



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/054,020	02/25/2016	An Liu	MPS15-SP02	6551
106809	7590	01/11/2018		
Docket Clerk - SAMS P.O. Drawer 800889 Dallas, TX 75380			EXAMINER ABEDIN, SHANTO	
			ART UNIT 2436	PAPER NUMBER
			NOTIFICATION DATE 01/11/2018	DELIVERY MODE ELECTRONIC

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

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

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

patents@munckwilson.com
munckwilson@gmail.com
patent.srad@samsung.com

Office Action Summary	Application No. 15/054,020	Applicant(s) LIU ET AL.	
	Examiner SHANTO M. ABEDIN	Art Unit 2436	AIA (First Inventor to File) 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 03 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 02/25/2016.
☐ 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 02/25/2016 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 02/25/16; 03/01/16; 09/01/16 and 02/06/17.
- 3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date: ____.
- 4) ☐ Other: ____.

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

DETAILED ACTION

1. This office action is in response to the communication filed on 02/25/2016. Claims 1-20 are pending in the application. Claims 1-20 have been rejected.

Information Disclosure Statement

2. The information disclosure statements (IDS) submitted on 02/25/2016, 03/01/2016, 09/01/2016 and 02/06/2017 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement are being considered by the examiner.

Claim Rejections - 35 USC § 101

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

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

There are two criteria for determining subject matter eligibility under 35 U.S.C. 101 and both must be satisfied. The claimed invention (1) must be directed to one of the four statutory categories, and (2) must not be wholly directed to subject matter encompassing a judicially recognized exception, as defined below. The following two step analysis is used to evaluate these criteria.

Step 1 analysis: Is the claim directed to one of the four patent-eligible subject matter categories: process, machine, manufacture, or composition of matter? The subject matter of the claim must be directed to one of the four subject matter categories. If it is not, the claim is not eligible for patent protection and should be rejected under 35 U.S.C. 101, for at least this reason.

Step 2 analysis: Following the decision in *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 134 S.Ct. 2347 (2014) (citing *Mayo Collaborative Services v. Prometheus Labs., Inc.*, 132 S.Ct. 1289, 1300 (2012)), the claims are analyzed where the abstract idea judicial exception to the categories of statutory subject matter is at issue using the following two-part analysis set forth in *Mayo*: 1, e.g. step 2A) Determine whether the claim is directed to an abstract idea; and 2 e.g. step 2B) if an abstract idea is present in the claim, determine whether any element, or combination of elements, in the claim is sufficient to ensure that the claim amounts to significantly more than the abstract idea itself. See *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 134 S.Ct. at 2350.

For a detailed discussion of the analysis required to determine whether a claim is directed to patent-eligible subject matter, MPEP 2106 Patent Subject Matter Eligibility [R-07.2015] for detail explanations; and also the *2014 Interim Guidance on Patent Subject Matter Eligibility*, 79 Fed. Reg. 74618 (December 16, 2014) and related materials available at www.uspto.gov/patent/laws-and-regulations/examination-policy/2014-interim-guidance-subject-matter-eligibility-0.

3. Claims 15-20 are rejected under 35 USC 101 as the claimed invention is directed to non-statutory subject matter. The claim(s) does/do not fall within at least one of the four categories of patent eligible subject matter because of the reasons explained as bellows:

Regarding claims 15-20, they are directed to a ‘system’ comprising a processor and a communication interface configured to perform the claimed functionalities.

However, at the time of invention, software implementation of a processor (Note US 2007/0204153 A1, Tome et al, and US 2013/0007114 A1, WEE et al: virtual or software processor) and a communication interface (Note US 2016/0080468, Lambert et al, Para 0331: virtual NIC; and US 2016/0036892, Twitchell, JR, Para 114: virtual network interface) were also well known in the art. Furthermore, according to the specification (please see applicant’s specification Para 010: implementation using software and/ or firmware etc.), the claimed processor/ controller and communication system could optionally be implemented in software/ firmware only.

Therefore, the claimed system is interpreted as software only implemented system, or program per se product, and consequently fails “step 1” of the subject matter eligibility test. See MPEP 2106 Patent Subject Matter Eligibility [R-07. 2015]: non-limiting examples of non-statutory categories to include computer program per se products.

Claim Rejections - 35 USC § 103

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

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

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103 are summarized as follows:

1. Determining the scope and contents of the prior art.
 2. Ascertaining the differences between the prior art and the claims at issue.
 3. Resolving the level of ordinary skill in the pertinent art.
 4. Considering objective evidence present in the application indicating obviousness or nonobviousness.
4. Claims 1-5, 7-12, 14-18 and 20 are rejected under 35 U.S.C. 103 as being unpatentable over US 2014/0122873 A1 (hereinafter DEUTSCH et al) in view of US 2011/0022835 A1 (hereinafter Schibuk)

Regarding claim 1, DEUTSCH et al teaches a method for exchanging encrypted information by an electronic device, the method comprising:

generating one or more device certificates and one or more device keys, the one or more device certificates signed using a device unique key that is pre-stored on the electronic device (Note Para 034, 043, 073, 126: generated device certificates signed by attestation identity key, AIK);

transmitting the one or more device certificates to a token service provider (TSP) server (Note Figure 2A.207 and Figure 3.315; and Para 021, 126-127: trust broker sending certificate to the service provider; note, trust broker is interpreted as token service provider);

receiving one or more TSP certificates from the TSP server (Note Figure 2A.208; and Para 126-127: client receiving certificate from the trust broker; note, trust broker is interpreted as token service provider, TSP);

identifying one or more TSP public keys of the TSP server based on the one or more received TSP certificates (Note Para 020, 073, 127-129: affirming mutual attestation between service provider and client); and

transmitting a message including (i) the information encrypted based on the one or more identified TSP keys and (ii) a signature of the electronic device (Note Para 034, 039, 061, 127, 130: transmitting signed certificate, and providing service/ information encrypted by AIK key)

DEUTSCH et al fails to teach expressly the one or more device certificates signed using a device unique private key; and transmitting a message including the information encrypted based on the one or more identified TSP public keys.

However, Schibuk teaches the one or more device certificates signed using a device unique private key (Note Para 037, 057, 079: public key certificate associated with client/ device; may signed by the server); and transmitting a message including the information encrypted based on the one or more identified TSP public keys (Note Para 066, 092-093, 099: encrypted communication between client and server using asymmetric keys) Examiner notes, Schibuk further teaches authenticating a certificate from a token facility or credit issuer (Note Para 025, 076, 086, 093) that can also be interpreted as TSP.

