	2014-02-20	Leonard et al.	
	20	20120214444	A1	2012-08-23	McBride et al.	
	21	20050050323	A1	2005-03-03	Mizrah	
	22	20090183541	A1	2009-07-23	Sadighi et al.	
	23	20100195833	A1	2010-08-05	Priestley et al.	
	24	20150222604	A1	2015-08-06	Ylonen	
	25	20110268022	A1	2011-11-03	Xu	
	26	20140357229	A1	2014-12-04	Lee et al.	
	27	20110167272	A1	2011-07-07	Kolesnikov	
	28	20160127132	A1	2016-05-05	Lee et al.	
	29	20170206532	A1	2017-07-20	Choi	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	30	20160294829	A1	2016-10-06	Angus	
	31	20150215126	A1	2015-07-30	Ashdown	
	32	20040162472	A1	2004-08-19	Berson et al.	
	33	20110269422	A1	2011-11-03	Xu et al.	
	34	20110269461	A1	2011-11-03	Xu et al.	
	35	20110269472	A1	2011-11-03	Xu et al.	
	36	20110270747	A1	2011-11-03	Xu	
	37	20130294602	A1	2013-11-07	Huxham et al.	
	38	20130340040	A1	2013-12-19	Park et al.	
	39	20140308991	A1	2014-10-16	Lee et al.	
	40	20140329502	A1	2014-10-06	Lee et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	41	20150281964	A1	2015-10-01	Seo et al.	
	42	20070158439	A1	2007-07-12	Conner et al.	
	43	20130183932	A1	2013-07-18	Lemilainen et al.	
	44	20120033613	A1	2012-02-09	Lin et al.	
	45	20130028184	A1	2013-01-31	Lee et al.	
	46	20130182586	A1	2013-07-18	Paladugu et al.	
	47	20020018569	A1	2002-02-14	Panjwani et al.	
	48	20030003895	A1	2003-01-02	Wallentin et al.	
	49	20030211842	A1	2003-11-13	Kempf et al.	
	50	20040179684	A1	2004-09-16	Appenzeller et al.	
	51	20050008159	A1	2005-01-13	Grilli et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	52	20050021875	A1	2005-01-27	Bouthemy et al.	
	53	20050120202	A1	2005-06-02	Cuellar et al.	
	54	20050138353	A1	2005-06-23	Spies et al.	
	55	20050193199	A1	2005-09-01	Asokan et al.	
	56	20050246282	A1	2005-11-03	Naslund et al.	
	57	20050278787	A1	2005-12-15	Naslund et al.	
	58	20060021063	A1	2006-01-26	Hori	
	59	20060056355	A1	2006-03-16	Love et al.	
	60	20060059344	A1	2006-03-16	Mononen	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	1							

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	Cakulev et al., "An EAP Authentication Method Based on Identity-Based Authenticated Key Exchange," August 2012, pp. 1-32.	
	2	Gollmann, "Authentication - Myths and Misconceptions," Progress in Computer Science and Applied Logic, Vol. 20, 2001, pp. 203-225.	
	3	Tin et al., "Provably Secure Mobile Key Exchange: Applying the Canetti-Krawczyk Approach," Information Security Research Centre, Queensland University of Technology, Australia, 2003, pp. 166-179.	
	4	Hegland et al., "A Framework for Authentication in NBD Tactical Ad Hoc Networks," IEEE Communications Magazine, October 2011, pp. 64-71.	
	5	Nicholson et al., "Mobile Device Security Using Transient Authentication," IEEE Transactions on Mobile Computing, Vol. 5, No.II, November 2006, pp.1489-1502.	
	6	Schwaiger et al., "Smart Card Security for Fieldbus Systems," 2003, pp. 398-406.	
	7	CSMG, Reprogrammable SIMs: Technology, Evolution and Implications, 25 SEP 2012, pp. 1-95.	
	8	GlobalPlatform Inc., GlobalPlatform Card Specification, Version 2.2.1, JAN 2011, pp. 1-303.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	9	GlobalPlatform Inc., GlobalPlatform Card Security Upgrade for Card Content Management, Card Specification v 2.2. - Amendment E, Version 1.0, NOV 2011, pp. 1-35.
	10	GSM Association, Embedded SIM Task Force Requirements and Use Cases, Version 1.0, 21 FEB 2011, pp. 1-38.
	11	Kirk H.M. Wong et al., A Dynamic User Authentication Scheme for Wireless Sensor Networks, Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), pp. 1-8.
	12	Pierre E. ABI-CHAR, et al., A Fast and Secure Elliptic Curve Based Authenticated Key Agreement Protocol For Low Power Mobile Communications, The 2007 International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST 2007), pp. 1-6.
	13	Jun Shao, et al., An Improved Deniable Authentication Protocol, Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200030, People's Republic of China, pp. 1-3. 2006
	14	Chris Foresman, Embedded SIM could cause carrier conflict for Apple, November 19, 2010, pp. 1-2.
	15	Embedded UICC Remote Provisioning Discussion, Source: Rogers Wireless, 3GPP/SA3-LI#46, Quebec City, Canada, July 17-19, 2012, p. 1-39.
	16	GSMA LAUNCHES EMBEDDED SIM INITIATIVE TO SUPPORT THE CONNECTED FUTURE, November 18, 2010, p. 1-4.
	17	Chang-Seop Park, On Certificate-Based Security Protocols for Wireless Mobile Communication Systems, Dankook University, IEEE Network September/October 1997, pp. 50-55.
	18	M. Prasad, et al., Secure Authentication Key Agreement Protocol for Long Term Evolution - Advanced, Research Scholar, Associate Professor, Department of Computer Science & Engineering, Pondicherry Engineering College, Puducherry, India, Elsevier, 2012, pp. 158-162.
	19	Eun-Jun Yoon, et al., Secure Deniable Authentication Protocol Based on ElGamal Cryptography, 2008 International Conference on Information Security and Assurance, pp. 36-39.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	20	PIETRE-CAMBACEDES et al., Cryptographic key management for SCADA systems - issues and perspectives, 2008 International Conference on Information Security and Assurance, IEEE, pp. 156-161.
	21	BENDER et al., Evolution of SIM provisioning towards a flexible MCIM provisioning in M2M vertical industries, 16th International Conference on Intelligence in Next Generation Networks, IEEE, 2012, pp. 57-64.
	22	PARK et al., Secure Profile Provisioning Architecture for Embedded UICC, 2013 International Conference on Availability, Reliability and Security, IEEE, 2013, pp. 297-303.
	23	Appenzeller et al., Identity-Based Encryption Architecture and Supporting Data Structures RFC 5408, 2009, pp. 1-30.
	24	Baugher et al., Group Key Management Architecture, RFC Draft, 2001, pp. 1-20.
	25	Ben Saied, Yosra; Olivereau, Alexis; Laurent, Maryline; "A Distributed Approach for Secure M2M Communications", 6th International Conference on New Technologies, Mobility and Security (NTMS), 7-10 May 2012, pgs. 1-7.
	26	Boyen et al., Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles), 2006.
	27	Boyen et al., Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BBI Cryptosystems, RFC 5091, 2007, pp. 1-63.
	28	Harney et al., Group Key Management Protocol (GKMP) Architecture, 1994, pp. 1-19.
	29	Kiltz et al., CCA2 Secure IBE: Standard Model Efficiency through Authenticated Symmetric Encryption, 2008.
	30	Krylov, What is Kerberos Authtentication?, 2003, pp. 1-4.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	31	Martin, Introduction to Identity-Based Encryption, ISBN-13 978-1-59693-238-8, 2008.
	32	Merrian-Webster, Network, 2014.
	33	Park et al., A New Practical Identity-Based Encryption System, 2003, pp_ 1-27.
	34	Park et al., Secure Profile Provisioning Architecture for Embedded UICC, 2013 IEEE, pp_ 297-303.
	35	Shih, Jie-Ren; Hu, Yongbo; Hsiao, Ming-Chun; Chen, Ming-Shing; Shen, Wen-Chng; Yang, Bo-Yin; Wu, An-Yeu; Cheng, Chen-Mou; "Securing M2M with Post-Quantum Public-Key Cryptography", IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 7 March 2013, pgs_ 106-116.
	36	Voltage Security, The Identity-Based Encryption Advantage, 2015.
	37	Yang et al., Identity-Based Key Agreement and Encryption for Wireless Sensor Networks, IJCSNS International Journal of Computer Science and Network Security, Vol. 6, No. 5B, May 2006, pp_ 182-189.
	38	Youngblood, An Introduction to Identity-based Cryptography, 2005.

