

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A SUBMISSION UNDER 35 U.S.C. 371		Attorney Docket No. P41624US
International Application No. PCT/US2011/065069		U.S. Application No. (if known, see 37 CFR 1.5) New Application
International Filing Date December 15, 2011		Priority Date Claimed December 15, 2011
Title of Invention METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE		
First Named Inventor Hormuzd M. Khosravi		
Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information. 1. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). NOTE: The express request under 35 U.S.C. 371(f) will not be effective unless the requirements under 35 U.S.C. 371(c)(1), (2), and (4) for payment of the basic national fee, copy of the International Application and English translation thereof (if required), and the oath or declaration of the inventor(s) have been received. 2. ☒ A copy of the International Application (35 U.S.C. 371(c)(2)) is attached hereto (not required if the International Application was previously communicated by the International Bureau or was filed in the United States Receiving Office (RO/US)). 3. An English language translation of the International Application (35 U.S.C. 371(c)(2)) a. ☒ is attached hereto. b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4). 4. An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)) a. ☐ is attached. b. ☐ was previously filed in the international phase under PCT Rule 4.17(iv). Items 5 to 8 below concern amendments made in the international phase. <u>PCT Article 19 and 34 amendments</u> 5. ☐ Amendments to the claims under PCT Article 19 are attached (not required if communicated by the International Bureau) (35 U.S.C. 371(c)(3)). 6. ☐ English translation of the PCT Article 19 amendment is attached (35 U.S.C. 371(c)(3)). 7. ☐ English translation of annexes (Article 19 and/or 34 amendments only) of the International Preliminary Examination Report is attached (35 U.S.C. 371(c)(5)). <u>Cancellation of amendments made in the international phase</u> 8a. ☐ Do not enter the amendment made in the international phase under PCT Article 19. 8b. ☐ Do not enter the amendment made in the international phase under PCT Article 34. NOTE: A proper amendment made in English under Article 19 or 34 will be entered in the U.S. national phase application absent a clear instruction from applicant not to enter the amendment(s). The following items 9 to 17 concern a document(s) or information included. 9. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98. 10. ☒ A preliminary amendment. 11. ☒ An Application Data Sheet under 37 CFR 1.76. 12. ☐ A substitute specification. NOTE: A substitute specification cannot include claims. See 37 CFR 1.125(b). 13. ☐ A power of attorney and/or change of address letter. 14. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.3 and 37 CFR 1.821-1.825. 15. ☐ Assignment papers (<i>cover sheet and document(s)</i>). Name of Assignee: _____ 16. ☐ 37 CFR 3.73(c) Statement (<i>when there is an Assignee</i>). _____		

This collection of information is required by 37 CFR 1.414 and 1.491-1.492. The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 15 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

U.S. APPLN. No. (if known – see 37 CFR 1.5) New Application	INTERNATIONAL APPLICATION No. PCT/US2011/065069	ATTORNEY DOCKET No. P41624US
17. ☒ Other items or information: International Search Report and Written Opinion		
The following fees have been submitted.		CALCULATIONS PTO USE ONLY
18. ☒ Basic national fee (37 CFR 1.492(a)) \$280		\$ 280
19. ☒ Examination fee (37 CFR 1.492(c)) If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4) \$0 All other situations \$720		720 \$
20. ☒ Search fee (37 CFR 1.492(b)) If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4) \$0 Search fee (37 CFR 1.445(a)(2)) has been paid on the international application to the USPTO as an International Searching Authority \$120 International Search Report prepared by an ISA other than the US and provided to the Office or previously communicated to the US by the IB \$480 All other situations \$600		480 \$
TOTAL OF 18, 19, and 20 =		\$ 1480
☐ Additional fee for specification and drawings filed in paper over 100 sheets (excluding sequence listing in compliance with 37 CFR 1.821(c) or (e) in an electronic medium or computer program listing in an electronic medium) (37 CFR 1.492(j)). Fee for each additional 50 sheets of paper or fraction thereof \$400		
Total Sheets	Extra Sheets	
- 100 =	/ 50 =	
		x \$400
		\$
Surcharge of \$140.00 for furnishing any of the search fee, examination fee, or the oath or declaration after the date of commencement of the national stage (37 CFR 1.492(h)).		\$
CLAIMS	NUMBER FILED	NUMBER EXTRA
Total claims	24 - 20 =	4
Independent claims	3 - 3 =	
		x \$80
		\$ 320
		\$
MULTIPLE DEPENDENT CLAIM(S) (if applicable)		+ \$780
		\$
Processing fee of \$140.00 for furnishing the English translation later than 30 months from the earliest claimed priority date (37 CFR 1.492(i)).		\$
TOTAL OF ABOVE CALCULATIONS =		\$ 320
☐ Applicant asserts small entity status. See 37 CFR 1.27. Fees above are reduced by ½.		
☐ Applicant certifies micro entity status. See 37 CFR 1.29. Fees above are reduced by ¾. Applicant must attach form PTO/SB/15A or B or equivalent.		
TOTAL NATIONAL FEE =		\$ 1800
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). \$40.00 per property.		\$
TOTAL FEES ENCLOSED =		\$ 1800
		Amount to be refunded:
		\$
		Amount to be charged:
		\$

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.

a. ☐ A check in the amount of \$ _____ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. 504238 in the amount of \$ 1800 to cover the above fees.

c. ☒ The Director is hereby authorized to charge additional fees which may be required, or credit any overpayment, to Deposit Account No. 504238 as follows:

i. ☒ any required fee.

ii. ☐ any required fee except for excess claims fees required under 37 CFR 1.492(d) and (e) and multiple dependent claim fee required under 37 CFR 1.492(f).

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038. The PTO-2038 should only be mailed or faxed to the USPTO. However, when paying the basic national fee, the PTO-2038 may NOT be faxed to the USPTO.

ADVISORY: If filing by EFS-Web, do **NOT** attach the PTO-2038 form as a PDF along with your EFS-Web submission. Please be advised that this is **not** recommended and by doing so your **credit card information may be displayed via PAIR**. To protect your information, it is recommended to pay fees online by using the electronic payment method.

NOTE: Where an appropriate time limit under 37 CFR 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the International Application to pending status.

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

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013, and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.

NOTE: A U.S. national stage application may not claim priority to the international application of which it is the national phase. The filing date of a U.S. national stage application is the international filing date. See 35 U.S.C. 363.

Correspondence Address

☒ The address associated with Customer Number: 73466 OR ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country				Telephone	
Email					

Signature	/Glen M. Kellett, Reg No. 60202/	Date	June 19, 2013	
Name (Print/Type)	Glen M. Kellett	Registration No. (Attorney/Agent)	60,202	

Privacy Act Statement

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

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

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

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No. : TBD
Applicant : Hormuzd M. Khosravi et al.
International Filing Date : December 15, 2011
TC/A.U. : TBD
Examiner : TBD

Docket No. : P41624US
Customer No. : 73486

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

PRELIMINARY AMENDMENT

SIR:

Please consider the above-identified application (the “Patent Application”) in view of the following preliminary amendments and remarks.

Amendments to the Claims are reflected in the listing of claims, which begins on page 2 of this paper.

Remarks/Arguments begin on page 9 of this paper.

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

Claims 1-47 (Canceled)

48. (New) A system-on-a-chip apparatus comprising:

a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, the security engine to:

generate a random nonce for initiating a request for a secure communication session with a server over a network using the nonce;

perform a cryptographic key exchange with the server to generate a symmetric session key to encrypt messages sent to the server and decrypt messages received from the server during the secure communication session;

store the session key in the secure memory,

the system-on-a-chip to establish the secure communication session with the server over the network using the session key.

49. (New) The system-on-a-chip apparatus of claim 48, wherein the security engine to receive a server nonce from the server in response to the request for the secure communication session, the response message including a server nonce and store the server nonce in the secure memory.

50. (New) The system-on-a-chip apparatus of claim 48, wherein the security engine to generate a pre-master key, encrypt the pre-master key using a security key of the security engine, and send the encrypted pre-master key to the server.

51. (New) The system-on-a-chip apparatus of claim 50, wherein the security engine to wrap the pre-master key using a server public key and store the wrapped pre-master key in the secure storage.

52. (New) The system-on-a-chip apparatus of claim 50, wherein the security engine to:

generate the session key as a function of the pre-master key; and

calculate a hash function as a function of the random nonce generated by the security engine and a nonce received from the server.

53. (New) The system-on-a-chip apparatus of claim 48, wherein the security engine to generate a public Diffie-Hellman client key and a private Diffie-Hellman client key, sign the public Diffie-Hellman client key using a security key of the security engine, and send the signed public Diffie-Hellman key to the server.

54. (New) The system-on-a-chip apparatus of claim 53, wherein the security engine to receive a public Diffie-Hellman server key from the server and generate the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

55. (New) The system-on-a-chip apparatus of claim 48, wherein the security engine to receive Diffie-Hellman global values and a public Diffie-Hellman server key from the server and store at least one of the Diffie-Hellman global values and the public Diffie-Hellman server key in the secure storage.

56. (New) A method comprising:

generating a random nonce in a security engine of a system-on-a-chip of a client device;

initiating, using the client device, a request for a secure communication session with a server over a network, the request including the random nonce;

performing a cryptographic key exchange, using the security engine of the system-on-a-chip, with the server to generate a symmetric session key to encrypt messages sent to the server and decrypt messages received from the server during the secure communication session;

storing the session key in a secure memory of the security engine of the system-on-a-chip; and

establishing, using the client device, the secure communication session with the server using the session key.

57. (New) The method of claim 56, wherein initiating a request for a secure communication session comprises sending a ClientHello message, including the nonce, to the server; and further comprising:

receiving a ServerHello message from the server, the ServerHello message including a server nonce; and

storing the server nonce in the secure memory of the security engine of the system-on-a-chip.