Schibuk and DEUTSCH et al are from the same field of art of managing and authenticating secure transactions utilizing digital certificates. Therefore, at the time of invention, it would have been obvious to a person of ordinary skill in the art to combine the teaching of Schibuk with

DEUTSCH et al to implement a method further comprising the features of the one or more device certificates signed using a device unique private key, and transmitting a message including the information encrypted based on the one or more identified TSP public keys in order to provide users with alternative and well-known authentication mechanism utilizing public key based device certificates instead of AIK key based certificates (Note Schibuk, Para 003, 007)

Regarding claim 2, it is rejected applying as same motivation and rationale applied above rejecting claim 1, furthermore, Schibuk teaches the method, wherein:

a certificate of the device unique private key is signed using a root certificate authority (CA) private key of a manufacturer of the electronic device (Note Para 019, 057, 099: client device receiving public key certificate from certificate authority; determining root certificate), and the device unique private key is stored on the electronic device by the manufacturer for access by a trusted application of the electronic device (Note Para 057, 099: private key tied to the public key of the certificate)

Regarding claim 3, it is rejected applying as same motivation and rationale applied above rejecting claim 2, furthermore, Schibuk teaches the method wherein a public key for the root CA private key of the manufacturer of the electronic device is provided to the TSP by the manufacturer of the electronic device prior to the generating of the one or more device certificates and the one or more device public private key pairs (Note Para 057, 099)

Regarding claim 4, DEUTSCH et al teaches the method of claim 1, wherein identifying the one or more TSP public keys of the TSP server based on the one or more received TSP certificates comprises:

identifying a certificate of the TSP that is pre-stored on the electronic device for access by a trusted application of the electronic device (Note Para 020, 073, 127-129);

verifying authenticity of the one or more received TSP certificates based on the certificate using the trusted application (Note Para 020, 073, 127-129: affirming mutual attestation between service provider and client); and

identifying the one or more TSP keys in response to verifying the authenticity of the one or more received TSP certificates (Note Para 020, 039, 073, 128)

DEUTSCH et al teaches authentication of the client device and the trust broker or service provider using AIK key certificate, but fails to teach expressly identifying a root certificate authority (CA) certificate that is pre-stored on the electronic device; verifying authenticity of the one or more received certificates based on the root CA certificate; and identifying the one or more public keys in response to verifying the authenticity of the certificates.

However, Schibuk teaches identifying a root certificate authority (CA) certificate that is pre-stored on the electronic device (Note Para 019, 057, 099); verifying authenticity of the one or more received certificates based on the root CA certificate (Note Para 057, 099: client device receiving public key certificate from certificate authority; determining root certificate); and identifying the one or more public keys in response to verifying the authenticity of the certificates (Note Para 019, 057, 099: private key tied to the public key of the certificate) Schibuk further teaches authenticating a certificate from a token facility or credit issuer (Note Para 025, 076, 086, 093) that can also be interpreted as TSP.

Regarding claim 5, it is rejected applying as same motivation and rationale applied above rejecting claim 1, furthermore, Schibuk teaches the method, wherein:

the one or more device certificates include an encryption certificate and a signing certificate, the one or more device public private key pairs include a unique signing public private key pair (Note Para 037, 079, 099), and

the signature of the electronic device is based on a unique signing private key of the unique signing public private key pair (Note Para 019, 037, 079)

Regarding claim 7, it is rejected applying as same motivation and rationale applied above rejecting claim 1, furthermore, Schibuk teaches the method of claim 1, wherein the information includes information for registering payment information with the TSP, the payment information associated with the electronic device (Note Para 094-096: storing customer's credit/ payment information) Examiner notes, Schibuk further teaches a token facility or credit issuer (Note Para 025, 076, 086, 093) that can also be interpreted as TSP.

Regarding claim 8, DEUTSCH et al teaches an electronic device for exchanging encrypted information, the electronic device comprising:

at least one processor (Note Figure 7B.710: processor) configured to generate one or more device certificates and one or more device keys, the one or more device certificates signed using a device unique key that is pre-stored on the electronic device (Note Para 034, 043, 073, 126: generated device certificates signed by attestation identity key, AIK); and

a transceiver (Note Figure 7B.770: connectivity component) configured to transmit the one or more device certificates to a token service provider (TSP) server and receive one or more TSP certificates from the TSP server (Note Figure 2A.207 and Figure 3.315; and Para 021, 126-127: trust broker sending certificate to the service provider; note, trust broker is interpreted as token service provider),

wherein the at least one processor is further configured to identify one or more TSP keys of the TSP server based on the one or more received TSP certificates (Note Para 020, 073, 127-129: affirming mutual attestation between service provider and client), and

wherein the at least one transceiver is configured to transmit a message including (i) the information encrypted based on the one or more identified TSP keys and (ii) a signature of the electronic device (Note Para 034, 039, 061, 127, 130: transmitting signed certificate, and providing service/ information encrypted by AIK key)

DEUTSCH et al fails to teach expressly the one or more device certificates signed using a device unique private key; and transmitting a message including the information encrypted based on the one or more identified TSP public keys.

However, Schibuk teaches the one or more device certificates signed using a device unique private key (Note Para 037, 057, 079: public key certificate associated with client/ device; may signed by the server); and transmitting a message including the information encrypted based on the one or more identified TSP public keys (Note Para 066, 092-093, 099: encrypted communication between client and server using asymmetric keys) Examiner notes, Schibuk further teaches authenticating a certificate from a token facility or credit issuer (Note Para 025, 076, 086, 093) that can also be interpreted as TSP.

Schibuk and DEUTSCH et al are from the same field of art of managing and authenticating secure transactions utilizing digital certificates. Therefore, at the time of invention, it would have been obvious to a person of ordinary skill in the art to combine the teaching of Schibuk with DEUTSCH et al to implement a device further comprising the features of the one or more device certificates signed using a device unique private key, and transmitting a message including the

information encrypted based on the one or more identified TSP public keys in order to provide users with alternative and well-known authentication mechanism utilizing public key based device certificates instead of AIK key based certificates (Note Schibuk, Para 003, 007)

Regarding claim 9, it is rejected applying as same motivation and rationale applied above rejecting claim 8, furthermore, Schibuk teaches the electronic device wherein: a certificate of the device unique private key is signed using a root certificate authority (CA) private key of a manufacturer of the electronic device (Note Para 019, 057, 099: client device receiving public key certificate from certificate authority; determining root certificate), and the device unique private key is stored on the electronic device by the manufacturer for access by a trusted application of the electronic device (Note Para 057, 099: private key tied to the public key of the certificate)

Regarding claim 10, it is rejected applying as same motivation and rationale applied above rejecting claim 8, furthermore, Schibuk teaches the electronic device of claim 9, wherein a public key for the root CA private key of the manufacturer of the electronic device is provided to the TSP by the manufacturer of the electronic device prior to the generating of the one or more device certificates and the one or more device public private key pairs (Note Para 057, 099)