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

EXAMINER SIGNATURE

Examiner Signature	/David J Pearson/	Date Considered	04/11/2022

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

U.S.PATENTS Remove

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20130149996	A1	2013-06-13	King et al.	
	2	20130166915	A1	2013-06-27	Desai et al.	
	3	20130173747	A1	2013-07-04	Kim et al.	
	4	20130212637	A1	2013-08-15	Guccione et al.	
	5	20130227646	A1	2013-08-29	Haggerty et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	6	20130305345	A1	2013-11-14	Bugenhagen	
	7	20130322621	A1	2013-12-05	Yoon et al.	
	8	20130331063	A1	2013-12-12	Cormier et al.	
	9	20140003604	A1	2014-01-02	Campagna et al.	
	10	20140053241	A1	2014-02-20	Norman et al.	
	11	20140073375	A1	2014-03-13	Li et al.	
	12	20140082538	A1	2014-03-20	Nakhjiri et al.	
	13	20140082539	A1	2014-03-20	Nakhjiri et al.	
	14	20140087790	A1	2014-03-27	Babbage et al.	
	15	20140101444	A1	2014-04-10	Lee et al.	
	16	20140108801	A1	2014-04-17	McBride et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	17	20140140507	A1	2014-05-22	Park et al.	
	18	20140143826	A1	2014-05-22	Sharp et al.	
	19	20140161113	A1	2014-06-12	Cui et al.	
	20	20140165155	A1	2014-06-12	Zhang	
	21	20140192976	A1	2014-07-10	Yoon et al.	
	22	20140219447	A1	2014-08-07	Park et al.	
	23	20140219448	A1	2014-08-07	Froels et al.	
	24	20140244994	A1	2014-08-28	Yu	
	25	20140273913	A1	2014-09-18	Michel et al.	
	26	20140287725	A1	2014-09-25	Lee	
	27	20140337937	A1	2014-11-13	Truskovsky et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	28	20140351403	A1	2014-11-27	Lin et al.	
	29	20150012743	A1	2015-01-08	Holtmanns et al.	
	30	20150017910	A1	2015-01-15	Li et al.	
	31	20150071139	A1	2015-03-12	Nix	
	32	20150092590	A1	2015-04-02	Zhu et al.	
	33	20150095514	A1	2015-04-02	Yu	
	34	20150095648	A1	2015-04-02	Nix	
	35	20150113275	A1	2015-04-23	Kim et al.	
	36	20150121495	A1	2015-04-30	Gao et al.	
	37	20130231087	A1	2013-09-05	O'Leary	
	38	20130165073	A1	2013-06-27	Madsen	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	39	20130007442	A1	2013-01-03	Yinian Mao et al.	
	40	20120170451	A1	2012-07-05	Harish Viswanathan et al.	
	41	20120084568	A1	2012-04-05	Bellcet Sarikaya et al.	
	42	20120030461	A1	2012-02-02	William Daniel Willey et al.	
	43	20080307218	A1	2008-12-11	Oleg Logvinov	
	44	20110035584	A1	2011-02-10	Meyerstein et al.	
	45	20090060197	A1	2009-03-05	Taylor et al.	
	46	20150089214	A1	2015-03-26	Dupre	
	47	20140122878	A1	2014-05-01	Cho et al.	
	48	20140115335	A1	2014-04-24	Jorden et al.	
	49	20130173926	A1	2013-07-04	Morese et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	17647812
	Filing Date	2022-01-12
	First Named Inventor	John A. Nix
	Art Unit	2438
	Examiner Name	David J. PEARSON
	Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

	50	20130012168	A1	2013-01-10	Rajadurai et al.	
	51	20120331298	A1	2012-12-27	Xu et al.	
	52	20120190354	A1	2012-07-26	Merrien et al.	
	53	20040221163	A1	2004-11-04	Jorgensen et al.	
	54	20090113203	A1	2009-04-30	Tsuge et al.	
	55	20150163056	A1	2015-06-11	Nix	
	56	20090217348	A1	2009-08-27	Salmela et al.	
	57	20080130879	A1	2008-06-05	Heinonen et al.	
	58	20130122864	A1	2013-05-16	Haggerty et al.	
	59	20150071139	A1	2015-03-12	Nix	
	60	20150095648	A1	2015-04-02	Nix	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

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

EXAMINER SIGNATURE

Examiner Signature	/David J Pearson/	Date Considered	04/11/2022

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
17/647,812	01/12/2022	John A. Nix	63121/0213

CONFIRMATION NO. 6784

1912
AMSTER, ROTHSTEIN & EBENSTEIN LLP
90 PARK AVENUE
NEW YORK, NY 10016

PUBLICATION NOTICE

OC000000133640290

Title: Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)

Publication No.US-2022-0141010-A1
Publication Date:05/05/2022

NOTICE OF PUBLICATION OF APPLICATION

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

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

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

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

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

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

Petitioner Samsung Ex-1038, 0495

Doc Code: DIST.E.FILE **Document Description: Electronic Terminal Disclaimer - Filed**	PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT**
Application Number	17647812
Filing Date	12-Jan-2022
First Named Inventor	John Nix
Attorney Docket Number	63121/0213
Title of Invention	Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
Network-1 Technologies, Inc.	100%

The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

11258595

10530575

10057059

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:
- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

(●) Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.

( ) I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.

Applicant claims the following fee status:

(●) Small Entity

( ) Micro Entity

( ) Regular Undiscounted

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

(●) An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

Registration Number 51431

( ) A sole inventor

( ) A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application

( ) A joint inventor; all of whom are signing this request

Signature	/Keith J. Barkaus/
Name	Keith J. Barkaus

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal

Application Number:	17647812
Filing Date:	12-Jan-2022
Title of Invention:	Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)
First Named Inventor/Applicant Name:	John A. Nix
Filer:	Keith J. Barkaus/Victoria Gilmore
Attorney Docket Number:	63121/0213

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
STATUTORY OR TERMINAL DISCLAIMER	2814	1	170	170
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**170**

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 17647812

Filing Date: 12-Jan-2022

Applicant/Patent under Reexamination: Nix

Electronic Terminal Disclaimer filed on October 13, 2022

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt

EFS ID:	46805219
Application Number:	17647812
International Application Number:	
Confirmation Number:	6784
Title of Invention:	Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)
First Named Inventor/Applicant Name:	John A. Nix
Customer Number:	1912
Filer:	Keith J. Barkaus/Victoria Gilmore
Filer Authorized By:	Keith J. Barkaus
Attorney Docket Number:	63121/0213
Receipt Date:	13-OCT-2022
Filing Date:	12-JAN-2022
Time Stamp:	15:48:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$170
RAM confirmation Number	E20220CF48563673
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Terminal Disclaimer-Filed (Electronic)	eTerminal-Disclaimer.pdf	41648 d7c5fa995bdf0ae2fb3547670fab0be57715d78e	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	38733 b3cb03397c59071da598e237d53f2abc49a172ba	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	80381		

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Network-1 Technologies, Inc.	Confirmation No.: 6784
Title:	Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)	
Appl. No.:	17/647,812	
Filing Date:	January 12, 2022	
Examiner:	PEARSON, David J.	
Art Unit:	2438	
Docket No.:	63121/0213	
Customer No.:	01912	

RESPONSE TO NON-FINAL OFFICE ACTION DATED APRIL 14, 2022

VIA EFS

Mail Stop AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is a response to the Office Action dated April 14, 2022. A response to the Office Action was due July 14, 2022. Applicant submits herewith a petition for a three-month extension of time such that the present response is being timely filed.

Remarks begin on page 2.