58. (New) The method of claim 56, wherein performing the cryptographic key exchange with the server comprises:

generating a pre-master key in the security engine;

encrypting the pre-master key using a security key of the security engine;

and

sending the encrypted pre-master key to the server.

59. (New) The method of claim 58, further comprising:

wrapping the pre-master key in the security engine of the system-on-a-chip using a server public key, and

storing the wrapped pre-master key in the secure storage of the security engine of the system-on-a-chip.

60. (New) The method of claim 58, wherein performing the cryptographic key exchange with the server comprises generating the session key in the security engine of the system-on-a-chip as a function of the pre-master key.

61. (New) The method of claim 60, wherein generating the session key in the security engine comprises calculating, using the security engine of the system-on-a-chip, a hash function as a function of the random nonce generated by the security engine and a nonce received from the server.

62. (New) The method of claim 56, wherein performing the cryptographic key exchange with the server comprises:

generating, in the security engine of the system-on-a-chip, a public Diffie-Hellman client key and a private Diffie-Hellman client key;

signing the public Diffie-Hellman client key using a security key of the security engine of the system-on-a-chip;

sending the signed public Diffie-Hellman key to the server;

receiving a public Diffie-Hellman server key from the server; and

generating, in the security engine of the system-on-a-chip, the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

63. (New) The method of claim 56, further comprising:

generating, in the security engine of the system-on-a-chip, a hash code of a preceding message sent from the client to the server;

signing the hash code using a security key stored in a secure memory of the security engine; and

sending a client certificate verification message to the server, the client certificate verification message including the signed hash code.

64. (New) One or more machine-readable storage media comprising a plurality of instructions stored thereon that, in response to execution by a computing device, cause the computing device to:

generate a random nonce in a security engine of a system-on-a-chip of the computing device;

initiate a request for a secure communication session with a server over a network, the request including the random nonce;

perform a cryptographic key exchange, using the security engine of the system-on-a-chip, with the server to generate a symmetric session key to encrypt messages sent to the server and decrypt messages received from the server during the secure communication session;

store the session key in a secure memory of the security engine of the system-on-a-chip; and

establish the secure communication session with the server using the session key.

65. (New) The one or more machine-readable storage media of claim 64, wherein to initiate a request for a secure communication session comprises to send a ClientHello message, including the nonce, to the server; and wherein the plurality of instructions further cause the computing device to:

receive a ServerHello message from the server, the ServerHello message including a server nonce; and

store the server nonce in the secure memory of the security engine of the system-on-a-chip.

66. (New) The one or more machine-readable storage media of claim 64, wherein to perform the cryptographic key exchange with the server comprises to:

generate a pre-master key in the security engine;

encrypt the pre-master key using a security key of the security engine; and

send the encrypted pre-master key to the server.

67. (New) The one or more machine-readable storage media of claim 66, wherein the plurality of instructions further cause the computing device to:

wrap the pre-master key in the security engine of the system-on-a-chip with a server public key, and

store the wrapped pre-master key in the secure storage of the security engine of the system-on-a-chip.

68. (New) The one or more machine-readable storage media of claim 66, wherein to perform the cryptographic key exchange with the server comprises to generate the session key in the security engine of the system-on-a-chip as a function of the pre-master key.

69. (New) The one or more machine-readable storage media of claim 68, wherein to generate the session key in the security engine comprises to calculate, using the security engine of the system-on-a-chip, a hash function as a function of the random nonce generated by the security engine and a nonce received from the server.

70. (New) The one or more machine-readable storage media of claim 64, wherein to perform the cryptographic key exchange with the server comprises to:

generate, in the security engine of the system-on-a-chip, a public Diffie-Hellman client key and a private Diffie-Hellman client key;

sign the public Diffie-Hellman client key using a security key of the security engine of the system-on-a-chip;

send the signed public Diffie-Hellman key to the server;

receive a public Diffie-Hellman server key from the server; and

generate, in the security engine of the system-on-a-chip, the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

71. (New) The one or more machine-readable storage media of claim 64, wherein the plurality of instructions further cause the computing device to:

- generate, in the security engine of the system-on-a-chip, a hash code of a preceding message sent from the client to the server;
- sign the hash code using a security key stored in a secure memory of the security engine; and
- send a client certificate verification message to the server, the client certificate verification message including the signed hash code.

Appl. No. TBD
Preliminary Amendment Dated June 20, 2013

Docket No.: P41624US
Examiner: TBD
TC/A.U. TBD

REMARKS

These amendments and remarks are set forth prior to examination. Claims 1-47 have been cancelled. Claims 48-71 new claims have been added. Favorable consideration and allowance of the pending claims are respectfully requested.

Appl. No. TBD
Preliminary Amendment Dated June 20, 2013

Docket No.: P41624US
Examiner: TBD
TC/A.U. TBD

Conclusion

Applicant respectfully submits that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney (317) 261-7959 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 50-4238.

Respectfully submitted,
Barnes & Thornburg LLP
CUSTOMER NO. 73486

Date: June 20, 2013

/Glen M. Kellett, Reg No. 60202/
Glen M. Kellett
Registration No. 60,202
Barnes & Thornburg LLP
11 South Meridian Street
Indianapolis, Indiana 46204-3535
Telephone: (317) 261-7959
Fax: (317) 231-7433

**METHOD AND DEVICE FOR SECURE COMMUNICATIONS
OVER A NETWORK USING A HARDWARE SECURITY ENGINE**

BACKGROUND

5 Cryptographic communication protocols are used to establish a secure communication session between computing devices over an untrusted network or communication link. One commonly used cryptographic communication protocol is the Secure Sockets Layer (SSL) protocol. The SSL protocol, and the related Transport Layer Security (TLS) protocol, is used for many different types of secure communication sessions including, for example, secure web-browsing, ecommerce, secure upgrades, and other secure communication sessions between two computing devices on an untrusted network such as the Internet. Other communication protocols may utilize the SSL/TLS protocol to provide the underlying security. For example, the Hypertext Transfer Protocol Secure (HTTPS) uses SSL/TLS for encryption of messages between devices. Typically, the cryptographic security offered by the SSL/TLS protocols is done so in-band and performed at the software application level.

10 Some computing and electronic devices utilize system-on-a-chip (SOC) designs due to their relatively small footprint. SOC devices are integrated circuits that incorporate various components, in addition to the processing core, of electronic systems on a single die. For example, an SOC may include a processor core, memory controller, video components, audio components, and/or communication components on a single chip.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention described herein is illustrated by way of example and not by way of limitation in the accompanying figures. For simplicity and clarity of illustration, elements illustrated in the figures are not necessarily drawn to scale. For example, the dimensions of some elements may be exaggerated relative to other elements for clarity. Further, where considered appropriate, reference labels have been repeated among the figures to indicate corresponding or analogous elements.

25 FIG. 1 is a simplified block diagram of at least one embodiment of a system for establishing a secure communication session between a client device having a system-on-a-chip (SOC) and a server over a network;

30 FIG. 2 is a block diagram of at least one embodiment of a security scheme for the system of FIG. 1;

FIG. 3 is a simplified sequence diagram of at least one embodiment of a communication sequence of the client device and server of FIG. 1 to establish a secure communication session; and

5 FIG. 4 is a simplified flow diagram of at least one embodiment of a method for establishing a secure communication session executed by the client device of FIG. 1.

DETAILED DESCRIPTION OF THE DRAWINGS

While the concepts of the present disclosure are susceptible to various modifications and alternative forms, specific exemplary embodiments thereof have been shown by way of example in the drawings and will herein be described in detail. It should be understood,
10 however, that there is no intent to limit the concepts of the present disclosure to the particular forms disclosed, but on the contrary, the intention is to cover all modifications, equivalents, and alternatives consistent with the present disclosure and the appended claims.

In the following description, numerous specific details such as logic implementations,
15 opcodes, means to specify operands, resource partitioning/sharing/duplication implementations, types and interrelationships of system components, and logic partitioning/integration choices are set forth in order to provide a more thorough understanding of the present disclosure. It will be appreciated, however, by one skilled in the art that embodiments of the disclosure may be practiced without such specific details.

20 In other instances, control structures, gate level circuits and full software instruction sequences have not been shown in detail in order not to obscure the invention. Those of ordinary skill in the art, with the included descriptions, will be able to implement appropriate functionality without undue experimentation.

References in the specification to “one embodiment,” “an embodiment,” “an example embodiment,” etc., indicate that the embodiment described may include a particular
25 feature, structure, or characteristic, but every embodiment may not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is
30 within the knowledge of one skilled in the art to effect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described.

Embodiments of the invention may be implemented in hardware, firmware, software, or any combination thereof. Embodiments of the invention implemented in a computer

system may include one or more bus-based interconnects between components and/or one or more point-to-point interconnects between components. Embodiments of the invention may also be implemented as instructions carried by or stored on a machine-readable medium, which may be read and executed by one or more processors. A machine-readable
5 medium may be embodied as any device, mechanism, or physical structure for storing or transmitting information in a form readable by a machine (e.g., a computing device). For example, a machine-readable medium may be embodied as read only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices; mini- or micro-SD cards, memory sticks, electrical signals, and others.

10 In the drawings, specific arrangements or orderings of schematic elements, such as those representing devices, modules, instruction blocks and data elements, may be shown for ease of description. However, it should be understood by those skilled in the art that the specific ordering or arrangement of the schematic elements in the drawings is not meant to imply that a particular order or sequence of processing, or separation of processes, is
15 required. Further, the inclusion of a schematic element in a drawing is not meant to imply that such element is required in all embodiments or that the features represented by such element may not be included in or combined with other elements in some embodiments.