Regarding claim 11, DEUTSCH et al teaches the electronic device of claim 8, wherein to identify the one or more TSP public keys of the TSP server based on the one or more received TSP certificates, the at least one processor is configured to: identify a certificate of the TSP that is pre-stored on the electronic device for access by a trusted application of the electronic device ((Note Para 020, 073, 127-129); verify authenticity of the one or more received TSP certificates based on the TSP certificate using the trusted application (Note Para 020, 073, 127-129: affirming mutual attestation between service provider and client); and identify the one or more TSP public keys in

response to verifying the authenticity of the one or more received TSP certificates (Note Para 020, 039, 073, 128)

DEUTSCH et al teaches authentication of the client device and the trust broker or service provider using AIK key certificate, but fails to teach expressly identifying a root certificate authority (CA) certificate that is pre-stored on the electronic device; verifying authenticity of the one or more received certificates based on the root CA certificate; and identifying the one or more public keys in response to verifying the authenticity of the certificates.

However, Schibuk teaches identifying a root certificate authority (CA) certificate that is pre-stored on the electronic device (Note Para 019, 057, 099); verifying authenticity of the one or more received certificates based on the root CA certificate (Note Para 057, 099: client device receiving public key certificate from certificate authority; determining root certificate); and identifying the one or more public keys in response to verifying the authenticity of the certificates (Note Para 019, 057, 099: private key tied to the public key of the certificate) Schibuk further teaches authenticating a certificate from a token facility or credit issuer (Note Para 025, 076, 086, 093) that can also be interpreted as TSP.

Regarding claim 12, it is rejected applying as same motivation and rationale applied above rejecting claim 8, furthermore, Schibuk teaches the electronic device wherein: the one or more device certificates include an encryption certificate and a signing certificate, the one or more device public private key pairs include a unique signing public private key pair (Note Para 037, 079, 099), and the signature of the electronic device is based on a unique signing private key of the unique signing public private key pair (Note Para 019, 037, 079)

Regarding claim 14, it is rejected applying as same motivation and rationale applied above rejecting claim 8, furthermore, Schibuk teaches the electronic device wherein the information includes information for registering payment information with the TSP, the payment information associated with the electronic device (Note Para 094-096: storing customer's credit/ payment information) Examiner notes, Schibuk further teaches a token facility or credit issuer (Note Para 025, 076, 086, 093) that can also be interpreted as TSP.

Regarding claim 15, DEUTSCH et al teaches a system for exchanging encrypted information of a token service provider (TSP), the system comprising:

at least one processor (Note Figure 7B.710: processor) configured to generate one or more TSP certificates and one or more TSP keys (Note Para 034, 043, 073, 126: generated device certificates signed by attestation identity key, AIK); and

a communication interface (Note Figure 7B.770: connectivity component) configured to transmit the one or more TSP certificates to an electronic device and receive one or more device certificates from the electronic device (Note Figure 2A.207 and Figure 3.315; and Para 021, 126-127: trust broker sending certificate to the service provider; note, trust broker is interpreted as token service provider),

wherein the at least one processor is further configured to verify an authenticity of the one or more device certificates based on a key of a manufacturer of the electronic device (Note Para 020, 073, 127-129: affirming mutual attestation between service provider and client using certificates and AIK key), and

wherein the communication interface is configured to receive, from the electronic device, a message including (i) the information encrypted based on one or more TSP keys of the one or more

TSP keys and (ii) a signature of the electronic device (Note Para 034, 039, 061, 127, 130: transmitting signed certificate, and providing service/ information encrypted by AIK key)

DEUTSCH et al fails to teach expressly the one or more TSP certificates signed using a TSP root certificate authority (CA) private key; verifying an authenticity of the certificates based on a public key for a root CA private key; and receiving a message including the information encrypted based on the one or more identified TSP public keys.

However, Schibuk teaches the one or more TSP certificates signed using a TSP root certificate authority (CA) private key (Note Para 037, 057, 079, 099: public key certificate associated with client/ device; may signed by the server); verifying an authenticity of the certificates based on a public key for a root CA private key (Note Para 019, 057, 099: client device receiving public key certificate from certificate authority; determining root certificate); and receiving a message including the information encrypted based on the one or more identified TSP public keys (Note Para 066, 092-093, 099: encrypted communication between client and server using asymmetric keys) Examiner notes, Schibuk further teaches authenticating a certificate from a token facility or credit issuer (Note Para 025, 076, 086, 093) that can also be interpreted as TSP.

Schibuk and DEUTSCH et al are from the same field of art of managing and authenticating secure transactions utilizing digital certificates. Therefore, at the time of invention, it would have been obvious to a person of ordinary skill in the art to combine the teaching of Schibuk with DEUTSCH et al to implement a device further comprising the features of one or more TSP certificates signed using a TSP root certificate authority (CA) private key, verifying an authenticity of the certificates based on a public key for a root CA private key, and receiving a message including the information encrypted based on the one or more identified TSP public keys in order to provide

users with alternative and well-known authentication mechanism utilizing public key based device certificates instead of AIK key based certificates (Note Schibuk, Para 003, 007)

Regarding claim 16, it is rejected applying as same motivation and rationale applied above rejecting claim 15, furthermore, Schibuk teaches the system wherein: the communication interface is configured to receive a root CA certificate of the manufacturer of the electronic device during a secure certificate exchange with a server of the manufacturer (Note Para 019, 057, 099: client device receiving public key certificate from certificate authority; determining root certificate), and the at least one processor is further configured to identify the public key for the root CA private key of the manufacturer based on the received root CA certificate of the manufacturer (Note Para 057, 099: private key tied to the public key of the certificate)

Regarding claim 17, it is rejected applying as same motivation and rationale applied above rejecting claim 16, furthermore, Schibuk teaches the system wherein the communication interface is configured to provide a root certificate authority (CA) certificate of the TSP to the server of the manufacturer during the secure certificate exchange for storage on the electronic device and verification of the TSP (Note Para 057, 099)

Regarding claim 18, it is rejected applying as same motivation and rationale applied above rejecting claim 15, furthermore, Schibuk teaches the system wherein: the one or more TSP certificates include an encryption certificate and a signing certificate (Note Para 037, 079, 099), and the one or more TSP public private key pairs include a unique signing public private key pair (Note Para 019, 037, 079)

Regarding claim 20, it is rejected applying as same motivation and rationale applied above rejecting claim 15, furthermore, Schibuk teaches the system wherein the information includes

information for registering payment information with the TSP, the payment information associated with the electronic device (Note Para 094-096: storing customer's credit/ payment information) Examiner notes, Schibuk further teaches a token facility or credit issuer (Note Para 025, 076, 086, 093) that can also be interpreted as TSP.