Petitioner Samsung Ex-1038, 0503

REMARKS

This is a response to the Office Action dated April 14, 2022. Claims 1-20 are pending with claim 1 being in independent form. No amendments have been made in the present response.

Claims 1-2, 4-7, 9, 11, 14 and 20 have been rejected based on nonstatutory double patenting as allegedly being unpatentable over claims 1-18 of U.S. Patent No. 11,258,595. Claims 3, 8, 10, 12-13 and 15-19 have been rejected based on nonstatutoru double patenting over claims 1-18 of U.S. Patent No. 11,258,595 in view of Office Notice. Applicant respectfully requests reconsideration of this rejection.

While Applicant does not necessarily agree with this rejection, in an effort to advance prosecution of the present application, Applicant submits herewith a terminal disclaimer to overcome this rejection.

Claims 1-2 and 6-7 have been rejected based on nonstatutory double patenting as allegedly being unpatentable over claims 1-9 of U.S. Patent No. 10,530,575. Claims 3-5 and 8-20 have been rejected based on nonstatutory double patenting in view of claims 1-9 of U.S Patent No. 10,530,575 in view of Office Notice. Applicant respectfully requests reconsideration of this rejection.

While Applicant does not necessarily agree with this rejection, in an effort to advance prosecution of the present application, Applicant submits herewith a terminal disclaimer to overcome this rejection.

Claims 1-2 and 6-7 have been rejected based on nonstatutory double patenting as allegedly being unpatentable over claims 1-9 of U.S. Patent No. 10,057,059. Claims 3-5 and 8-20 have been rejected based on nonstatutory double patenting in view of claims 1-9 of U.S Patent No. 10,057,059 in view of Office Notice. Applicant respectfully requests reconsideration of this rejection.

While Applicant does not necessarily agree with this rejection, in an effort to advance prosecution of the present application, Applicant submits herewith a terminal disclaimer to overcome this rejection.

Accordingly, Applicant respectfully requests reconsideration and withdrawal of the

Petitioner Samsung Ex-1038, 0504

rejection of the claims based on nonstatutory double patenting.

Since there are no other objections or rejections of the claims, Applicant respectfully submits tat claims 1-20 are patentable over the cited art and are in condition for allowance.

In the event that the Examiner disagrees, Applicant respectfully requests that the Examiner contact Applicant's undersigned attorney to disucss any remaing issues prior ot issuing another Office Action.

Reference to Related Patents and Co-pending Applications

The below chart provides information regarding related issued patents and co-pending applications filed by the present Applicant:

Petitioner Samsung Ex-1038, 0505

Serial No.	Attorney Docket No.	Filing Date	Status
17/647,812	**63121/0213**	**2022-01-12**	**Present Application**
17/547,990	63121/0212	2021-12-10	Pending - Ready for Examination
17/304,922	63121/0209	2021-06-28	Pending - Ready for Examination
17/249,242	63121/0202	2021-02-24	Non-Final Action issued on August 11, 2022
16/879,325	63121/0198	2020-05-20	USP 11,082,218
16/843,107	63121/0197	2020-04-08	USP 11,283,603
16/721,153	63121/0195	2019-12-19	Notice of Allowance issued on August 22, 2022
16/593,561	63121/0190	2019-10-04	USP 11,258,595
16/453,682	63121/0184	2019-06-26	USP 11,233,780
16/271,455	63121/0181	2019-02-08	USP 10,594,679
16/271,428	63121/0180	2019-02-08	USP 10,523,432
16/201,401	63121/0179	2018-11-27	USP 10,700,856
16/200,118	63121/0178	2018-11-26	USP 10,498,530
16/110,804	63121/0168	2018-08-23	USP 10,382,422
16/036,506	63121/0167	2018-07-16	USP 10,530,575
15/983,957	63121/0163	2018-05-18	USP 10,177,911
15/973,012	63121/0162	2018-05-07	USP 10,250,386
15/972,914	63121/0161	2018-05-07	USP 10,652,017
15/928,848	63121/0160	2018-03-22	USP 10,084,768
15/010,905	63121/0157	2016-01-29	USP 9,641,327
15/680,758	63121/0147	2017-08-18	USP 10,187,206
15/162,292	63121/0146	2016-05-23	USP 10,362,012
14/751,119	63121/0145	2015-06-25	USP 9,961,060
15/457,700	63121/0144	2017-03-13	USP 9,998,281
15/583,968	63121/0143	2017-05-01	USP 10,057,059
15/043,293	63121/0142	2016-02-12	USP 9,998,280
15/642,088	63121/0141	2017-07-05	USP 10,003,461
15/130,146	63121/0140	2016-04-15	USP 9,742,562
15/162,302	63121/0139	2016-05-23	USP 9,698,981
14/789,255	63121/0138	2015-07-01	USP 9,596,078
14/139,419	63121/0137	2013-12-23	USP 9,351,162
14/136,711	63121/0136	2013-12-20	USP 9,300,473
14/099,329	63121/0135	2013-12-06	USP 9,100,175
14/084,141	63121/0134	2013-11-19	USP 9,319,223
14/064,618	63121/0133	2013-10-28	USP 9,118,464
14/055,606	63121/0132	2013-10-16	USP 9,276,740

Petitioner Samsung Ex-1038, 0506

14/039,401	63121/0131	2013-09-27	USP 9,288,059
14/023,181	63121/0130	2013-09-10	USP 9,350,550
AU 2019246774	63121-0199	2019-10-08	Published on 2021-09-23
GB 1608573	63121-0151	2014-10-27	Published on 2016-08-03
GB 2100530	63121-0201	2014-10-27	Published on 2021-05-12
CA 2,965,119	63121-0152	2014-10-27	Published on 2015-05-07
HK 17101082.8	63121-0153	2014-10-27	Published on 2017-10-20
EU 14868381.6	63121-0154	2014-12-04	Published on 2017-01-04
CA 2,969,829	63121-0155	2014-12-04	Published on 2015-06-11
HK 17106540.3	63121-0156	2014-12-04	Published on 2018-01-19

The Examiner is invited to review the prosecution history of each of these applications, including the cited references of record and related office actions, as the Examiner deems appropriate.

CONCLUSION

In view of the foregoing, Applicant respectfully submits that all pending claims are patentable over the cited art and in condition for allowance. Reconsideration and prompt allowance of this application are both respectfully solicited.

Applicant respectfully asserts that the foregoing constitutes a bona fide response to all outstanding objections and rejections within this Office Action.

This application is in condition for immediate allowance. However, should any issue(s) of a minor nature remain, the Examiner is respectfully requested to telephone the undersigned at telephone number (212) 336-8000 so that the issue(s) might be promptly resolved.

Favorable reconsideration of the present application is respectfully requested.

* * * * * *

Petitioner Samsung Ex-1038, 0507

Any claim amendment(s), claim(s) added, claim(s) canceled, argument(s), remark(s), and/or any combination(s) thereof made in this response pertain solely to the specific aspects of this specific claimed invention. Further, any claim amendment(s), claim(s) added, claim(s) canceled, argument(s), remark(s), and/or any combination(s) thereof are made without prejudice to or disclaimer of Applicant's right to seek patent protection of any unclaimed subject matter such as, but not limited, to narrower unclaimed subject matter, broader unclaimed subject matter, different unclaimed subject matter, variations of unclaimed subject matter, any combination thereof, and/or any other unclaimed subject matter that may or may not be filed, for example, in any design and/or utility patent application(s) such as, but not limited to, continuation patent application(s), continuation-in-part patent application(s), and/or divisional patent application(s) and/or any other patent application(s).

Applicant's silence as to any assertion(s) by the Examiner in the Office Action and/or to any certain fact(s) or conclusion(s) that may be implied and/or alleged by objections(s) and/or rejection(s) in the Office Action is not in any way a concession by Applicant that such assertion(s), implication(s), and/or allegation(s) are accurate, and that all requirements for any objection(s) and/or a rejection(s) have been met. Accordingly, Applicant reserves the right to analyze and dispute any such assertion(s), implication(s), and/or allegation(s) in the future.