In general, schematic elements used to represent instruction blocks may be implemented using any suitable form of machine-readable instruction, such as software or firmware
20 applications, programs, functions, modules, routines, processes, procedures, plug-ins, applets, widgets, code fragments and/or others, and that each such instruction may be implemented using any suitable programming language, library, application programming interface (API), and/or other software development tools. For example, some embodiments may be implemented using Java, C++, and/or other programming languages.

25 Similarly, schematic elements used to represent data or information may be implemented using any suitable electronic arrangement or structure, such as a register, data store, table, record, array, index, hash, map, tree, list, graph, file (of any file type), folder, directory, database, and/or others.

30 Further, in the drawings, where connecting elements, such as solid or dashed lines or arrows, are used to illustrate a connection, relationship or association between or among two or more other schematic elements, the absence of any such connecting elements is not meant to imply that no connection, relationship or association can exist. In other words, some connections, relationships or associations between elements may not be shown in the drawings so as not to obscure the disclosure. In addition, for ease of illustration, a single

connecting element may be used to represent multiple connections, relationships or associations between elements. For example, where a connecting element represents a communication of signals, data or instructions, it should be understood by those skilled in the art that such element may represent one or multiple signal paths (e.g., a bus), as may be needed, to effect the communication.

Referring now to FIG. 1, a system 100 for establishing a secure communication session includes a client device 102, a server 104, and a network 106. In operation, the client device 102 initiates a request for a secure communication session with the server 104 over the network 106. To establish the secure communication session, the client device 102 and the server 104 perform a cryptographic key exchange, such as a Diffie-Hellman or a Rivest-Shamir-Adleman (RSA) key exchange, to generate a secret symmetric session key. The secret symmetric session key may then be used to encrypt and decrypt messages between the client device 102 and the server 104. To ensure a secure communication session, the various keys and other cryptographic functions generated by the client device 102 are done so within a security engine 110 of a system-on-a chip (SOC) 112 of the client device 102. The client device 102 maintains the keys in secrecy within a secure memory 114 of the security engine 110. For example, the security engine 110 may include a security key 150, as discussed below, used to sign and/or otherwise encrypt other keys and messages. In this way, the client device 102 and server 104 may establish a secure communication session across the network 106 using out-of-band (i.e., not application level), hardware security features of the client device 102. In the illustrative embodiments described herein, the secure communication session is a Secure Sockets Layer (SSL) communication session, but the system 100 and features described herein may be used to establish other types of secure communication sessions in other embodiments.

The client device 102 may be embodied as any type of computing device capable of communicating with the server 104 over the network 106. For example, the client device 102 may be embodied as a set-top box, a digital television, a smartphone, a tablet computer, a laptop computer, a mobile internet device (MID), a desktop computer, or other device capable of communicating with the server 104.

As discussed above, the client device 102 includes the SOC 112, which may be embodied as any type of system-on-a-chip device having various components and structures. In the illustrative embodiment of FIG. 1, the SOC 112 includes the security engine 110, a memory controller 116, a processor core 118, and a plurality of hardware peripherals 130, which are communicatively coupled to each other via a link 120. The link 120 may be

embodied as any type of interconnect such as a bus, point-to-point, or other interconnect capable of facilitating communication between the various components of the SOC 112. The hardware peripherals 130 may include any type of hardware peripheral component depending upon the intended functionality of the SOC 112. For example, in the illustrative embodiment, the hardware peripherals 130 include a demux 132 to separate audio and video content streams, video processing component(s) 134 to process video content, and audio processing component(s) 136 to process audio content. Of course, it should be appreciated that the hardware peripherals 130 of the SOC 112 have been simplified in the illustrative embodiment of FIG. 1 and that the SOC 112 may include additional, different, and/or greater detailed hardware peripherals 130, which are not illustrated in FIG. 1 for clarity of the disclosure.

The security engine 110 may be embodied as a security co-processor or processing circuitry separate from the processor core 118. The security engine 110 includes the security key 150 and the secure memory 114, which is accessible only by the security engine 110. The security engine 110 stores the security key 150, and other cryptographic keys as discussed below, in the secure memory 114. In the illustrative embodiment, the security key 150 is provisioned during the manufacturing of the SOC 112, but may be generated by the SOC 112 during operation in other embodiments. For example, in some embodiments, the security key 150 is based on blown fuses within the security engine 110 itself. Additionally or alternatively, the security engine 110 may include a key-generating module, such as a trusted platform module (TPM), to generate the security key 150. During use, the security engine 110 may use any number of security keys 150, which may be identical or different from each other.

In some embodiments, the client device 102 may include additional components and structures other than the SOC 112 depending on the type and intended use of the client device 102. For example, in the illustrative embodiment of FIG. 1, the client device 102 includes a system memory 160, a data storage 162, a communications output 164, and one or more input/output devices 166. The system memory 160 may be embodied as any type of main memory or data storage locations including, for example, dynamic random access memory devices (DRAM), synchronous dynamic random access memory devices (SDRAM), double-data rate synchronous dynamic random access memory device (DDR SDRAM), mask read-only memory (ROM) devices, erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM) devices, flash memory devices, and/or other volatile and/or non-volatile memory devices.

The data storage 162 may be embodied as any type of device or devices configured for the short-term or long-term storage of data such as, for example, memory devices and circuits, memory cards, hard disk drives, solid-state drives, or other data storage devices. The communications output 164 may be embodied as a simplified output or as various circuits and/or devices to facilitate, for example, communications with the server 104. For example, the communications output 164 (and/or communication circuitry within the SOC 112) may use any suitable communication protocol such as Ethernet (i.e. the IEEE 802.3 standard) or Wi-Fi® (i.e., the IEEE 802.11 standard), and/or other communication protocols or standards. Additionally, the input/output devices 166 may be embodied as any type of I/O device for interacting with the client device 102. For example, the I/O devices 166 may include output devices such as a display for displaying data on the client device 102, speakers for generating audio, and/or input devices such as a remote control receiver, a keyboard, a mouse, and/or the like.

The server 104 may be embodied as any type of data server capable of establishing a secure communication session with the client device 102. As such, the server 104 may include various hardware and software components typically found in a server for communicating, maintaining, and transferring data over a network. For example, the illustrative server 104 includes a processor 180, a memory 182, and communication circuitry 184, which may be similar to such components found in other data servers. For example, the processor 180 may be embodied as any type of processor capable of executing software/firmware, such as a microprocessor, digital signal processor, microcontroller, or the like, and may include one or more processing cores. The memory 182 may be embodied as any type of memory or data storage locations including, for example, dynamic random access memory devices (DRAM), synchronous dynamic random access memory devices (SDRAM), double-data rate synchronous dynamic random access memory device (DDR SDRAM), mask read-only memory (ROM) devices, erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM) devices, flash memory devices, and/or other volatile and/or non-volatile memory devices. The communication circuitry 184 may be embodied any type of circuitry and/or device to facilitate, for example, communications with the client device 102. For example, the communication circuitry 184 may support communication protocols such as Ethernet (i.e. the IEEE 802.3 standard) and/or Wi-Fi® (i.e., the IEEE 802.11 standard), and/or other communication protocols or standards.

The network 106 may be embodied as any number of various wired and/or wireless networks. For example, the network 106 may be embodied as or otherwise include a local area network (LAN), a wide area network (WAN), and/or a publicly accessible, global network such as the Internet. Additionally, the network 106 may include any number of additional devices to facilitate communication between the client device 102 and the server 104. As discussed above, in the illustrative embodiment, the client device 102 and the server 104 establish a SSL communication session over the network 106. However, other types of secure communication sessions may be established in other embodiments.

Referring now to FIG. 2, as discussed in more detail below, the use of the security engine 110 of the client device 102 to perform the cryptographic functions and store keying data associated with the establishment of the secure communication session allows the system 100 to offer several different levels of security. The particular level of security used in the system 100 may depend upon various criteria such as the nature of the network 106, the importance of the data being transferred between the client device 102 and the server 104, and/or the like. For example, one illustrative security scheme 200 includes three different levels of security as shown in FIG. 2. At level 0 security, the client device 102 is configured to protect the client private device key (i.e., the security key 150), which is used for encrypting, signing, and verification functions as discussed in more detail below.

At level 1 security, the client device 102 is configured to protect the session keys and related keys used for data encryption. For example, if an RSA key exchange is performed, the pre-master key and the master key (i.e., the session key) may be stored in the secure memory 114 of the security engine 110 of the SOC 112. Additionally, in some embodiments as discussed below, the master key may be stored in an encrypted or wrapped form (e.g., encrypted using the security key 150). In embodiments in which a Diffie-Hellman key exchange is used, the private Diffie-Hellman client key and/or shared secret key (i.e., the session key) may be stored in the secure memory 114 of the security engine 110 of the SOC 112. Again, in some embodiments, the private Diffie-Hellman client key and/or session key may be stored in an encrypted or wrapped form (e.g., encrypted using the security key 150).

Additionally, at level 2 security, the client device 102 may be configured to protect the data of the host application. For example, if the host application is being used to perform an e-commerce transaction, the bank account information used in such transaction may be encrypted using the security key 150 and stored in the secure memory 114. In this way, the bank account information is not available to the host application. Of course, it should

be appreciated that, in other embodiments, security schemes having more or fewer security levels may be used.

Referring now to FIG. 3, in operation, the client device 102 and the server 104 establish a secure communication session using the security engine 110 of the client device 102 to perform various cryptographic functions and store keying data therein. To do so, the client device 102 and server 104 may perform a handshake session as shown in the communication sequence 300 of FIG. 3. To establish the secure communication session, a security engine driver 302 of the security engine 110 communicates with a firmware of the security engine 110 and a client secure communication application 304 executed on the client device 102. The client secure communication application 304 also communicates with a corresponding server secure communication application 306 executed on the server 104.