5. Claims 6, 13 and 19 are rejected under 35 U.S.C. 103 as being unpatentable over DEUTSCH et al in view of Schibuk further in view of US 2014/0101679 A1 (hereinafter Yin et al)

Regarding claims 6, 13 and 19, they are rejected applying as same motivation and rationale applied above rejecting claims 1, 8 and 15, furthermore, Schibuk teaches the method/ device/ system wherein the information in the message is encrypted using a unique key and the unique key is encrypted using a public encryption key that is included in the one or more identified public keys (Note Para 066, 092-093, 099: encrypted communication between client and server using asymmetric keys; transmitting encryption in secure channel)

Modified Schibuk- DEUTSCH et al method fails to teach expressly wherein the information in the message is encrypted using a unique session key and the unique session key is encrypted using a TSP public encryption key.

However, Yin et al teaches wherein the information in the message is encrypted using a unique session key and the unique session key is encrypted using a TSP public encryption key (Note Para 071, 073: session key may be encrypted using public key) Yin et al further teaches authenticating a security token service that can be interpreted as TSP.

Yin et al and DEUTSCH et al are from the same field of art of managing and authenticating secure transactions utilizing digital certificates. Therefore, at the time of invention, it would have

Art Unit: 2436

been obvious to a person of ordinary skill in the art to combine the teaching of Yin et al with modified Schibuk-DEUTSCH et al method/ device/ system to further include the features of wherein the information in the message is encrypted using a unique session key and the unique session key is encrypted using a TSP public encryption key in order to provide users with a secure and efficient mechanism for transferring transactional/ keying information (Note Yin et al, Para 013, 073)

Conclusion

6. A shortened statutory period for response to this action is set to expire in 3 (Three) months and 0 (Zero) days from the mailing date of this letter. Failure to respond within the period for response will result in ABANDONMENT of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M. Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 8:30 AM to 6:30 PM.

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, Shewaye Gelagay, can be reached on 571-272-4219. The RightFax number for faxing directly to the examiner is 571-273-3551.

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

/SHANTO M ABEDIN/

Primary Examiner, Art Unit 2436

DOCKET NO.: MPS15-SP02 (SAMS12-00063)
Customer No. 106809

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of : An Liu, et al.
Application No. : 15/054,020
Filed : February 25, 2016
For : TRUST-ZONE-BASED END-TO-END SECURITY
Group No. : 2436
Examiner : Shanto Abedin
Confirmation No. : 6551

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

Sir:

AMENDMENT AND RESPONSE TO OFFICE ACTION

In response to the Office Action dated January 11, 2018, please amend the above-identified application as follows:

IN THE CLAIMS:

Please amend the claims as follows. Any other difference between the claims below and the previous state of the claims is unintentional and in the nature of a typographical error.

1. (Currently Amended) A method for exchanging encrypted information by an electronic device, the method comprising:

generating, by the device, a device signing certificate and a device signing public private key pair, and a device encryption certificate and a device encryption public private key pair ~~one or more device certificates and one or more device public private key pairs,~~ each of the device signing and encryption ~~the one or more device~~ certificates signed using a device unique private key that is pre-stored on the electronic device;

transmitting, by the device, the device signing and device encryption ~~the one or more device~~ certificates to a token service provider (TSP) server;

receiving, by the device, a TSP signing certificate and a TSP encryption certificate ~~one or more TSP certificates~~ from the TSP server;

identifying, by the device a TSP signing public key and a TSP encryption public key ~~one or more TSP public keys~~ of the TSP server based on the ~~one or more~~ received TSP signing and the received TSP encryption certificates; and

transmitting a message including (i) ~~[[the]]~~ information encrypted based on the TSP encryption public key ~~one or more identified TSP public keys~~ and (ii) a signature of the electronic device based on the device signing private key.

2. (Original) The method of Claim 1, wherein:
a certificate of the device unique private key is signed using a root certificate authority (CA)
private key of a manufacturer of the electronic device, and
the device unique private key is stored on the electronic device by the manufacturer for
access by a trusted application of the electronic device.

3. (Original) The method of Claim 2, wherein a public key for the root CA private
key of the manufacturer of the electronic device is provided to the TSP by the manufacturer of the
electronic device prior to the generating of the one or more device certificates and the one or more
device public private key pairs.

4. (Currently Amended) The method of Claim 1, wherein identifying the TSP signing
and TSP encryption ~~one or more TSP~~ public keys of the TSP server based on the ~~one or more~~
received TSP signing and TSP encryption certificates comprises:

identifying a root certificate authority (CA) certificate of the TSP that is pre-stored on the
electronic device for access by a trusted application of the electronic device;

verifying authenticity of the one or more received TSP signing and TSP encryption
certificates based on the TSP root CA certificate using the trusted application; and

identifying the ~~one or more~~ TSP signing and TSP encryption public keys in response to
verifying the authenticity of the ~~one or more~~ received TSP signing and TSP encryption certificates.

5. (Canceled)

6. (Currently Amended) The method of Claim 1, wherein the information in the message is encrypted using a unique session key and the unique session key is encrypted using the TSP encryption key of a TSP encryption public private key pair ~~a TSP public encryption key that is included in the one or more identified TSP public keys.~~

7. (Original) The method of Claim 1, wherein the information includes information for registering payment information with the TSP, the payment information associated with the electronic device.

8. (Currently Amended) An electronic device for exchanging encrypted information, the electronic device comprising:

at least one processor configured to generate a device signing certificate and a device signing public private key pair, and to generate a device encryption certificate and a device encryption public private key pair ~~one or more device certificates and one or more device public private key pairs~~, the ~~one or more~~ device signing and encryption certificates signed using a device unique private key that is pre-stored on the electronic device; and

a transceiver configured to transmit the ~~one or more~~ device signing and encryption certificates to a token service provider (TSP) server and to receive a TSP signing certificate and TSP encryption certificate ~~one or more TSP certificates~~ from the TSP server,

wherein the at least one processor is further configured to identify a TSP signing public key and a TSP encryption public key ~~one or more TSP public keys~~ of the TSP server based on the ~~one or more~~ received TSP signing and encryption certificates, and

wherein the ~~at least one~~ transceiver is configured to transmit a message including (i) ~~[[the]]~~ information encrypted based on the TSP encryption public key ~~one or more identified TSP public keys~~ and (ii) a signature of the electronic device based on the device signing private key.