Respectfully submitted,

AMSTER, ROTHSTEIN & EBENSTEIN LLP
Attorneys for Applicant
90 Park Avenue
New York, NY 10016
(212) 336-8000

Dated: October 13, 2022
New York, New York

By: / Keith J. Barkaus/
Keith J. Barkaus
Registration No. 51,431

Petitioner Samsung Ex-1038, 0508

PTO/AIA/22 (10-20)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): 63121/0213

Application Number: 17/647,812

Filed: January 12, 2022

For: Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)

Art Unit: 2438

Examiner: PEARSON, David J.

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$220	$110	$55	$
☐ Two months (37 CFR 1.17(a)(2))	$640	$320	$160	$
☑ Three months (37 CFR 1.17(a)(3))	$1,480	$740	$370	$ 740
☐ Four months (37 CFR 1.17(a)(4))	$2,320	$1,160	$580	$
☐ Five months (37 CFR 1.17(a)(5))	$3,160	$1,580	$790	$

☑ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

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

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 011785.

☑ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 51,431.

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____.

/Keith J. Barkaus/ — Signature

October 13, 2022 — Date

Keith J. Barkaus — Typed or printed name

212-336-8000 — Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☑ * Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.136(a). 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 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	17647812
Filing Date:	12-Jan-2022
Title of Invention:	Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)
First Named Inventor/Applicant Name:	John A. Nix
Filer:	Keith J. Barkaus/Victoria Gilmore
Attorney Docket Number:	63121/0213

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	2253	1	740	740
Miscellaneous:				
			Total in USD ($)	**740**

Electronic Acknowledgement Receipt

EFS ID:	46814113
Application Number:	17647812
International Application Number:	
Confirmation Number:	6784
Title of Invention:	Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)
First Named Inventor/Applicant Name:	John A. Nix
Customer Number:	1912
Filer:	Keith J. Barkaus/Victoria Gilmore
Filer Authorized By:	Keith J. Barkaus
Attorney Docket Number:	63121/0213
Receipt Date:	13-OCT-2022
Filing Date:	12-JAN-2022
Time Stamp:	15:50:26
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$740
RAM confirmation Number	E20220CF50393707
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		1-ResponsetoNFOA.pdf	109866 38f69d04722c5603348b30546e2e3a088944f714	yes	6
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Amendment/Request for Reconsideration-After Non-Final Rejection		1	1	
	Applicant Arguments/Remarks Made in an Amendment		2	6	
Warnings:					
Information:					
2	Extension of Time	2-ExtensionofTime.pdf	165952 0fad067b09aa57f8a5ce877947b0c8811d1015b7	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	38630 9a659e51c04712066cefc666a2fc69a4ef37a1e0	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	314448		

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.

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

1912 7590 10/31/2022

AMSTER, ROTHSTEIN & EBENSTEIN LLP
90 PARK AVENUE
NEW YORK, NY 10016

EXAMINER
PEARSON, DAVID J

ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 10/31/2022

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/647,812	01/12/2022	John A. Nix	63121/0213	6784

TITLE OF INVENTION: Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	01/31/2023

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. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

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

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

PTOL-85 (Rev. 02/11)

Petitioner Samsung Ex-1038, 0516

PART B - FEE(S) TRANSMITTAL

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

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

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

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

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

1912 7590 10/31/2022

AMSTER, ROTHSTEIN & EBENSTEIN LLP
90 PARK AVENUE
NEW YORK, NY 10016

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

Certificate of Mailing or Transmission

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

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/647,812	01/12/2022	John A. Nix	63121/0213	6784

TITLE OF INVENTION: Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	01/31/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS
PEARSON, DAVID J	2438	713-156000

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/AIA/122 or PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or 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 must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

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

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

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

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

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

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

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

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

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

Petitioner Samsung Ex-1038, 0517

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.
17/647,812	01/12/2022	John A. Nix	63121/0213	6784

1912 7590 10/31/2022

AMSTER, ROTHSTEIN & EBENSTEIN LLP
90 PARK AVENUE
NEW YORK, NY 10016

EXAMINER	
PEARSON, DAVID J	
ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 10/31/2022

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.

Petitioner Samsung Ex-1038, 0518

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

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

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

Privacy Act Statement

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

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

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

Notice of Allowability	Application No. 17/647,812	Applicant(s) Nix, John A.	
	Examiner DAVID J PEARSON	Art Unit 2438	AIA (FITF) Status Yes

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

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

1. ☑ This communication is responsive to 10/13/2022.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

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

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

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

   Certified copies:

   a) ☐ All b) ☐ Some* c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

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

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

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

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

Attachment(s)

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

/David J Pearson/
Primary Examiner, Art Unit 2438

Petitioner Samsung Ex-1038, 0520

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.

1. Claims 1-20 have been examined.

Terminal Disclaimer

2. The terminal disclaimer filed on 10/13/2022 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of **U.S. Patents 11258595, 10530575 and 10057059** has been reviewed and is accepted. The terminal disclaimer has been recorded.

Allowable Subject Matter

3. Claims 1-20 are allowed.

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

For independent claim 1, the prior art of record, alone or in combination, fails to teach the following limitations in conjunction with the rest of the claimed limitations:

(1) storing a server public key, a module identity, cryptographic algorithms, and a pre-shared secret key, wherein the module identity comprises a permanent identifier for the mobile device and the cryptographic algorithms includes a symmetric ciphering algorithm;...
(5) sending a message to a server for the wireless network, the message comprising the module encrypted data and the module public key, wherein the server mutually derives the symmetric ciphering key using at least the module public key, and wherein the wireless network selects the pre-shared secret key for the mobile device using the module identity; and (6) authenticating with the wireless network using a message digest with the pre-shared secret key

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

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAVID J PEARSON whose telephone number is (571)272-0711. The examiner can normally be reached 6:00 - 5:30 pm; Monday through Thursday.

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

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197

(toll-free). If you would like assistance from a USPTO Customer Service

Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/David J Pearson/
Primary Examiner, Art Unit 2438

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/647,812	Nix, John A.
	Examiner	Art Unit
	DAVID J PEARSON	2438

CPC - Searched*		
Symbol	**Date**	**Examiner**
H04W12/40, 069	04/11/2022	DP
G06F21/445	04/11/2022	DP
H04L9/0841, 0816, 32	04/11/2022	DP
H04L63/0272, 045, 061	04/11/2022	DP
G06F2221/2115	04/11/2022	DP

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**

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

Search Notes		
Search Notes	**Date**	**Examiner**
Inventor name search	04/11/2022	DP
CPC class and keyword search	04/11/2022	DP
See attached NPL searches - IP.com; Google Scholar; Dialog	04/11/2022	DP
See attached SEARCH report	04/12/2022	DP
Updated inventor name search	10/24/2022	DP
Updated CPC class and keyword search	10/24/2022	DP
See attached SEARCH report	10/24/2022	DP

Petitioner Samsung Ex-1038, 0524

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/647,812	Nix, John A.
	Examiner	Art Unit
	DAVID J PEARSON	2438

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
	See attached .CLM. search	10/24/2022	DP

Petitioner Samsung Ex-1038, 0525

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/647,812	Nix, John A.
	Examiner	**Art Unit**
	DAVID J PEARSON	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☑ Claims renumbered in the same order as presented by applicant ☐ CPA ☑ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/12/2022	10/24/2022							
	1	✓	=							
	2	✓	=							
	3	✓	=							
	4	✓	=							
	5	✓	=							
	6	✓	=							
	7	✓	=							
	8	✓	=							
	9	✓	=							
	10	✓	=							
	11	✓	=							
	12	✓	=							
	13	✓	=							
	14	✓	=							
	15	✓	=							
	16	✓	=							
	17	✓	=							
	18	✓	=							
	19	✓	=							
	20	✓	=							

Petitioner Samsung Ex-1038, 0526

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/647,812	Nix, John A.
	Examiner	**Art Unit**
	DAVID J PEARSON	2438