The communication sequence 300 begins with block 310 in which the client secure communication application 304 sends a ClientHello message to the server secure communication application 306 to request the initiation of a secure communication session. As discussed above, the secure communication session is a SSL session in the illustrative embodiment. To facilitate the request, the security engine driver 302 communicates with security engine 110 of the SOC 112 to request a random nonce from the security engine 110 in block 312. The security engine 110 may use any suitable random number-generating algorithm to generate the random nonce in block 312. The nonce is embodied as random or pseudo-random number intended to be used only once in cryptographic functions to thwart, for example, replay attacked. In the illustrative embodiment, the random nonce includes a 32-bit timestamp and a 28-byte random number. Of course, other numeric formats for the random nonce may be used in other embodiments. Regardless, it should be appreciated that because the random nonce is generated in the security engine 110, the generation and storage of the random nonce is protected compared to generation of the nonce at, for example, the application level.

The random nonce generated in block 312 is included in the ClientHello message sent to the server secure communication application 306 in block 310. Additionally, the ClientHello message may include a list of cipher suites, compression methods, and other cryptographic protocols or algorithms from which the server 104 may make a selection for use in establishing the secure communication session. In response to the secure communication session request, the server secure communication application 306 sends a ServerHello message in block 314. The ServerHello message may be substantially similar

to the ClientHello message. For example, in the illustrative embodiment, the ServerHello message includes a server random nonce generated by the server 104. Additionally, the ServerHello message includes the selection(s) of the cryptographic protocols and/or other options made by the server 104 from the list included in the ClientHello message. The
5 ServerHello message completes the session initiation phase (Phase 1) of the illustrative handshake session.

In block 316, the server secure communication application 306 sends a server certificate to the client secure communication application 304. The server certificate, like the client certificate discussed below, is typically generated by a certification authority organization, which acts as a third-party verifier of the authentication of the server 104. The server
10 certificate may include unique identifier or number assigned to the server 104 by the certification authority organization to verify the server 104 to other devices on the network 106. As such, in block 318, the client device 102 may verify the server certificate. In some embodiments, the client device 102 verifies the server certificate using a public
15 certificate key issued by the certification authority organization. In such embodiments, the security engine 110 may store the public certificate key in the secure memory 114 in an unencrypted or encrypted state (e.g., using the security key 150).

To establish the secure communication session, the client device 102 and the server 104 perform a key exchange to establish a shared secret key (i.e., a master or session key) in
20 each of the client device 102 and server 104. The client device 102 and the server 104 may use any appropriate key exchange algorithm to effect the establishment of the shared secret. In the illustrative embodiment, the key exchange may be embodied as an RSA key exchange or a Diffie-Hellman key exchange. In embodiments wherein a RSA key exchange is used, the server secure communication application 306 performs a server RSA
25 key exchange in block 320. In such embodiments, the server 104 may generate a temporary RSA public/private key pair and send the RSA public key to the client device 102 in block 320. Such message may be signed by the server 104 and verified by the client device 102 using a public server key, which may be stored in the secure memory 114 as discussed above.

Alternatively, the server secure communication application 306 may perform a server
30 Diffie-Hellman key exchange in block 320. In such embodiments, the server 104 selects or otherwise generates the Diffie-Hellman global values (e.g., a prime number and a primitive root of the prime number), generates a private and public Diffie-Hellman server key, and sends the Diffie-Hellman global values and public Diffie-Hellman server key to the client

device 102 in block 320. Again, such message may be signed by the server 104 and verified by the client device 102 using a public server key.

In some embodiments, the sever secure communication application 306 may send a client certification request in block 322. If so, the request may specify the types of certificates accepted by the server 104 (e.g., the public key algorithm used), acceptable certificate authorities, and/or other certificate parameters. Subsequently, in block 324, the server secure communication application 306 sends a server completion message (a "ServerHelloDone" message) to the client secure communication application 304 to indicate that the server 104 has completed this phase of the handshake session. In the illustrative embodiment, no parameters or other data are required for the server completion message. The ServerHelloDone message completes the server authentication and key exchange phase (Phase 2) of the illustrative handshake session.

After receiving the server completion message, the client secure communication application 304 initiates the client authentication and key exchange phase (Phase 3) of the handshake session by sending the client certificate in block 326. As discussed above, the client certificate is typically generated by the certification authority organization and may include a unique identifier or number assigned to the client device 102 by the certification authority organization to verify the client device 102 to other devices on the network 106. In some embodiments, the client certificate may be stored in the secure memory 114 of the security engine 110 of the SOC 112 in an unencrypted or encrypted state. Additionally, the client device 102 may use a private device key issued by the certification authority organization to sign the certificate prior to sending it to the server 104.

In block 328, the client secure communication application 304 performs a client key exchange. Again, the client device 102 and the server 104 may use any appropriate key exchange algorithm to effect the establishment of the shared secret as discussed above. In embodiments wherein an RSA key exchange is used, the security engine 110 of the SOC 112 of the client device 102 generates a random pre-master key in block 330. Illustratively, the pre-master key is embodied as a 48-byte random number, but other numeric formats may be used in other embodiments. In block 332, the pre-master key generated in block 330 is encrypted or otherwise wrapped using the server public key provided by the server in server authentication and key exchange phase (Phase 2). The encrypted pre-master key may be stored in the secure memory 114 of the security engine 110 of the SOC 112 and sent to the server 104 in block 328.

Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 generates, in block 334, a private Diffie-Hellman client key and a public Diffie-Hellman client key using the Diffie-Hellman global values received from the server 104 in block 320. The private Diffie-Hellman client key may be embodied as a random value generated by the security engine 110, while the public Diffie-Hellman client key is generated by the security engine 110 using the Diffie-Hellman global values received from the server 104. The private Diffie-Hellman client key may be stored in the secure memory 114 of the security engine 110. Of course, in some embodiments, the client device 102 may generate the Diffie-Hellman global values in block 334 and send such global values to the server 104 in block 328 to allow the server 104 to generate the public Diffie-Hellman server key based thereon. Regardless, in block 336, the security engine 110 of the SOC 112 signs the public Diffie-Hellman client key (and Diffie-Hellman global values if generated by the client device 102) in block 336 using the security key 150 or other private client key of the security engine 110. The signed Diffie-Hellman parameters may be further encrypted using the public server key and sent to the server 104 in block 328.

In some embodiments, the client secure communication application 304 may send a client certification verification message to the sever secure communication application 306 in block 338. To do so, the security engine 110 generates a hash code based on the preceding message and signs the hash code using the security key 150 of the security engine 110 in block 340. The client device 102 sends the signed hash code to the server 104 in block 338 as verification of the preceding message. It should be appreciated that such client certification verification messages may be used subsequent to any message sent to the server 104 from the client device 102 to provide an added level of security and verification to the secure communication session. The client certification verification message in block 338 completes the client authentication and key exchange phase (Phase 3) of the illustrative handshake session.

In block 342, the client secure communication application 304 sends a change cipher specification message to the server secure communication application 306 to inform the server 104 that subsequent communications will use the agreed-upon cipher (e.g., the generated session key). In block 344, the security engine 110 of the client device 102 generates a session key (i.e., the "master" key). In embodiments wherein an RSA key exchange is used, the security engine 110 generates the session key as a function of the pre-master key generated in block 330. To do so, the security engine 110 calculates a hash

function of the pre-master key, the client random nonce generated in block 312, and the server random nonce received in block 314. Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 generates the session key as a function of the Diffie-Hellman global values, the public Diffie-Hellman server key, and the private Diffie-Hellman client key. As discussed above, the session key is stored in the secure memory 114 of the security engine 110.

In block 346, the security engine 110 generates a hash code of the session key, which may include additional padding depending on the type of hash function used. The hash code of the session key is sent to the server 104 for verification in a client-finished message in block 348. The hash code of the session key may be encrypted by the security engine 110 using the public server key as discussed above.

In response to the client-finished message, the server 104 sends a change cipher specification message that acknowledges the use of the agreed-upon cipher (e.g., the session key) in block 350. The server 104 also sends a server-finished message in block 352 that includes a similar hash code of the session key for verification by the client device 102. Assuming that the client device 102 and the server 104 verify the hash code of the session key, the handshake session is complete and each of the client device 102 and server 104 have a shared secret session key that is used to encrypt and decrypt subsequent messages. Again, it should be appreciated that the security engine 110 of the SOC 112 of the client device 102 is used for all cryptographic functions and storage of sensitive keying data to provide hardware-based protection of the cryptographic keys and certificate keys used during the communication sequence 300.

Referring now to FIG. 4, in use, the client device 102 may execute a method 400 to establish a secure communication session with the server 104. The method 400 begins with block 402 in which the security engine 110 of the SOC 112 of the client device 102 is provisioned. To do so, in one embodiment, the security engine 110 receives a client device certificate, a private client device key, and a public certification key. The client device certificate, the private client device key, and the public certification key are typically generated by the certification authority organization, which acts as a third-party verifier of the authentication of the client device 102 as discussed above. The client device certificate may include a unique device identifier or number assigned to the client device 102 by the certification authority organization to verify the client device 102 to other devices on the network 106. The private client device key may be used by the client device 102 to sign the client device certificate so as to authenticate the client device 102 to other devices as

discussed in more detail below. Conversely, the public certification key may be used by the client device 102 to verify certification of other devices on the network 106 by the certification authority organization.

5 The security engine 110 encrypts the private client device key using the security key 150 and stores the encrypted private client device key in the secure memory 114. The security engine 110 may also store the client device certificate and/or the public certification key in the secure memory 114. Additionally, in some embodiments, the security engine 110 may encrypt the client device certificate and/or the public certification key using the security key 150 stored in the security engine 110.

10 After the security engine 110 has been provisioned in block 402, the client device 102 determines whether to establish a secure communication session (e.g., an SSL session) with the server 104 in block 404. If so, in block 406, the security engine 110 generates a random nonce value. As discussed above, the security engine 110 may use any suitable random number-generating algorithm to generate the random nonce. In block 408, the client device 102 sends a request (a ClientHello message) to initiate the secure communication session to the server 104. The request includes the random nonce generated in block 406 along with a list of cipher protocols, compression methods, and/or other cryptographic choices from which the server 104 may select.