9. (Original) The electronic device of Claim 8, wherein:
a certificate of the device unique private key is signed using a root certificate authority (CA)
private key of a manufacturer of the electronic device, and
the device unique private key is stored on the electronic device by the manufacturer for
access by a trusted application of the electronic device.

10. (Original) The electronic device of Claim 9, wherein a public key for the root CA
private key of the manufacturer of the electronic device is provided to the TSP by the manufacturer
of the electronic device prior to the generating of the one or more device certificates and the one or
more device public private key pairs.

11. (Currently Amended) The electronic device of Claim 8, wherein to identify the TSP
signing and TSP encryption ~~one or more~~ TSP public keys of the TSP server based on the ~~one or
more~~ received TSP signing and TSP encryption certificates, the at least one processor is configured
to:

identify a root certificate authority (CA) certificate of the TSP that is pre-stored on the
electronic device for access by a trusted application of the electronic device;

verify authenticity of the ~~one or more~~ received TSP signing and TSP encryption certificates
based on the TSP root CA certificate using the trusted application; and

identify the ~~one or more~~ TSP signing and TSP encryption public keys in response to
verifying the authenticity of the ~~one or more~~ received TSP signing and TSP encryption certificates.

12. (Canceled)

13. (Currently Amended) The electronic device of Claim 8, wherein the information in the message is encrypted using a unique session key and the unique session key is encrypted using the TSP encryption public a TSP public encryption key of a TSP encryption public private key pair ~~that is included in the one or more identified TSP public keys.~~

14. (Original) The electronic device of Claim 8, wherein the information includes information for registering payment information with the TSP, the payment information associated with the electronic device.

15. (Currently Amended) A system for exchanging encrypted information of a token service provider (TSP), the system comprising:

a TSP server comprising:

at least one processor configured to generate a TSP signing certificate and a TSP signing public private key pair, and a TSP encryption certificate and a TSP encryption public private key pair, the TSP signing and TSP encryption ~~one or more TSP certificates and one or more TSP public private key pairs, the one or more TSP certificates signed using a TSP root certificate authority (CA) private key; and~~

a communication interface configured to transmit the ~~one or more~~ TSP signing and TSP encryption certificates to an electronic device and to receive a device signing certificate and a device encryption certificate ~~one or more device certificates~~ from the electronic device,

wherein the at least one processor is further configured to verify an authenticity of the ~~one or more~~ device signing and device encryption certificates based on a public key for a root CA private key of a manufacturer of the electronic device, and

wherein the communication interface is configured to receive, from the electronic device, a message including (i) ~~[[the]]~~ information encrypted based on the TSP encryption public key of the TSP encryption public private key pair ~~one or more TSP public keys of the one or more TSP public private key pairs~~ and (ii) a signature of the electronic device.

16. (Original) The system of Claim 15, wherein:

the communication interface is configured to receive a root CA certificate of the manufacturer of the electronic device during a secure certificate exchange with a server of the manufacturer, and

the at least one processor is further configured to identify the public key for the root CA private key of the manufacturer based on the received root CA certificate of the manufacturer.

17. (Original) The system of Claim 16, wherein the communication interface is configured to provide a root certificate authority (CA) certificate of the TSP to the server of the manufacturer during the secure certificate exchange for storage on the electronic device and verification of the TSP.

18. (Canceled)

19. (Currently Amended) The system of Claim 15, wherein the information in the message is encrypted using a unique session key and the unique session key is encrypted using the TSP encryption public key ~~a TSP public encryption key that is included in the one or more TSP public keys.~~

20. (Original) The system of Claim 15, wherein the information includes information for registering payment information with the TSP, the payment information associated with the electronic device.

REMARKS

Claims 1-20 were pending in this application.

Claims 1-20 have been rejected.

Claims 1, 4, 6, 8, 11, 13, 15 and 19 have been amended.

Claims 5, 12 and 18 have been canceled.

Claims 1-4, 6-11, 13-17, 19 and 20 are now pending in this application.

Reconsideration of the claims is respectfully requested.

I. CLAIMS REJECTIONS – 35 U.S.C. § 101

Claims 15-20 were rejected under 35 U.S.C. § 101 because the claims are directed to non-statutory subject matter. This rejection respectfully is traversed.

As an initial matter, the Office Action broadly treats all claims 15-20 as a group, with no individual analysis. The Office Action does not address the differences in scope between independent Claim 15 and any of the dependent Claims 16-20. Such blanket treatment without individual analysis is improper. “[T]he question of eligible subject matter must be determined on a claim-by-claim basis.” *Ultramercial, Inc. v. Hulu, LLC*, 722 F.3d 1335, 1340 (Fed. Cir. 2013), *judgment vacated on other grounds by WildTangent, Inc. v. Ultramercial, LLC*, 134 S.Ct. 2870 (2014).

The Office Action asserts that “the claimed system is interpreted as software only implemented system, or program per se product.” *Office Action*, p. 4. This is not correct. For example, Claim 15 recites a TSP server comprising at least one processor. A person of ordinary skill in the art would readily interpret a server comprising a processor as being a physical device, not

merely software. As such, Applicant respectfully submits that the claims recite a machine, which is a “concrete thing, consisting of parts, or of certain devices and combination of devices and, as such, is within the four categories of statutory subject matter and, furthermore, is not Abstract.

Accordingly, the Applicant respectfully requests that the § 101 rejection with respect to Claims 15-17, 19 and 20 be withdrawn.

II. CLAIM REJECTIONS – 35 U.S.C. § 103

Claims 1-5, 7-12, 14-18, and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Publication No. 2014/0122873 to *Deutsch et al.* (“*Deutsch*”) in view of U.S. Patent Publication No. 2011/0022835 to *Schibuk* (“*Schibuk*”). Claims 6, 13, and 19 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Deutsch* in view of *Schibuk* and further in view of U.S. Patent Publication No. 2014/0101679 to *Yin et al.* (“*Yin*”). The Applicant respectfully traverses the rejection.

In *ex parte* examination of patent applications, the Patent Office bears the burden of establishing a *prima facie* case of obviousness. *MPEP* § 2142. Absent such a *prima facie* case, the Applicant is under no obligation to produce evidence of nonobviousness. *MPEP* § 2142.

Amended Claim 1 recites:

A method for exchanging encrypted information by an electronic device, the method comprising:

generating, by the device, a device signing certificate and a device signing public private key pair, and a device encryption certificate and a device encryption public private key pair, each of the device signing and encryption certificates signed using a device unique private key that is pre-stored on the electronic device;

transmitting, by the device, the device signing and device encryption certificates to a token service provider (TSP) server;

receiving, by the device, a TSP signing certificate and a TSP encryption certificate from the TSP server;

identifying, by the device a TSP signing public key and a TSP encryption public key of the TSP server based on the received TSP signing and the received TSP encryption certificates; and

transmitting a message including (i) information encrypted based on the TSP encryption public key and (ii) a signature of the electronic device based on the device signing private key.