CPC						
Symbol					**Type**	**Version**
H04L	/	9	/	0861	F	2013-01-01
H04W	/	52	/	0235	I	2013-01-01
H04W	/	12	/	04	I	2013-01-01
H04W	/	4	/	70	I	2018-02-01
H04W	/	76	/	27	I	2018-02-01
H04L	/	9	/	0841	I	2013-01-01
H04W	/	52	/	0216	I	2013-01-01
H04L	/	63	/	0442	I	2013-01-01
H04L	/	63	/	123	I	2013-01-01
G06F	/	21	/	35	I	2013-01-01
H04W	/	12	/	033	I	2021-01-01
G06F	/	21	/	445	I	2013-01-01
H04W	/	12	/	40	I	2021-01-01
H04W	/	12	/	069	I	2021-01-01
H04L	/	9	/	3247	I	2013-01-01
H04W	/	12	/	06	I	2013-01-01
H04W	/	12	/	02	I	2013-01-01
H04L	/	63	/	061	I	2013-01-01
H04L	/	9	/	0894	I	2013-01-01
H04L	/	9	/	14	I	2013-01-01
H04L	/	9	/	3066	I	2013-01-01
H04L	/	9	/	088	I	2013-01-01
H04J	/	11	/	00	I	2013-01-01
H04L	/	12	/	2854	I	2013-01-01
H04W	/	8	/	082	I	2013-01-01
H04W	/	40	/	005	I	2013-01-01
H04W	/	52	/	0277	I	2013-01-01
H04W	/	80	/	04	I	2013-01-01
H04L	/	9	/	006	I	2013-01-01
H04L	/	63	/	0435	I	2013-01-01
H04L	/	63	/	0807	I	2013-01-01

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	20	
/David J Pearson/ Primary Examiner, Art Unit 2438	24 October 2022	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	5b

U.S. Patent and Trademark Office — Part of Paper No.: 20221024A

Petitioner Samsung Ex-1038, 0527

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/647,812	Nix, John A.
	Examiner	**Art Unit**
	DAVID J PEARSON	2438

CPC								
Symbol							**Type**	**Version**
H04L	/	9	/	0816			I	2013-01-01
H04L	/	9	/	085			I	2013-01-01
H04L	/	9	/	30			I	2013-01-01
H04L	/	9	/	32			I	2013-01-01
H04L	/	9	/	321			I	2013-01-01
H04L	/	63	/	0272			I	2013-01-01
H04L	/	63	/	045			I	2013-01-01
H04L	/	67	/	04			I	2013-01-01
H04L	/	9	/	3239			I	2013-01-01
H04L	/	9	/	3249			I	2013-01-01
H04L	/	9	/	3263			I	2013-01-01
H04L	/	63	/	166			I	2013-01-01
H05K	/	999	/	99			I	2013-01-01
G06F	/	2221	/	2105			A	2013-01-01
G06F	/	2221	/	2107			A	2013-01-01
G06F	/	2221	/	2115			A	2013-01-01
H04L	/	2209	/	805			A	2013-01-01
H04L	/	63	/	0464			A	2013-01-01
Y02D	/	30	/	70			A	2020-08-01
H04L	/	2209	/	24			A	2013-01-01
H04L	/	2209	/	72			A	2013-01-01
H04W	/	84	/	12			A	2013-01-01
H04W	/	88	/	12			A	2013-01-01

CPC Combination Sets								
Symbol							**Type**	**Set**	**Ranking**	**Version**
	/		/							

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	20	
/David J Pearson/ Primary Examiner, Art Unit 2438	24 October 2022	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	5b

U.S. Patent and Trademark Office — Part of Paper No.: 20221024A

Petitioner Samsung Ex-1038, 0528

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/647,812	Nix, John A.
	Examiner	**Art Unit**
	DAVID J PEARSON	2438

INTERNATIONAL CLASSIFICATION					
CLAIMED					
H04L	/	9	/	08	

NON-CLAIMED					
	/		/		

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

NONE (Assistant Examiner) (Date)	**Total Claims Allowed:** 20	
/David J Pearson/ Primary Examiner, Art Unit 2438 (Primary Examiner) 24 October 2022 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 5b

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	17/647,812	Nix, John A.
	Examiner	**Art Unit**
	DAVID J PEARSON	2438

☑ Claims renumbered in the same order as presented by applicant ☐ CPA ☑ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		10		19										
	2		11		20										
	3		12												
	4		13												
	5		14												
	6		15												
	7		16												
	8		17												
	9		18												

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 20	
/David J Pearson/ Primary Examiner, Art Unit 2438 (Primary Examiner)	24 October 2022 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 5b

U.S. Patent and Trademark Office

Part of Paper No.: 20221024A

Petitioner Samsung Ex-1038, 0530

PE2E SEARCH - Search History (Prior Art)

There are no Prior Art searches to show.

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N154	5	((common shared mutual symmetric) near (secret key) with (token credential certificate) with (encrypt$3 decrypt$3) with ((temp temporary ephemeral) near3 (public adj key))).clm.	(USPAT)	OR	ON	ON	2022/10/24 12:02 PM
N155	0	((diffie DH diffie-hellman) with (token credential certificate) with (encrypt$3 decrypt$3) with ((temp temporary ephemeral) near3 (public adj key))).clm.	(USPAT)	OR	ON	ON	2022/10/24 12:02 PM
N156	9	((second other 2nd next new) near3 (common shared mutual symmetric) near (secret key) with (token credential certificate) with (encrypt$3 decrypt$3) with (public adj key) with (private adj key)).clm.	(USPAT)	OR	ON	ON	2022/10/24 12:02 PM

Petitioner Samsung Ex-1038, 0531

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L283	153	(nix-john$).in.	(US-PGPUB; USPAT)	OR	OFF	OFF	2022/10/24 10:07 AM
L284	24853	(H04W12/40 OR G06F21/445 OR H04L9/0841 OR H04L9/0816 OR H04L9/32 OR H04L63/0272 OR H04L63/045 OR G06F2221/2115).cpc.	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L285	475	L151 AND (PSK (preshared pre-shared) near2 (secret key)) AND (ECDH DH diffie)	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L286	428	L151 AND (PSK (preshared pre-shared) near2 (secret key)) same3 (challenge authenticat$3 hash$3 signature digest) AND (ECDH DH diffie)	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L287	373	L151 AND (PSK (preshared pre-shared) near2 (secret key)) SAME (challenge authenticat$3 hash$3 signature digest) AND (ECDH DH diffie)	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L288	316	L151 AND (PSK (preshared pre-shared) near2 (secret key)) AND (challenge authenticat$3) SAME (hash$3 signature digest) AND (ECDH DH diffie)	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L289	106	(L154 L155) AND @ad<"20131016"	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L290	386	L151 AND (challenge authenticat$3) SAME (hash$3 signature digest) SAME (secret key) same4 (ECDH elliptic$2 near2(DH diffie diffie-hellman))	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L291	23	L2 and ((ID identity identif$4) with ((private public) adj key) with (server) with (authenticat$3)).clm.	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM

Petitioner Samsung Ex-1038, 0532

L292	67	("20050058294" OR "20060129848" OR "20080044032" OR "20080107083" OR "20110035604" OR "20110213959" OR "20110268022" OR "20110269422" OR "20110269461" OR "20110269472" OR "20110270747" OR "20120011362" OR "20120087493" OR "20120190354" OR "20120263298" OR "20130012168" OR "20130122864" OR "20130157673" OR "20130165075" OR "20130227646" OR "20130283047" OR "20130294602" OR "20130340040" OR "20130344864" OR "20140003604" OR "20140082358" OR "20140082359" OR "20140120874" OR "20140140507" OR "20140219447" OR "20140235210" OR "20140237101" OR "20140287725" OR "20140308991" OR "20140329502" OR "20140357229" OR "20150121495" OR "20150281964" OR "20150350881" OR "20160057725" OR "20160088096" OR "20160127132" OR "20160149903" OR "5216715" OR "5642420" OR "5664017" OR "5852665" OR "5995625" OR "6256733" OR "6721886" OR "6804357" OR "6842628" OR "7957532" OR "8352739" OR "8452017" OR "8577337" OR "8965366" OR "9020479" OR	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM

Petitioner Samsung Ex-1038, 0533

		"9270653" OR "9332129" OR "9572016" OR "9628981" OR "9674690" OR "9794775" OR "9800993" OR "9807605" OR "9923724").pn.					
L293	7	L167 AND (PSK (preshared pre-shared shared) near2 (secret key)) SAME (challenge authenticat$3 hash$3 signature digest identi$7) AND (ECDH DH diffie)	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L294	0	L167 AND (PSK (preshared pre-shared shared) near2 (secret key)) WITH (challenge authenticat$3 hash$3 signature digest) SAME (identi$7) AND (server) near3 (public private) ADJ (key) SAME (client user device) near3 (public private) ADJ (key) SAME (generat$3 deriv$5 diffie DH ECDH elliptic$2) WITH (key)	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L295	6	L167 AND (PSK (preshared pre-shared shared) near2 (secret key)) WITH (challenge authenticat$3 hash$3 signature digest) SAME (identi$7)	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L296	1	L167 AND (server) near3 (public private) ADJ (key) SAME (client user device) near3 (public private) ADJ (key) SAME (generat$3 deriv$5 diffie DH ECDH elliptic$2) WITH (key)	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L297	53128	(H04W12/40 OR G06F21/445 OR H04L9/0841 OR H04L9/0816 OR H04L9/32 OR H04L63/0272 OR H04L63/045 OR H04L63/0442 OR H04L63/123 OR H04W52/0216 OR	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM

		H04L63/061 OR G06F2221/2115).cpc.					
L298	1175	L172 AND (PSK (preshared pre-shared shared) near2 (secret key)) SAME (challenge authenticat$3 hash$3 signature digest) SAME (ID identi$7) AND (ECDH DH diffie)	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L299	44	L172 AND (PSK (preshared pre-shared shared) near2 (secret key)) SAME (challenge hash$3 signature digest) SAME (ID identi$7) near4 (client EUICC user SIM UICC device) SAME (server) WITH (authenticat$3 verif$7 validat$3 compar$3 confirm$5) same4 (ECDH DH diffie)	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L300	86	L172 AND (PSK (preshared pre-shared shared) near2 (secret key)) SAME (challenge hash$3 signature digest) SAME (ID identi$7) near4 (client EUICC user SIM UICC device) SAME (server) WITH (authenticat$3 verif$7 validat$3 compar$3 confirm$5) AND (ECDH DH diffie)	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L301	108	L172 AND (PSK (preshared pre-shared shared) near2 (secret key)) SAME (challenge hash$3 signature digest) SAME (ID identi$7) SAME (server) SAME (authenticat$3 verif$7 validat$3 compar$3 confirm$5) same4 (ECDH DH diffie)	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L302	88	L172 AND (PSK (preshared pre-shared shared) near2 (secret key)) WITH (challenge authenticat$3 hash$3 signature digest) SAME (identi$7) AND (server)	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM

Petitioner Samsung Ex-1038, 0535

		near3 (public private) ADJ (key) SAME (client user device) near3 (public private) ADJ (key) SAME (generat$3 deriv$5 diffie DH ECDH elliptic$2) WITH (key)					
L303	27	L172 AND (ECDH diffie near4 elliptic$2) SAME (decrypt$3) WITH (respon$4 challenge reply digest hash) WITH (server client SIM EUICC UICC token)	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L304	109	L172 AND (ECDH diffie near4 elliptic$2) same3 (decrypt$3) WITH (respon$4 challenge reply digest hash) WITH (server client SIM EUICC UICC token)	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L305	237	L172 AND (ECDH diffie near4 elliptic$2) same3 (decrypt$3) SAME (respon$4 challenge reply digest hash) SAME (server client SIM EUICC UICC token) SAME (PSK (pre-shared shared stored) near2 (key secret))	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L306	211	L172 AND (ECDH diffie near4 elliptic$2) same3 (decrypt$3) SAME (respon$4 challenge reply digest hash token) SAME (server client SIM EUICC UICC) SAME (PSK (pre-shared shared stored) near2 (key secret))	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L307	53	(L174 L175 L176 L177 L178 L179 L180 L181) AND @ad<"20131016"	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L308	3	("20110158411" "20130145151" "20140068252").pn.	(US-PGPUB; USPAT)	OR	OFF	OFF	2022/10/24 10:07 AM
L309	241	("10169587" OR "10621352" OR "20010029581" OR "20020018569" OR "20030003895" OR "20030211842" OR "20040162472" OR "20040179684" OR	(US-PGPUB; USPAT)	OR	OFF	OFF	2022/10/24 10:07 AM

Petitioner Samsung Ex-1038, 0536

		"20040221163" OR "20050008159" OR "20050021875" OR "20050050323" OR "20050058294" OR "20050120202" OR "20050138353" OR "20050193199" OR "20050246282" OR "20050278787" OR "20060021063" OR "20060056355" OR "20060059344" OR "20060095771" OR "20060129848" OR "20060206710" OR "20060281442" OR "20070101400" OR "20070158439" OR "20070206799" OR "20080016230" OR "20080022089" OR "20080031204" OR "20080044032" OR "20080107083" OR "20080114978" OR "20080130879" OR "20080165698" OR "20080307218" OR "20090028341" OR "20090041110" OR "20090060197" OR "20090077643" OR "20090113203" OR "20090116642" OR "20090125996" OR "20090132806" OR "20090183541" OR "20090191857" OR "20090209232" OR "20090217348" OR "20090268909" OR "20090274306" OR "20090282246" OR "20090313472" OR "20100031042" OR "20100062808" OR "20100093347" OR "20100098253" OR "20100166167" OR "20100195833" OR "20100199334" OR "20100223461" OR "20100275028" OR "20100291907" OR "20110016321" OR "20110035584" OR "20110035604" OR				

Petitioner Samsung Ex-1038, 0537

		"20110055553" OR "20110158411" OR "20110167272" OR "20110213959" OR "20110237281" OR "20110268022" OR "20110269422" OR "20110269461" OR "20110269472" OR "20110270747" OR "20110291803" OR "20110314287" OR "20120011360" OR "20120011362" OR "20120023336" OR "20120030461" OR "20120033613" OR "20120072732" OR "20120084568" OR "20120087493" OR "20120089568" OR "20120108205" OR "20120117635" OR "20120159153" OR "20120170451" OR "20120190354" OR "20120214444" OR "20120260086" OR "20120260090" OR "20120260095" OR "20120263298" OR "20120278490" OR "20120300932" OR "20120331292" OR "20120331298" OR "20130007442" OR "20130012168" OR "20130028184" OR "20130091556" OR "20130114810" OR "20130117824" OR "20130122864" OR "20130149996" OR "20130157673" OR "20130165073" OR "20130165075" OR "20130166915" OR "20130173747" OR "20130173926" OR "20130179962" OR "20130182586" OR "20130183932" OR "20130212637" OR "20130227646" OR "20130231087" OR "20130283047" OR "20130294602" OR "20130305345" OR				

Petitioner Samsung Ex-1038, 0538

		"20130322621" OR "20130331063" OR "20130340040" OR "20130344864" OR "20140003604" OR "20140040628" OR "20140049653" OR "20140053241" OR "20140073375" OR "20140082358" OR "20140082359" OR "20140082538" OR "20140082539" OR "20140087790" OR "20140101444" OR "20140108801" OR "20140115335" OR "20140120874" OR "20140122878" OR "20140140507" OR "20140140509" OR "20140143534" OR "20140143826" OR "20140161113" OR "20140165155" OR "20140192976" OR "20140219447" OR "20140219448" OR "20140235210" OR "20140237101" OR "20140244994" OR "20140273913" OR "20140281483" OR "20140287725" OR "20140308991" OR "20140329502" OR "20140337937" OR "20140351403" OR "20140357229" OR "20150012743" OR "20150017910" OR "20150071139" OR "20150089214" OR "20150092590" OR "20150095514" OR "20150095648" OR "20150106616" OR "20150113275" OR "20150121066" OR "20150121495" OR "20150143125" OR "20150163056" OR "20150215126" OR "20150222604" OR "20150222619" OR "20150281964" OR "20150350881" OR "20160014112" OR					