20 In block 410, the client device 102 completes the server authentication and server key exchange. In so doing, the client device 102 may receive a corresponding ServerHello message including a server random nonce, the server's 104 public key, and the server's 104 selection of cryptographic choices presented in the ClientHello message. As discussed above, the server random nonce, along with the client random nonce, is used to generate the session key. As such, the security engine 110 may store the server random nonce in the secure memory 114. Additionally, in some embodiments, the security engine 110 may store the server certificate and/or other keying data in the secure memory 114. For example, in embodiments wherein an RSA key exchange is used, the security engine 110 may store the public RSA key received from the server in the secure memory 114. Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 may store the Diffie-Hellman global values and/or public Diffie-Hellman server key in the secure memory 114.

30 In block 414, the client 104 determines whether the server 104 is successfully authenticated. If not, the method 400 loops back to block 404 in which the client device 102 may reattempt to establish a secure communication session with the server 104.

However, if the server 104 is successfully authenticated, the method 400 advances to block 416 in which the client device 102 sends the server 104 the client certificate. If the client certificate has been encrypted (e.g., using the secure key 150), the security engine 110 decrypts the client certificate and signs the client certificate using the private client device key.

In block 418, the client 104 completes the client key exchange using the security engine 110 to maintain the security of the keying functions. For example, if a RSA key exchange was selected, the security engine 110 generates the pre-master key and encrypts the pre-master key using the server public key received in block 410 prior to sending the encrypted pre-master key to the server 104 in block 420. Alternatively, if a Diffie-Hellman key exchange was selected, the security engine 110 generates the public and private Diffie-Hellman client keys using the Diffie-Hellman global values received from the server 104 in block 410. The security engine 110 may sign the public Diffie-Hellman client key using the security key 150 or the public client device key provisioned in block 402. The client device 102 sends the signed public Diffie-Hellman client key to the server 104 in block 422. The keys and related keying data generated during the client key exchange may be stored in the secure memory 114 in an encrypted state (using the security key 150) or an unencrypted state.

In block 424, the client device 102 determines whether the client device 102 has been successfully authenticated by the server 104. If not, the method 400 loops back to block 404 in which the client device 102 may reattempt to establish a secure communication session with the server 104. However, if the client device 102 is successfully authenticated, the method 400 advances to block 426 in which the client device 102 confirms the cipher suite with the server 104 by informing the server 104 that subsequent messages will use the agreed-upon cryptographic protocols. In so doing, the security engine 110 may generate the master or session key. To do so, in embodiments wherein an RSA key exchange is used, the security engine 110 calculates a hash function of the pre-master key, the client random nonce generated in block 406, and the server random nonce received in block 410. Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 generates the session key as a function of the Diffie-Hellman global values, the public Diffie-Hellman server key, and the private Diffie-Hellman client key. Once generated, the security engine 110 of the SOC 112 may store the session key in the secure memory 114 of the security engine 110. In some embodiments,

the session key may be encrypted using the security key 150 while stored in the secure memory 114.

5 In block 428, the security engine 110 generates a hash function of the session key, which is sent to the server 104 for verification in a client finished message. Again, the hash code of the session key may be encrypted by the security engine 110 using the public server key as discussed above. In response, the server 104 confirms the cipher suite with the client device 102 to acknowledge the agreed-upon cipher (e.g., the session key). The server 104 also sends a server finished message that includes a similar hash code of the session key for verification by the client device 102. Assuming that the client device 102 and the
10 server 104 verify the hash code of the session key, the handshake session is complete and each of the client device 102 and server 104 have a shared secret session key that is used to encrypt and decrypt subsequent messages.

While the disclosure has been illustrated and described in detail in the drawings and foregoing description, such an illustration and description is to be considered as exemplary
15 and not restrictive in character, it being understood that only illustrative embodiments have been shown and described and that all changes and modifications consistent with the disclosure and recited claims are desired to be protected.

CLAIMS:

1. A system-on-a-chip apparatus comprising:
a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, the security engine to:
5 generate a random nonce for initiating a request for a secure communication session with a server over a network using the nonce;
perform a cryptographic key exchange with the server to generate a symmetric session key to encrypt messages sent to the server and decrypt messages received from the server during the secure communication session;
10 store the session key in the secure memory,
the system-on-a-chip to establish the secure communication session with the server over the network using the session key.
2. The system-on-a-chip apparatus of claim 1, wherein the system-on-a-chip
15 to establish a Secure Sockets Layer communication session with the server over the network using the session key.
3. The system-on-a-chip apparatus of claim 1, wherein the security engine to receive a server nonce from the server in response to the request for the secure communication
20 session, the response message including a server nonce and store the server nonce in the secure memory.
- 4 The system-on-a-chip apparatus of claim 1, wherein the security engine to receive a server certificate from the server and store the server certificate in the secure memory.
25
- 5 The system-on-a-chip apparatus of claim 1, wherein the security engine to perform a Rivest-Shamir-Adleman key exchange with the server to generate the symmetric session key.
- 30 6. The system-on-a-chip apparatus of claim 5, wherein the security engine to generate a pre-master key, encrypt the pre-master key using a security key of the security engine, and send the encrypted pre-master key to the server.

7. The system-on-a-chip apparatus of claim 6, wherein the security engine to wrap the pre-master key using a server public key and store the wrapped pre-master key in the secure storage.

5 8. The system-on-a-chip apparatus of claim 6, wherein the security engine to generate the session key as a function of the pre-master key.

9. The system-on-a-chip apparatus of claim 8, wherein the security engine to calculate a hash function as a function of the random nonce generated by the security engine and
10 a nonce received from the server.

10. The system-on-a-chip apparatus of claim 5, wherein the security engine to receive a public Rivest-Shamir-Adleman server key from the server and store the public Rivest-Shamir-Adleman server key in the secure memory.

15

11. The system-on-a-chip apparatus of claim 1, wherein the security engine to perform a Diffie-Hellman key exchange with the server to generate the symmetric session key.

12. The system-on-a-chip apparatus of claim 11, wherein the security engine
20 to generate a public Diffie-Hellman client key and a private Diffie-Hellman client key, sign the public Diffie-Hellman client key using a security key of the security engine, and send the signed public Diffie-Hellman key to the server.

13. The system-on-a-chip apparatus of claim 12, wherein the security engine
25 to receive a public Diffie-Hellman server key from the server and generate the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

14. The system-on-a-chip apparatus of claim 13, wherein the security engine
to use the session key to encrypt a subsequent message sent from the client device to the server.

30

15. The system-on-a-chip apparatus of claim 11, wherein the security engine to receive Diffie-Hellman global values and a public Diffie-Hellman server key from the server and store at least one of the Diffie-Hellman global values and the public Diffie-Hellman server key in the secure storage.

16. A method comprising:
generating a random nonce in a security engine of a system-on-a-chip of a client device;
initiating, using the client device, a request for a secure communication session
5 with a server over a network, the request including the random nonce;
performing a cryptographic key exchange, using the security engine of the system-on-a-chip, with the server to generate a symmetric session key to encrypt messages sent to the server and decrypt messages received from the server during the secure communication session;
10 storing the session key in a secure memory of the security engine of the system-on-a-chip; and
establishing, using the client device, the secure communication session with the server using the session key.
17. The method of claim 16, wherein initiating a request for a secure communication session comprises initiating a request for a Secure Sockets Layer communication session.
18. The method of claim 16, further comprising:
20 receiving a response message from the server in response to the request for a secure communication session, the response message including a server nonce, and
storing the server nonce in the secure memory of the security engine of the system-on-a-chip.
19. The method of claim 16, wherein initiating a request for a secure communication session comprises sending a ClientHello message, including the nonce, to the server; and further comprising:
25 receiving a ServerHello message from the server, the ServerHello message including a server nonce; and
30 storing the server nonce in the secure memory of the security engine of the system-on-a-chip.

20. The method of claim 16, further comprising receiving a server certificate from the server and storing the server certificate in the secure memory of the security engine of the system-on-a-chip of the client device.

5 21. The method of claim 16, wherein performing the cryptographic key exchange with the server comprises performing a Rivest-Shamir-Adleman key exchange, using the security engine of the system-on-a-chip, with the server.

22. The method of claim 21, wherein performing the Rivest-Shamir-Adleman
10 key exchange with the server comprises:

generating a pre-master key in the security engine;
encrypting the pre-master key using a security key of the security engine; and
sending the encrypted pre-master key to the server.

15 23. The method of claim 22, further comprising:
wrapping the pre-master key in the security engine of the system-on-a-chip using a server public key, and
storing the wrapped pre-master key in the secure storage of the security engine of the system-on-a-chip.

20 24. The method of claim 22, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises generating the session key in the security engine of the system-on-a-chip as a function of the pre-master key.

25 25. The method of claim 24, wherein generating the session key in the security engine comprises calculating, using the security engine of the system-on-a-chip, a hash function as a function of the random nonce generated by the security engine and a nonce received from the server.

30 26. The method of claim 21, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises:
receiving a public Rivest-Shamir-Adleman server key from the server; and
storing the public Rivest-Shamir-Adleman server key in the secure memory of the security engine of the system-on-a-chip.

27. The method of claim 16, wherein performing the cryptographic key exchange with the server comprises performing a Diffie-Hellman key exchange, using the security engine of the system-on-a-chip, with the server.

5

28. The method of claim 27, wherein performing a Diffie-Hellman key exchange with the server comprises:

generating, in the security engine of the system-on-a-chip, a public Diffie-Hellman client key and a private Diffie-Hellman client key;

10 signing the public Diffie-Hellman client key using a security key of the security engine of the system-on-a-chip; and

sending the signed public Diffie-Hellman key to the server.