Non-limiting support for this amendment can be found in the Specification as filed, such as in paragraphs [0055]-[0059] and FIG. 6. No new matter has been added.

Deutsch relates to a system of cryptographic enforcement based on mutual attestation for cloud services. *Deutsch*, para. [0037]. None of the cited *Deutsch* paragraphs [0034], [0043], [0073], [0126], [0021], [0126]-[0127], [0020], [0127]-[0129], [0034], [0039], [0061], [0130], and, in fact nothing in *Deutsch* teaches, suggests or contemplates “generating, by the device, a device signing certificate and a device signing public private key pair, and a device encryption certificate and a device encryption public private key pair, each of the device signing and encryption certificates signed using a device unique private key that is pre-stored on the electronic device” and “transmitting, by the device, the device signing and device encryption certificates to a token service provider (TSP) server.” Further, there is no teaching suggestion or contemplation in *Deutsch* for “receiving, by the device, a TSP signing certificate and a TSP encryption certificate from the TSP server” and “identifying, by the device a TSP signing public key and a TSP encryption public key of the TSP server based on the received TSP signing and the received TSP encryption certificates.”

The Office Action concedes that *Deutsch* fails to teach expressly the one or more device certificates signed used a device unique private key; and transmitting a message including the information encrypted based on the one or more identified TSP public keys. Office Action, p. 6.

The Office Action cites paragraphs [0037], [0057], [0079] of *Schibuk*, which like *Deutsch*, do not teach suggest or contemplate “generating, by the device, a device signing certificate and a device signing public private key pair, and a device encryption certificate and a device encryption public private key pair, each of the device signing and encryption certificates signed using a device unique private key that is pre-stored on the electronic device.”

Schibuk at cited paragraphs [0057] and [0079] states:

[0057] In the prior art, attackers have circumvented this restriction by attacking the encryption and decryption keys themselves. Prior art servers would obtain the public encryption key of a client device from a certificate authority (CA) in a public key infrastructure, typically by accessing the Internet. As the Internet is insecure, would-be attackers have successfully posed as the CA in addition to posing as the client 110. Thus, the attacker posing as the CA provides the server with a public key purportedly tied to a private key of the individual, that is in reality tied to a private key of the attacker. Thus, the server encrypts the response message using the attacker's public key, which the attacker then decrypts using the associated private key. *Schibuk*, para. [0057].

[0079] In process 440 the server creates a light-weight certificate (LWC) containing the shared secret. The LWC may be digitally signed by the server using the server's public key for added security, but a digital signature is not required. The certificate does not contain any information that a third party may rely upon to securely identify the individual. But, because it created the LWC for the individual, the server has unique knowledge of the association between the LWC and the individual. In process 450, the server stores data representing this association, and the shared secret, in a secure location accessible only to the authentication service. As noted before, the server need not store these data locally, but may store them in a storage network so that other servers may have access to them. For example, the data

may be stored in a shared database as a database record, although other embodiments may be used. *Schibuk*, para. [0079].

Although *Schibuk* discusses a light weight certificate (LWC) containing a shared secret (i.e., a public key), the LWC is created by the server, not the individual [device]. Furthermore, the server's public key is used to sign the certificate, not "a device unique private key that is pre-stored on the electronic device."

Applicant further points out that *Schibuk* does not remedy the inadequacies of *Deutsch*. *Schibuk* also does not provide any teaching suggestion or contemplation of "generating, by the device, a device signing certificate and a device signing public private key pair, and a device encryption certificate and a device encryption public private key pair, each of the device signing and encryption certificates signed using a device unique private key that is pre-stored on the electronic device; transmitting, by the device, the device signing and device encryption certificates to a token service provider (TSP) server; receiving, by the device, a TSP signing certificate and a TSP encryption certificate from the TSP server; identifying, by the device a TSP signing public key and a TSP encryption public key of the TSP server based on the received TSP signing and the received TSP encryption certificates; and transmitting a message including (i) information encrypted based on the TSP encryption public key and (ii) a signature of the electronic device based on the device signing private key."

Yin is provided for its alleged teaching regarding information in a message using a unique session key and the unique session key being encrypted using a TSP public encryption key. Office Action, p. 16. *Yin* does not provide a disclosure that remedies the deficiencies of *Deutsch* and *Schibuk*.

For at least these reasons, Claim 1 is patentable over the cited references, *Deutsch*, *Schibuk*, and *Yin*, alone or in combination. Furthermore, Claim 8 recites features analogous to those recited in Claim 1. Therefore, Claim 8 is allowable for the same or similar reasons as Claim 1. Accordingly, Applicant respectfully requests that the § 103 rejection of Claims 1 and 8, and their respective dependent claims be withdrawn.

Amended independent Claim 15 is analogous to Claim 1, except it is written with respect to this TSP server rather than with respect to the electronic device. For example, Claim 15 recites that the TSP server comprises “at least one processor configured to generate a TSP signing certificate and a TSP signing public private key pair, and a TSP encryption certificate and a TSP encryption public private key pair, the TSP signing and TSP encryption certificates signed using a TSP root certificate authority (CA) private key.” As discussed above with respect to Claim 1, the cited references, alone or in combination, do not teach suggest or contemplate each and every element of Claim 15. Accordingly, Claim 15 and its dependent claims are allowable over the cited references. Accordingly, Applicant respectfully requests that the § 103 rejection of Claim 15 and its dependent claims be withdrawn.

CONCLUSION

The Applicant respectfully asserts that all pending claims in this application are in condition for allowance and respectfully requests full allowance of the claims.

If any issues arise or if the Examiner has any suggestions for expediting allowance of this application, the Applicant respectfully invites the Examiner to contact the undersigned at the telephone number below or at *mrodriguez@munckwilson.com*.

The Commissioner is hereby authorized to charge any fees connected with this communication (including any extension of time fee) or credit any overpayment to Deposit Account No. 50-0208.

Respectfully submitted,

MUNCK WILSON MANDALA, LLP

Date: April 11, 2018

/Michael G. Rodriguez, #60,236/
Michael G. Rodriguez
Registration No. 60,236

P.O. Drawer 800889
Dallas, Texas 75380
(972) 628-3600 (main number)
(972) 628-3616 (fax)
E-mail: *mrodriguez@munckwilson.com*



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

106809 7590 08/02/2018
Docket Clerk - SAMS
P.O. Drawer 800889
Dallas, TEXAS 75380
UNITED STATES OF AMERICA

EXAMINER	
ABEDIN, SHANTO	
ART UNIT	PAPER NUMBER
2494	

DATE MAILED: 08/02/2018

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/054,020	02/25/2016	An Liu	MPS15-SP02	6551

TITLE OF INVENTION: TRUST-ZONE-BASED END-TO-END SECURITY

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$1000	\$0.00	\$0.00	\$1000	11/02/2018

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

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

HOW TO REPLY TO THIS NOTICE:

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

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

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

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

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

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

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

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail** Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

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

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

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.