Petitioner Samsung Ex-1038, 0539

		"20160057725" OR "20160088096" OR "20160127132" OR "20160149903" OR "20160294829" OR "20170206532" OR "20190313246" OR "20190332774" OR "20190356482" OR "20200162247" OR "20200162269" OR "20200226258" OR "20200280436" OR "20210126801" OR "20210184842" OR "20210194681" OR "20210211279" OR "20210218560" OR "5216715" OR "5642420" OR "5664017" OR "5852665" OR "5995625" OR "6038322" OR "6256733" OR "6721886" OR "6804357" OR "6842628" OR "7921292" OR "7957532" OR "8127142" OR "8352739" OR "8434139" OR "8452017" OR "8522013" OR "8526606" OR "8555067" OR "8577337" OR "8590028" OR "8782774" OR "8843179" OR "8924715" OR "8948386" OR "8965366" OR "9002018" OR "9020479" OR "9253643" OR "9270653" OR "9332129" OR "9408012" OR "9572016" OR "9596078" OR "9628981" OR "9674690" OR "9698981" OR "9794775" OR "9800993" OR "9807605" OR					

Petitioner Samsung Ex-1038, 0540

		"9923724").pn.					
L310	30	L263 AND (challenge authenticat$3) SAME (hash$3 signature digest) SAME (secret key) AND (ECDH elliptic$2 near2(DH diffie diffie-hellman))	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L311	93	L263 AND (challenge authenticat$3) SAME (hash$3 signature digest) SAME (secret key) AND (generat$3 determin$5 deriv$5) WITH (key) SAME (public ADJ key) SAME (private ADJ key)	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L312	34	L263 AND (challenge authenticat$3) SAME (hash$3 signature digest) SAME (secret key) AND (generat$3 determin$5 deriv$5) WITH (key) SAME (public ADJ key) SAME (private ADJ key) SAME (server network) SAME (mobile client module)	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L313	46	(L264 L266)	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L314	30	L263 AND (challenge authenticat$3 validat$3 verif$7) WITH (mobile client module SIM) SAME (hash$3 signature digest) WITH (seed secret key) AND (generat$3 determin$5 deriv$5) WITH (key) SAME (public ADJ key) SAME (private ADJ key) SAME (server network) SAME (mobile client module)	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L315	17235	(H04L63/045 OR H04L63/061 OR H04W12/069 OR H04W12/40).cpc.	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L316	626	L269 AND (challenge authenticat$3 validat$3 verif$7) WITH (mobile client module SIM) SAME (hash$3 signature digest) WITH (seed secret key) AND	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM

Petitioner Samsung Ex-1038, 0541

		(generat$3 determin$5 deriv$5) WITH (key) SAME (public ADJ key) SAME (private ADJ key) SAME (server network) SAME (mobile client module)					
L317	254	L269 AND (challenge authenticat$3 validat$3 verif$7) WITH (mobile client module SIM) SAME (hash$3 signature digest) WITH (seed secret key) AND (ECDH elliptic$2 near2(DH diffie diffie-hellman))	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L318	177	(L270 L271) AND @ad<"20131016"	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L319	93	(seed shared near2 (secret key)) SAME (generat$3) WITH ((private public) ADJ key) AND (challenge authenticat$3 validat$3 verif$7) WITH (mobile client module SIM) SAME (hash$3 signature digest) WITH (seed (shared) near2 (secret key)) AND (ECDH elliptic$2 near2(DH diffie diffie-hellman))	(US-PGPUB; USPAT)	OR	ON	ON	2022/10/24 10:07 AM
L320	4	("20140082358" "20140235210" "20150350881" "20100291907").pn.	(US-PGPUB; USPAT)	OR	OFF	OFF	2022/10/24 10:07 AM
L321	159	(seed shared near2 (secret key)) SAME (generat$3) WITH ((private public) ADJ key) AND (challenge authenticat$3 validat$3 verif$7) WITH (mobile client module SIM) SAME (hash$3 signature digest) WITH (seed (shared) near2 (secret key)) AND (ECDH elliptic$2 near2(DH diffie diffie-hellman))	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/10/24 10:07 AM
L322	3	(L275) AND @ad<"20131016"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	ON	2022/10/24 10:07 AM

			IBM_TDB)				
L323	665	(seed shared secret) SAME (generat$3) WITH ((private public) ADJ key) AND (challenge authenticat$3 validat$3 verif$7) WITH (mobile client module SIM) SAME (hash$3 signature digest) WITH (seed shared secret key) AND (ECDH elliptic$2 near2(DH diffie diffie-hellman))	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/10/24 10:07 AM
L324	42	(L277) AND @ad<"20131016"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/10/24 10:07 AM
L325	152	(seed shared secret) SAME (generat$3) WITH ((private public) ADJ key) AND (challenge authenticat$3 validat$3 verif$7) WITH (mobile client module SIM) SAME (hash$3 signature digest) WITH (seed shared secret key) AND (generat$3 creat$3 calculat$3 deriv$5) WITH (shared symmetric) near3 (key) SAME (server) near2 ((private public) ADJ key) SAME (client mobile SIM) near2 ((private public) ADJ key)	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/10/24 10:07 AM
L326	554	(seed shared secret) SAME (generat$3) WITH ((private public) ADJ key) AND (challenge authenticat$3 validat$3 verif$7) WITH (mobile client module SIM) SAME (hash$3 signature digest) WITH (seed shared secret key) AND (generat$3 creat$3 calculat$3 deriv$5) near5 (shared symmetric key) SAME (server) near2 ((private public) ADJ key) SAME	(US-PGPUB; USPAT; USOCR; FIT (CN, FR, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/10/24 10:07 AM

		(client mobile SIM) near2 ((private public) ADJ key)					
L327	117	(L280 L279) AND @ad<"20131016"	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/10/24 10:07 AM
L328	155	(L278 L281)	(US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/10/24 10:07 AM

PE2E SEARCH - Search History (Interference)

There are no Interference searches to show.

Petitioner Samsung Ex-1038, 0544

Application Data Sheet 37 CFR 1.76

The Application Data Sheet is part of the provisional or non-provisional 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.

Inventor Information

of inventors: 1

1. **John A. Nix**

Residence Information
US Residency
Evanston, IL
UNITED STATES

Mailing Address
807 Davis Street, Unit 409
Evanston, IL 60201
UNITED STATES

Application Information

Customer number	**1912 -**
Correspondence address	----
Title of invention	**Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)**
Attorney docket number	**63121/0213**
Entity status	Small
Application type	Nonprovisional Application under 35 USC 111(a)

Petitioner Samsung Ex-1038, 0545

Subject matter	Utility
Total number of drawing sheets	17
Suggested figure for publication	---
Filing by reference	No
Publication request	Normal eighteen-month publication

Representative Information

of representatives: 1

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).

Customer number 1912

Domestic Benefit/National Stage Information

of benefit claims: 5

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c), 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(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior app status	Pending
Application number	---
Continuity type	**Continuation of**
Prior app number	**16593561**
Filing Date	10/04/2019

Prior app status	Patented
Application number	**16593561**
Continuity type	**Continuation of**

Petitioner Samsung Ex-1038, 0546

Prior app number	**16036506**
Filing Date	07/16/2018
Patent number	10530575
Issue date	01/07/2020

Prior app status	Patented
Application number	**16036506**
Continuity type	**Continuation of**
Prior app number	**15583968**
Filing Date	05/01/2017
Patent number	10057059
Issue date	08/21/2018

Prior app status	Patented
Application number	**15583968**
Continuity type	**Continuation of**
Prior app number	**15010905**
Filing Date	01/29/2016
Patent number	9641327
Issue date	05/02/2017

Prior app status	Patented
Application number	**15010905**
Continuity type	**Continuation of**
Prior app number	**14055606**
Filing Date	10/16/2013
Patent number	9276740
Issue date	03/01/2016

Foreign Priority Information

of foreign priority claims: 0

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. 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) 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).

Data was not provided for this section.

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

Checking this box will cause the application to be examined under the first inventor to file provisions of the AIA.

☐ 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 2016, 2013, will be examined under the first inventor to file provisions of the AIA.

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.

Petitioner Samsung Ex-1038, 0548

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 the 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.

Applicant Information

of applicants: 1

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.