29. The method of claim 28, wherein performing a Diffie-Hellman key exchange with the server comprises:

15

receiving a public Diffie-Hellman server key from the server;

generating, in the security engine of the system-on-a-chip, the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

30. The method of claim 29, wherein performing a Diffie-Hellman key exchange with the server comprises using the session key to encrypt a subsequent message sent from the client device to the server.

20

31. The method of claim 27, wherein performing a Diffie-Hellman key exchange with the server comprises:

receiving Diffie-Hellman global values and a public Diffie-Hellman server key from the server, and

5 storing at least one of the Diffie-Hellman global values and the public Diffie-Hellman server key in the secure storage of the security engine of the system-on-a-chip.

32. The method of claim 16, further comprising:

retrieving a client certificate stored on the client device;

10 signing a client certificate using a security key stored in a secure memory of the security engine of the system-on-a-chip; and

sending the client certificate to the server.

33. The method of claim 16, further comprising:

15 generating, in the security engine of the system-on-a-chip, a hash code of a preceding message sent from the client to the server;

signing the hash code using a security key stored in a secure memory of the security engine; and

20 sending a client certificate verification message to the server, the client certificate verification message including the signed hash code.

34. The method of claim 16, wherein establishing the secure communication session comprises:

generating, in the security engine, a hash code as a function of the session key;

and

5 sending a client completion message that includes the hash code to the server to indicate the client has completed an initial handshake procedure.

35. A source device comprising:

10 a system-on-a-chip having a security engine, the system-on-a-chip including a plurality of instructions that when executed results in the system-on-a-chip performing the method of claim 16-34.

36. One or more machine readable media comprising a plurality of instructions that in response to being executed by a client device result in the client device
15 performing the method of claims 16-34.

37. A method comprising:

generating a random nonce in a security engine of a system-on-a-chip of a client device;

20 initiating, using the client device, a request for a Secure Sockets Layer communication session with a server over a network, the request including the random nonce;

performing a cryptographic key exchange, using the security engine of the system-on-a-chip, with the server to generate a symmetric session key to encrypt messages sent to the server and decrypt messages received from the server during the Secure Sockets Layer
25 communication session;

storing the session key in a secure memory of the security engine of the system-on-a-chip; and

generating, in the security engine, a hash code as a function of the session key;

and

30 sending a client completion message to the server that includes the hash code to indicate the client has completed an initial handshake procedure.

38. The method of claim 37, wherein performing the cryptographic key exchange with the server comprises performing a Rivest-Shamir-Adleman key exchange, using the security engine of the system-on-a-chip, with the server.

5 39. The method of claim 38, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises:

generating a pre-master key in the security engine;
encrypting the pre-master key using a security key of the security engine; and
sending the encrypted pre-master key to the server.

10

40. The method of claim 39, further comprising:
wrapping the pre-master key in the security engine using a server public key, and
storing the wrapped pre-master key in the secure storage of the security engine of
the system-on-a-chip.

15

41. The method of claim 39, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises generating the session key in the security engine of the system-on-a-chip as a function of the pre-master key.

20

42. The method of claim 41, wherein generating the session key in the security engine comprises calculating, using the security engine of the system-on-a-chip, a hash function as a function of the random nonce generated by the security engine and a nonce received from the server.

25

43. The method of claim 37, wherein performing the cryptographic key exchange with the server comprises performing a Diffie-Hellman key exchange, using the security engine of the system-on-a-chip, with the server.

30

44. The method of claim 43, wherein performing a Diffie-Hellman key exchange with the server comprises:

generating, in the security engine of the system-on-a-chip, a public Diffie-Hellman client key and a private Diffie-Hellman client key;
signing the public Diffie-Hellman client key using a security key of the security engine of the system-on-a-chip; and

sending the signed public Diffie-Hellman key to the server.

45. The method of claim 44, wherein performing a Diffie-Hellman key exchange with the server comprises:

- 5 receiving a public Diffie-Hellman server key from the server;
 generating, in the security engine of the system-on-a-chip, the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

46. A source device comprising:

- 10 a system-on-a-chip having a security engine, the system-on-a-chip including a plurality of instructions that when executed results in the system-on-a-chip performing the method of claim 37-45.

47. One or more machine readable media comprising a plurality of
15 instructions that in response to being executed by a client device result in the client device performing the method of claims 37-45.

ABSTRACT OF THE DISCLOSURE

A method, device, and system for establishing a secure communication session with a server includes initiating a request for a secure communication session, such as a Secure Sockets Layer (SSL) communication session with a server using a nonce value generated in a security engine of a system-on-a-chip (SOC) of a client device. Additionally, a cryptographic key exchange is performed between the client and the server to generate a symmetric session key, which is stored in a secure storage of the security engine. The cryptographic key exchange may be, for example, a Rivest-Shamir-Adleman (RSA) key exchange or a Diffie-Hellman key exchange. Private keys and other data generated during the cryptographic key exchange may be generated and/or stored in the security engine.

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

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	P41624US
		Application Number	
Title of Invention	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE		
The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76. This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.			

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)
--

Inventor Information:

Inventor 1					Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Hormuzd	M.	Khosravi		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					
City	Portland	State/Province	OR	Country of Residence i	US
Mailing Address of Inventor:					
Address 1		4816 NW 166th Avenue			
Address 2					
City	Portland	State/Province	OR		
Postal Code	97229	Country i	US		
Inventor 2					Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Edward	C.	Epp		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					
City	Hillsboro	State/Province	OR	Country of Residence i	US
Mailing Address of Inventor:					
Address 1		2111 NE 25th Avenue			
Address 2					
City	Portland	State/Province	OR		
Postal Code	97124	Country i	US		
Inventor 3					Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Farhana		Kabir		
Residence Information (Select One) ☒ US Residency ☐ Non US Residency ☐ Active US Military Service					

Application Data Sheet 37 CFR 1.76		Attorney Docket Number		P41624US	
		Application Number			
Title of Invention		METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE			
City	Camas	State/Province	WA	Country of Residence i	US
Mailing Address of Inventor:					
Address 1		20021 SE 3rd Circle			
Address 2					
City	Camas	State/Province	WA		
Postal Code	98607	Country i	US		
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.					Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).			
☐ An Address is being provided for the correspondence information of this application.			
Customer Number	73486		
Email Address	inteldocs@cpaglobal.com	Add Email	Remove Email

Application Information:

Title of the Invention	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE		
Attorney Docket Number	P41624US	Small Entity Status Claimed	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	4	Suggested Figure for Publication (if any)	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐ Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.			
Please Select One:			
☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)	

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	P41624US
		Application Number	
Title of Invention	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE		
Customer Number	73486		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.			
Prior Application Status	Pending	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	a 371 of international	PCT/US2011/065069	2011-12-15
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.			Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).			
			Remove
Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Access Code ¹ (if applicable)
Additional Foreign Priority Data may be generated within this form by selecting the Add button.			Add

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

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.

Authorization to Permit Access:

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	P41624US
		Application Number	
Title of Invention	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE		

☒ Authorization to Permit Access to the Instant Application by the Participating Offices
If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application. In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application. In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.				
Applicant 1				Remove
If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.				
Clear				
☐ Assignee	☐ Legal Representative under 35 U.S.C. 117	☐ Joint Inventor		
☐ Person to whom the inventor is obligated to assign.		☐ Person who shows sufficient proprietary interest		
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:				
Name of the Deceased or Legally Incapacitated Inventor :				
If the Applicant is an Organization check here. ☐				
Prefix	Given Name	Middle Name	Family Name	Suffix

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	P41624US
		Application Number	
Title of Invention	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE		

Mailing Address Information:			
Address 1			
Address 2			
City		State/Province	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			
Additional Applicant Data may be generated within this form by selecting the Add button.			Add

Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1				
Complete this section only if non-applicant assignee information is desired to be included on the patent application publication in accordance with 37 CFR 1.215(b). Do not include in this section an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest), as the patent application publication will include the name of the applicant(s).				
				Remove
If the Assignee is an Organization check here. ☐				
Prefix	Given Name	Middle Name	Family Name	Suffix
Mailing Address Information:				
Address 1				
Address 2				
City		State/Province		
Country i		Postal Code		
Phone Number		Fax Number		
Email Address				
Additional Assignee Data may be generated within this form by selecting the Add button.				Add

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

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	P41624US
		Application Number	
Title of Invention	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE		

Signature:

Remove

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications					
Signature	/Glen M. Kellett, Reg No. 60202/			Date (YYYY-MM-DD)	2013-06-19
First Name	Glen M.	Last Name	Kellett	Registration Number	60202
Additional Signature may be generated within this form by selecting the Add button.					Add

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal				
Application Number:				
Filing Date:				
Title of Invention:		METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE		
First Named Inventor/Applicant Name:		Hormuzd Khosravi		
Filer:		Glen Madison Kellett/Dannel Johnson		
Attorney Docket Number:		P41624US		
Filed as Large Entity				
U.S. National Stage under 35 USC 371 Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
National Stage Fee	1631	1	280	280
Natl Stage Search Fee - Report provided	1642	1	480	480
National Stage Exam - all other cases	1633	1	720	720
Pages:				
Claims:				
Claims in excess of 20	1615	4	80	320
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				1800