106809 7590 08/02/2018
Docket Clerk - SAMS
P.O. Drawer 800889
Dallas, TEXAS 75380
UNITED STATES OF AMERICA

Certificate of Mailing or Transmission

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

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/054,020	02/25/2016	An Liu	MPS15-SP02	6551

TITLE OF INVENTION: TRUST-ZONE-BASED END-TO-END SECURITY

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	\$1000	\$0.00	\$0.00	\$1000	11/02/2018

EXAMINER	ART UNIT	CLASS-SUBCLASS
ABEDIN, SHANTO	2494	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/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

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

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

1	_____
2	_____
3	_____

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

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

(A) NAME OF ASSIGNEE

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

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

4a. The following fee(s) are submitted:

☐ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies _____

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

☐ A check is enclosed.

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

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

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

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

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

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

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

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

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/054,020	02/25/2016	An Liu	MPS15-SP02	6551
106809	7590	08/02/2018	EXAMINER	
Docket Clerk - SAMS P.O. Drawer 800889 Dallas, TEXAS 75380 UNITED STATES OF AMERICA			ABEDIN, SHANTO	
			ART UNIT	PAPER NUMBER
			2494	

DATE MAILED: 08/02/2018

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

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

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

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

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

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

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

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

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

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

Notice of Allowability	Application No. 15/054,020	Applicant(s) Liu et al.	
	Examiner SHANTO ABEDIN	Art Unit 2494	AIA Status Yes

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

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

1. ☒ This communication is responsive to filing of 04/11/2018.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

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

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

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

Certified copies:

a) ☐ All b) ☐ Some *c) ☐ None of the:

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

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

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

* Certified copies not received: _____.

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

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

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

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

Attachment(s)

1. ☒ Notice of References Cited (PTO-892) 2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date <u>02/15/2018 and 06/13/2018</u> . 3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____. 4. ☒ Interview Summary (PTO-413), Paper No./Mail Date. <u>07/26/2018</u> .	5. ☒ Examiner's Amendment/Comment 6. ☒ Examiner's Statement of Reasons for Allowance 7. ☐ Other _____.
--	---

/SHANTO ABEDIN/
Primary Examiner, Art Unit 2494

Continuation of 3. The allowed claim(s) is/are: 1-4,6,8-11,13,15-17 and 19

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.

DETAILED ACTION

1. This is in response to the communication filed on 04/11/2018.
2. Claims 1-4, 6-11, 13-17 and 19-20 were pending in the application. Claims 7, 14 and 20 have been cancelled through examiner's amendments made in this office action. Claims 1-4, 6, 8-11, 13, 15-17 and 19 have been allowed.

Examiner's Amendment

3. An examiner's amendment to the record appears below. Should the changes and/ or additions be unacceptable to the applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee. Authorization for this examiner's amendment was given in a telephone interview with the applicant's representative Mr. Michael Rodriguez (Reg. No. 60,236) on July 26, 2018. Claims 1, 2, 7, 8, 9, 11, 14, 15, 16, 17 and 20 have been amended as follows:

Claim 1. (Currently Amended) A method for exchanging encrypted information by an electronic device, the method comprising:

generating, by the device, a device signing certificate and a device signing public private key pair, and a device encryption certificate and a device encryption public private key pair, each of the device signing and encryption certificates signed using a device unique private key that is pre-stored on the electronic device;

transmitting, by the device, the device signing and device encryption certificates to a token service provider (TSP) server;

receiving, by the device, a TSP signing certificate and a TSP encryption certificate from the TSP server;

identifying, by the device a TSP signing public key and a TSP encryption public key of the TSP server based on the received TSP signing and the received TSP encryption certificates; and

transmitting a message including (i) information encrypted based on the TSP encryption public key and (ii) a signature of the electronic device based on the device signing private key,

wherein the device unique private key is stored on the electronic device by the manufacturer for access by a trusted application of the electronic device and wherein the information includes information for registering payment information with the TSP, the payment information associated with the electronic device.

Claim 2. (Currently Amended) The method of Claim 1, wherein:
a certificate of the device unique private key is signed using a root certificate authority (CA) private key of a manufacturer of the electronic device; ~~and~~
~~the device unique private key is stored on the electronic device by the manufacturer for access by a trusted application of the electronic device.~~

Claim 7. (Canceled)

Claim 8. (Currently Amended) An electronic device for exchanging encrypted information, the electronic device comprising:

at least one hardware processor configured to generate a device signing certificate and a device signing public private key pair, and to generate a device encryption certificate and a device

encryption public private key pair, the device signing and encryption certificates signed using a device unique private key that is pre-stored on the electronic device; and

a transceiver configured to transmit the device signing and encryption certificates to a token service provider (TSP) server and to receive a TSP signing certificate and TSP encryption certificate from the TSP server,

wherein the at least one hardware processor is further configured to identify a TSP signing public key and a TSP encryption public key of the TSP server based on the received TSP signing and encryption certificates, and

wherein the transceiver is configured to transmit a message including (i) information encrypted based on the TSP encryption public key and (ii) a signature of the electronic device based on the device signing private key,

wherein the device unique private key is stored on the electronic device by the manufacturer for access by a trusted application of the electronic device and wherein the information includes information for registering payment information with the TSP, the payment information associated with the electronic device.

Claim 9. (Currently Amended) The electronic device of Claim 8, wherein:
a certificate of the device unique private key is signed using a root certificate authority (CA) private key of a manufacturer of the electronic device ~~;~~ and

~~—— the device unique private key is stored on the electronic device by the manufacturer for access by a trusted application of the electronic device.~~

Claim 11. (Currently Amended) The electronic device of Claim 8, wherein to identify the TSP signing and TSP encryption public keys of the TSP server based on the received TSP signing and TSP encryption certificates, the at least one hardware processor is configured to:

identify a root certificate authority (CA) certificate of the TSP that is pre-stored on the electronic device for access by a trusted application of the electronic device;

verify authenticity of the received TSP signing and TSP encryption certificates based on the TSP root CA certificate using the trusted application; and

identify the TSP signing and TSP encryption public keys in response to verifying the authenticity of the received TSP signing and TSP encryption certificates.