1. **Network-1 Technologies, Inc.**
~~445 Park Avenue, Suite 912~~
~~New York, NY 10022~~
UNITED STATES

65 Locust Avenue
New Canaan, CT 06840

Applicant Organization
Applicant type Assignee

Phone: ---
Fax: ---
Email: ---

Assignee Information including Non-Applicant Assignee Information

of assignees: 0

An assignee-applicant identified in the "Applicant" section will appear on the patent application as an applicant.

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.

Petitioner Samsung Ex-1038, 0549

Data was not provided for this section.

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 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	First name	Last name	Registration #	Date
/Keith J. Barkaus/	Keith J.	Barkaus	51431	01/30/2023

Electronic Acknowledgement Receipt

EFS ID:	47450178
Application Number:	17647812
International Application Number:	
Confirmation Number:	6784
Title of Invention:	Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)
First Named Inventor/Applicant Name:	John A. Nix
Customer Number:	1912
Filer:	Keith J. Barkaus/Victoria Gilmore
Filer Authorized By:	Keith J. Barkaus
Attorney Docket Number:	63121/0213
Receipt Date:	30-JAN-2023
Filing Date:	12-JAN-2022
Time Stamp:	16:37:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	1-UpdatedADS.pdf	326205 48f7c0faca825998197bae32ee3742ed486849d3	no	6

Warnings:

Information:	
This is not an USPTO supplied ADS fillable form	
Total Files Size (in bytes):	326205

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.

PART B - FEE(S) TRANSMITTAL

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

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

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

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

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

1912 7590 10/31/2022
AMSTER, ROTHSTEIN & EBENSTEIN LLP
90 PARK AVENUE
NEW YORK, NY 10016

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

Certificate of Mailing or Transmission

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

Keith J. Barkaus	(Typed or printed name)
/Keith J. Barkaus/	(Signature)
January 30, 2023	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/647,812	01/12/2022	John A. Nix	63121/0213	6784

TITLE OF INVENTION: Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	01/31/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS
PEARSON, DAVID J	2438	713-156000

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/AIA/122 or PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or 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 Amster, Rothstein & Ebenstein LLP
2 _____
3 _____

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

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

(A) NAME OF ASSIGNEE	(B) RESIDENCE: (CITY and STATE OR COUNTRY)
Network-1 Technologies, Inc.	New Canaan, CT

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

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

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

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

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 011785

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 /Keith J. Barkaus/ Date January 30, 2023

Typed or printed name Keith J. Barkaus Registration No. 51,431

Petitioner Samsung Ex-1038, 0553

Electronic Patent Application Fee Transmittal

Application Number:	17647812
Filing Date:	12-Jan-2022
Title of Invention:	Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)
First Named Inventor/Applicant Name:	John A. Nix
Filer:	Keith J. Barkaus/Victoria Gilmore
Attorney Docket Number:	63121/0213

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
PUBL. FEE- EARLY, VOLUNTARY, OR NORMAL	1504	1	0	0
UTILITY APPL ISSUE FEE	2501	1	600	600
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**600**

Electronic Acknowledgement Receipt

EFS ID:	47450196
Application Number:	17647812
International Application Number:	
Confirmation Number:	6784
Title of Invention:	Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)
First Named Inventor/Applicant Name:	John A. Nix
Customer Number:	1912
Filer:	Keith J. Barkaus/Victoria Gilmore
Filer Authorized By:	Keith J. Barkaus
Attorney Docket Number:	63121/0213
Receipt Date:	30-JAN-2023
Filing Date:	12-JAN-2022
Time Stamp:	16:39:19
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$600
RAM confirmation Number	E20231TG39442123
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	213-PTOL-85.pdf	206197 311381c03a0c9b8383289b0d0dc66f91c8050fe8	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	40955 d57f5e4fa7548e3e6adf557e534eed3e32ac74bb	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	247152		

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.

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
17/647,812	01/12/2022	2438	1040	63121/0213	20	1

CONFIRMATION NO. 6784

CORRECTED FILING RECEIPT

1912
AMSTER, ROTHSTEIN & EBENSTEIN LLP
90 PARK AVENUE
NEW YORK, NY 10016

OC000000137399017

Date Mailed: 02/14/2023

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, 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 corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction 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 provided that the request is grantable.

Inventor(s)

John A. Nix, Evanston, IL;

Applicant(s)

Network-1 Technologies, Inc., New Canaan, CT;

Power of Attorney: The patent practitioners associated with Customer Number 1912

Domestic Priority data as claimed by applicant

This application is a CON of 16/593,561 10/04/2019 PAT 11258595
which is a CON of 16/036,506 07/16/2018 PAT 10530575
which is a CON of 15/583,968 05/01/2017 PAT 10057059
which is a CON of 15/010,905 01/29/2016 PAT 9641327
which is a CON of 14/055,606 10/16/2013 PAT 9276740

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Petitioner Samsung Ex-1038, 0558

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: 01/24/2022
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/647,812**
Projected Publication Date: Not Applicable
Non-Publication Request: No
Early Publication Request: No
**** SMALL ENTITY ****
Title

Systems and Methods for "Machine-to-Machine" (M2M) Communications Between Modules, Servers, and an Application using Public Key Infrastructure (PKI)

Preliminary Class

713

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

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

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

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

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

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

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

Petitioner Samsung Ex-1038, 0561

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	17647812
Filing Date	2022-01-12
First Named Inventor	John A. Nix
Art Unit	2438
Examiner Name	David J. PEARSON
Attorney Docket Number	63121/0213

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	9807605	B2	2017-10-31	Gao et al.	
	2	8577337	B2	2013-11-05	O'Leary	
Change(s) applied to document, /C.S./ 11/4/2022	3	9800993	B2	10/2017 ~~2013-11-05~~	Lee et al.	
	4	9794775	B2	2017-10-17	Huber et al.	
	5	9674690	B2	2017-06-06	Lee et al.	
	6	9628981	B2	2017-04-18	Park et al.	
	7	9572016	B2	2017-02-14	Cormier et al.	
	8	9332129	B2	2016-05-03	Li et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

14/084,141	63121/0134	2013-11-19	USP 9,319,223
14/064,618	63121/0133	2013-10-28	USP 9,118,464
14/055,606	63121/0132	2013-10-16	USP 9,276,740
14/039,401	63121/0131	2013-09-27	USP 9,288,059
14/023,181	63121/0130	2013-09-10	USP 9,350,550
AU 2019246774	63121-0199	2019-10-08	Published on 2021-09-23
GB 1608573	63121-0151	2014-10-27	Published on 2016-08-03
GB 2100530	63121-0201	2014-10-27	Published on 2021-05-12
CA 2,965,119	63121-0152	2014-10-27	Published on 2015-05-07
HK 17101082.8	63121-0153	2014-10-27	Published on 2017-10-20
EU 14868381.6	63121-0154	2014-12-04 EP	Published on 2017-01-04
CA 2,969,829	63121-0155	2014-12-04	Published on 2015-06-11
HK 17106540.3	63121-0156	2014-12-04	Published on 2018-01-19

Change(s) applied to document, /Q.N./ 11/10/2022

The Examiner is invited to review the prosecution history of each of these applications, including the cited references of record and related office actions, as the Examiner deems appropriate.

* * * * *

This Information Disclosure Statement is being filed within three months of the filing date and before the mailing date of a first Office Action on the merits in the present application. No certification or fee is required. Applicant(s) hereby petition(s) that the Information Disclosure Statement be considered. Please charge any fee deficiency or credit any overpayment to Deposit Account No. 01-1785, under Docket No. 63121/0213.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /DP/

Petitioner Samsung Ex-1038, 0563

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.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/647,812	03/14/2023	11606204	63121/0213	6784

20280 7590 02/22/2023

MOTOROLA MOBILITY LLC
222 West Merchandise Mart Plaza
Suite 1800
Chicago, IL 60654

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

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

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

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

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

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Patents Stakeholder Experience (OPSE), Stakeholder Support Division (SSD) at (571)-272-4200.

INVENTOR(s) (Please see PAIR WEB site http://pair.uspto.gov for additional inventors):

John A. Nix, Evanston, IL;

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

Network-1 Technologies, Inc., New Canaan, CT;

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