Electronic Acknowledgement Receipt	
EFS ID:	16093266
Application Number:	13997412
International Application Number:	PCT/US11/65069
Confirmation Number:	1045
Title of Invention:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor/Applicant Name:	Hormuzd Khosravi
Customer Number:	73486
Filer:	Glen Madison Kellett/Dannel Johnson
Filer Authorized By:	Glen Madison Kellett
Attorney Docket Number:	P41624US
Receipt Date:	24-JUN-2013
Filing Date:	
Time Stamp:	14:27:46
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$1800
RAM confirmation Number	753
Deposit Account	504238
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. 1.492 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)					
Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)					
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Drawings-only black and white line drawings	P41624PCT_FIGS.pdf	48349	no	4
			066f1196ae2b2be216e2877db1a79ae2be583a1a		
Warnings:					
Information:					
2	Documents submitted with 371 Applications	P41624PCT_ISR.pdf	567205	no	11
			d2d8afd9c945eb595a9cabeecc581af1f7a18cd65c2		
Warnings:					
Information:					
3	Transmittal of New Application	P41624US_1390.pdf	222264	no	4
			eeb40af8b3acdb7b887f299d2f6ec8bf8609d6c6c		
Warnings:					
Information:					
4		P41624US_Preliminary_Amendment.pdf	35221	yes	10
			6ff8b5a23b35f42d1a9fad3fe4870a1a1242a656		
	Multipart Description/PDF files in .zip description				
	Document Description	Start		End	
	Preliminary Amendment	1		1	
	Claims	2		8	
	Applicant Arguments/Remarks Made in an Amendment	9		10	
Warnings:					
Information:					
5		P41624PCT_APPLN_Use.pdf	120430	yes	25
			434175b9358a0acc7296db74864c2f3934cf40be		
	Multipart Description/PDF files in .zip description				
	Document Description	Start		End	
	Specification	1		15	
	Claims	16		24	

	Abstract		25	25
Warnings:				
Information:				
6	Application Data Sheet	P41624US_ADS.pdf	1503119 b7b6e86a89c6ce56c7df8790ae51569e3da0d940	no 7
Warnings:				
Information:				
7	Fee Worksheet (SB06)	fee-info.pdf	36958 d3fadccf2239f543a216da67a214dd5a9ef5ad0	no 2
Warnings:				
Information:				
Total Files Size (in bytes):			2533546	
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.				

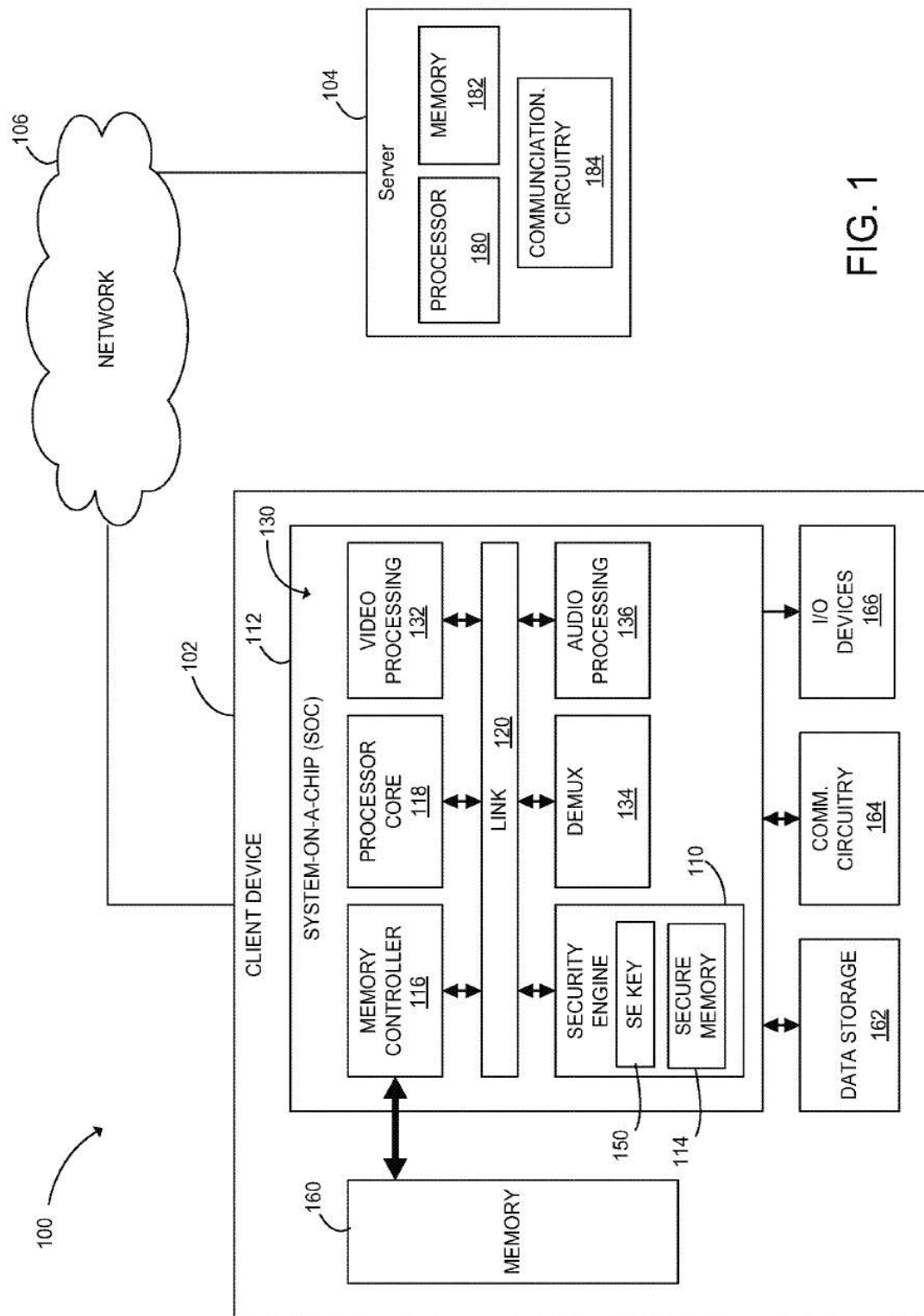


FIG. 1

200

LEVEL 0	PROTECTION OF CLIENT PRIVATE DEVICE KEY USED FOR SIGNING & VERIFICATION	
LEVEL 1	PROTECTION OF SESSION KEYS USED FOR DATA ENCRYPTION	
	RSA KEY EXCHANGE	DIFFIE-HELLMAN KEY EXCHANGE
	PROTECTION OF PRE-MASTER KEY	PROTECTION OF CLIENT PRIVATE DH KEY
LEVEL 2	PROTECTION OF APPLICATION DATA	