Claim 14. (Canceled)

Claim 15. (Currently Amended) A system for exchanging encrypted information of a token service provider (TSP), the system comprising:

a TSP server comprising:

at least one hardware processor configured to generate a TSP signing certificate and a TSP signing public private key pair, and a TSP encryption certificate and a TSP encryption public private key pair, the TSP signing and TSP encryption certificates signed using a TSP root certificate authority (CA) private key; and

a ~~communication interface~~ transceiver configured to transmit the TSP signing and TSP encryption certificates to an electronic device and to receive a device signing certificate and a device encryption certificate from the electronic device,

wherein the at least one hardware processor is further configured to verify an authenticity of the device signing and device encryption certificates based on a public key for a root CA private key of a manufacturer of the electronic device, and

wherein the ~~communication interface~~ transceiver is configured to receive, from the electronic device, a message including (i) information encrypted based on the TSP encryption public key of the TSP encryption public private key pair and (ii) a signature of the electronic device,

wherein the device unique private key is stored on the electronic device by the manufacturer for access by a trusted application of the electronic device and wherein the information includes information for registering payment information with the TSP, the payment information associated with the electronic device.

Claim 16. (Currently Amended) The system of Claim 15, wherein:

the ~~communication interface~~ transceiver is configured to receive a root CA certificate of the manufacturer of the electronic device during a secure certificate exchange with a server of the manufacturer, and

the at least one hardware processor is further configured to identify the public key for the root CA private key of the manufacturer based on the received root CA certificate of the manufacturer.

Claim 17. (Currently Amended) The system of Claim 16, wherein the ~~communication interface~~ transceiver is configured to provide a root certificate authority (CA) certificate of the

TSP to the server of the manufacturer during the secure certificate exchange for storage on the electronic device and verification of the TSP.

Claim 20. (Canceled)

Examiner's Reasons for Allowance

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

Independent claim 1 is patentable over the cited prior arts because they do not anticipate nor fairly and reasonably teach independently or in combination a method comprising besides other limitations: generating, by the device, a device signing certificate and a device signing public private key pair, and a device encryption certificate and a device encryption public private key pair, each of the device signing and encryption certificates signed using a device unique private key that is pre-stored on the electronic device; and identifying, by the device a TSP signing public key and a TSP encryption public key of the TSP server based on the received TSP signing and the received TSP encryption certificates; and transmitting a message including a signature of the electronic device based on the device signing private key, wherein the device unique private key is stored on the electronic device by the manufacturer for access by a trusted application of the electronic device and wherein the information includes information for registering payment information with the TSP.

Independent claim 8 is patentable over the cited prior arts because they do not anticipate nor fairly and reasonably teach independently or in combination a device comprising besides other limitations: at least one hardware processor configured to generate a device signing certificate and a device signing public private key pair, and to generate a device encryption certificate and a device encryption public private key pair, the device signing and encryption certificates signed using a

device unique private key that is pre-stored on the electronic device; and wherein the processor is further configured to identify a TSP signing public key and a TSP encryption public key of the TSP server based on the received TSP signing and encryption certificates, and wherein the transceiver is configured to transmit a message including a signature of the electronic device based on the device signing private key, and wherein the device unique private key is stored on the electronic device by the manufacturer for access by a trusted application of the electronic device and wherein the information includes information for registering payment information with the TSP..

Independent claim 15 is patentable over the cited prior arts because they do not anticipate nor fairly and reasonably teach independently or in combination a system comprising besides other limitations: a TSP server comprising: at least one hardware processor configured to generate a TSP signing certificate and a TSP signing public private key pair, and a TSP encryption certificate and a TSP encryption public private key pair, the TSP signing and TSP encryption certificates signed using a TSP root certificate authority (CA) private key; and wherein the processor is further configured to verify an authenticity of the device signing and device encryption certificates based on a public key for a root CA private key of a manufacturer of the electronic device, and wherein the device unique private key is stored on the electronic device by the manufacturer for access by a trusted application of the electronic device and wherein the information includes information for registering payment information with the TSP.

Response to Arguments

5. Applicant's arguments, see remarks filed on 04/11/2018, with respect to 35 USC 101 type rejections of claims 15-20 are fully considered. Previous 35 USC 101 type rejections are withdrawn based on applicant's arguments and because of further amendments are made to the

independent claim 15 through examiner's amendments presented in this office action.

Applicant's arguments, see remarks filed on 04/11/2018, with respect to 35 USC 103 type rejections of claims 1-5, 7-12, 14-18 and 20 have been fully considered and are persuasive. The previous 35 USC 103 type rejections of claims 1-5, 7-12, 14-18 and 20 have been withdrawn based on applicant's arguments and because of further amendments are made to the independent claims through examiner's amendments presented in this office action. Applicant's arguments, see remarks filed on 04/11/2018, with respect to 35 USC 103 type rejections of claims 6, 13 and 19 have been fully considered and are persuasive. The previous 35 USC 103 type rejections of claims 6, 13 and 19 have been withdrawn.

Conclusion

6. Claims 1-4, 6, 8-11, 13, 15-17 and 19 are patentable.

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

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHANTO ABEDIN whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 10:00 AM to 6:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jay Kim, can be reached on 571-272-3804. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/SHANTO ABEDIN/

Primary Examiner, Art Unit 2494

<i>Examiner-Initiated Interview Summary</i>	Application No.	Applicant(s)	
	15/054,020	Liu et al.	
	Examiner	Art Unit	AIA Status
	SHANTO ABEDIN	2494	Yes

All participants (applicant, applicant's representative, PTO personnel):

(1) SHANTO ABEDIN. (3) _____.

(2) MICHAEL RODRIGUEZ (Reg No. 60,236). (4) _____.

Date of Interview: 26 July 2018.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.

If Yes, brief description: _____.

Issues Discussed ☐ 101 ☐ 112 ☐ 102 ☐ 103 ☒ Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: 1.

Identification of prior art discussed: NONE.

Substance of Interview

(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant's representative was contacted by the examiner regarding proposed examiner's amendments to the independent claims in order to place the application in condition for allowance. An agreement was reached regarding the proposed examiner's amendments..

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/SHANTO ABEDIN/
Primary Examiner, Art Unit 2494



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.
15/054,020	01/29/2019	10193700	MPS15-SP02	6551

106809 7590 01/09/2019
Docket Clerk - SAMS
P.O. Drawer 800889
Dallas, TX 75380

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 156 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

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

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

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

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

Samsung Electronics Co., Ltd, Suwon-si, KOREA, REPUBLIC OF;
An Liu, Mountain View, CA;
Balakrishna Venkataram, Mountain View, CA;
Pai Peng, Mountain View, CA;
Bulent Kasman, Mountain View, CA;
Kunal Patel, Mountain View, CA;

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.