FIG. 2

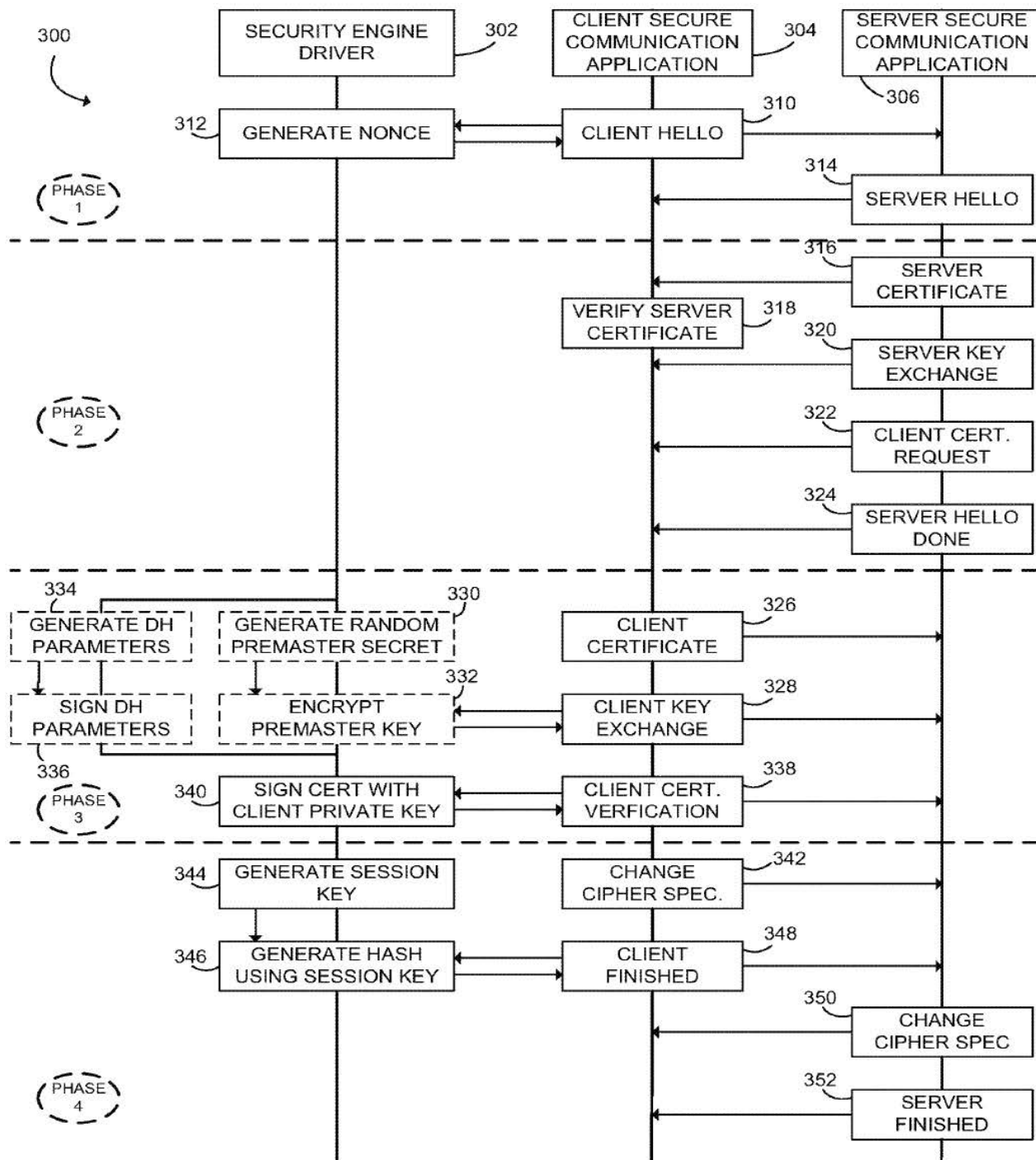


FIG. 3

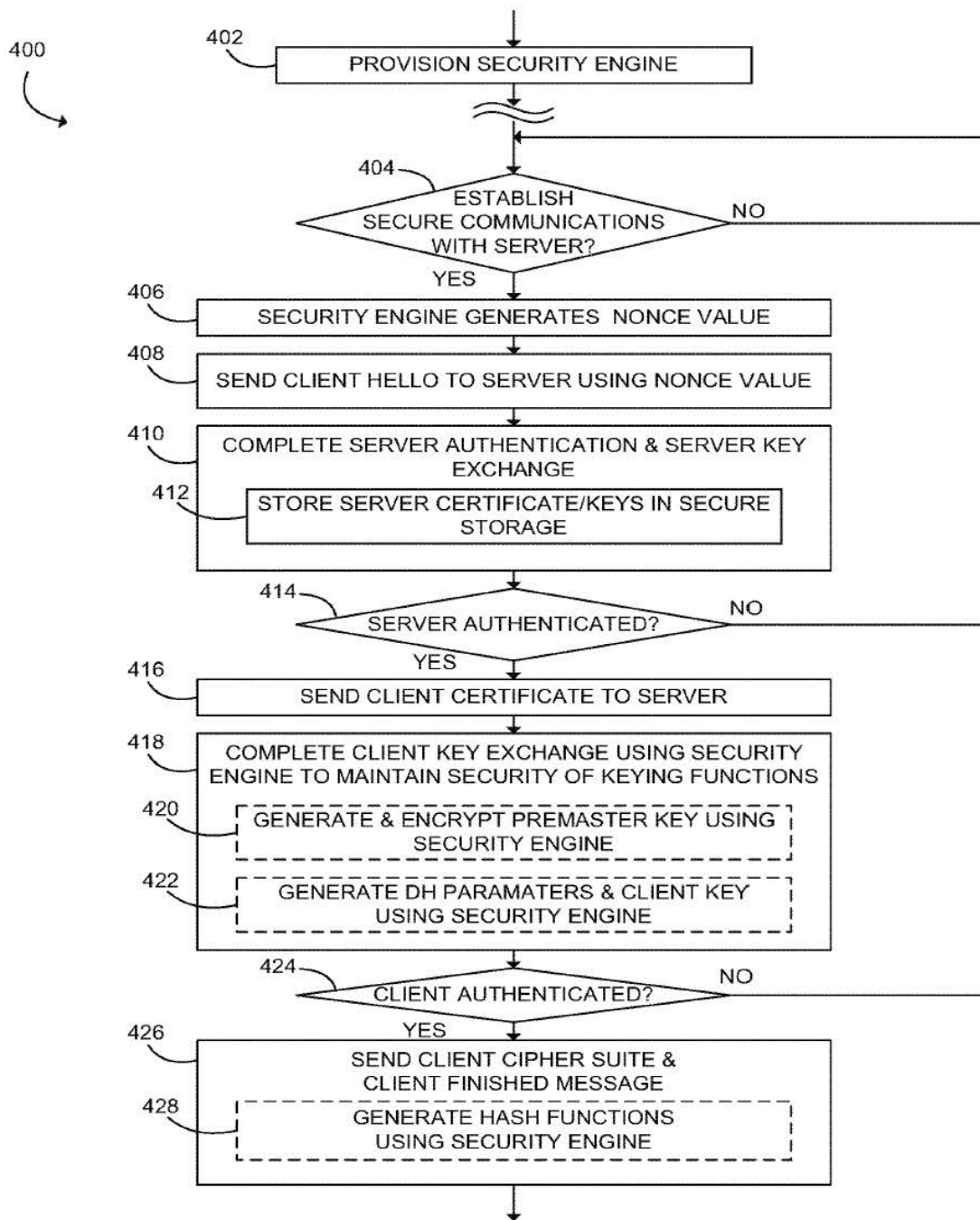


FIG. 4

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
KELLETT GLEN M.
BARNES & THORNBURG, LLP C/O CPA GLOBAL P.O. BOX 52050 MINNEAPOLIS MN 55402 USA

PCT

**NOTIFICATION OF TRANSMITTAL OF
THE INTERNATIONAL SEARCH REPORT AND
THE WRITTEN OPINION OF THE INTERNATIONAL
SEARCHING AUTHORITY, OR THE DECLARATION**

(PCT Rule 44.1)

Date of mailing (day/month/year) 30 AUGUST 2012 (30.08.2012)	
Applicant's or agent's file reference P41624PCT	FOR FURTHER ACTION See paragraphs 1 and 4 below
International application No. PCT/US2011/065069	International filing date (day/month/year) 15 DECEMBER 2011 (15.12.2011)
Applicant INTEL CORPORATION et al	

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.
Filing of amendments and statement under Article 19:
 The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):
When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.
Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes
 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 338 82 70
For more detailed instructions, see PCT Applicant's Guide, International Phase, paragraphs 9.004 - 9.011.
2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.
3. ☐ **With regard to any protest against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:**
☐ the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.
☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.
4. **Reminders**
 The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.
 Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90bis.1 and 90bis.3).
 Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.
 In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.
 For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the PCT Applicant's Guide, National Chapters.

Name and mailing address of the ISA/KR  Korean Intellectual Property Office 189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140 Form PCT/ISA/220 (July 2010)	Authorized officer COMMISSIONER Telephone No. 82-42-481-8754	CPA GLOBAL SEP 11 20 RECEIVED Coded _____ Verified _____
---	--	--

▼ Attention

Copies of the documents cited in the international search report can be searched in the following Korean Intellectual Property Office English website for three months from the date of mailing of the international search report.

<http://www.kipo.go.kr/en/> => PCT Services => PCT Services

ID : PCT international application number

PW : **CZKLKWRL**

Inquiries related to PCT International Search Report or Written Opinion prepared by KIPO as an International Searching Authority can be answered not only by KIPO but also through IPKC (Intellectual Property Korea Center), located in Vienna, VA, which functions as a PCT Help Desk for PCT applicants.

Homepage: <http://www.ipkcenter.com>

Email: ipkc@ipkcenter.com

Phone: +1 703 388 1066

Fax: +1 703 388 1084

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference P41624PCT	FOR FURTHER ACTION see Form PCT/ISA/220 as well as, where applicable, item 5 below.	
International application No. PCT/US2011/065069	International filing date (<i>day/month/year</i>) 15 DECEMBER 2011 (15.12.2011)	(Earliest) Priority Date (<i>day/month/year</i>)
Applicant INTEL CORPORATION et al		

This International search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

a. With regard to the language, the international search was carried out on the basis of:

- ☒ the international application in the language in which it was filed
☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

b. ☐ This international search report has been established taking into account the rectification of an obvious mistake authorized by or notified to this Authority under Rule 91 (Rule 43.6bis(a)).

c. ☐ With regard to any nucleotide and/or amino acid sequence disclosed in the international application, see Box No. I.

2. ☐ Certain claims were found unsearchable (See Box No. II)

3. ☐ Unity of invention is lacking (See Box No. III)

4. With regard to the title,

- ☒ the text is approved as submitted by the applicant.
☐ the text has been established by this Authority to read as follows:

5. With regard to the abstract,

- ☒ the text is approved as submitted by the applicant.
☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the drawings,

- a. the figure of the drawings to be published with the abstract is Figure No 1
☒ as suggested by the applicant.
☐ as selected by this Authority, because the applicant failed to suggest a figure
☐ as selected by this Authority, because this figure better characterizes the invention.
b. ☐ none of the figure is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/065069

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/14(2006.01); H04L 9/32(2006.01);

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 9/14; H04L 9/08; H04L 9/32; H04L 9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: secure communication, secure socket layer, SSL, transport layer security, IPSec, random
nonce, handshake initiate, key exchange, session key, secure memory, hash code, handshake completion

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2011-0231923 A1 (BOLLAY BENN SAPIN et al.) 22 September 2011 See Claims 1, 6; Paragraphs [27], [63], [70], [89]-[93], [95], [123]-[126]; Figures 2, 5, 8	1-32, 35-36
A		33-34, 37-47
Y	US 2005-0213768 A1 (DAVID DURHAM et al.) 20 September 2005 See Claims 1-4; Paragraphs [14], [15], [17], [20], [21], [26], [28], [33], [45], [49], [53], [54]; Figures 1, 2, 5	1-32, 35-36
A		33-34, 37-47
A	US 2010-0206525 A1 (SHAH PARAS et al.) 25 November 2010 See Claims 1, 6; Paragraphs [47], [50], [54]-[56], [59], [60]; Figures 2, 3	1-47
A	US 2006-0037793 A1 (BUER MARK) 14 February 2006 See Claims 11-17; Paragraphs [35], [39]-[43]; Figures 4, 7-9	1-47

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

29 AUGUST 2012 (29.08.2012)

Date of mailing of the international search report

30 AUGUST 2012 (30.08.2012)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan
City, 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Lee Hyoung Il

Telephone No. 82-42-481-8199



INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2011/065069

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011-0231923 A1	22.09.2011	CN 102195878 A	21.09.2011
		US 2011-231649 A1	22.09.2011
		US 2011-231651 A1	22.09.2011
		US 2011-231652 A1	22.09.2011
		US 2011-231653 A1	22.09.2011
		US 2011-231655 A1	22.09.2011
		WO 2011-116342 A2	22.09.2011
		WO 2011-116342 A3	22.12.2011
US 2005-0213768 A1	29.09.2005	CN 1926837 A	07.03.2007
		CN 1926837 B	06.04.2011
		EP 1728376 A1	06.12.2006
		EP 1728376 B1	15.07.2009
		JP 04-579969 B2	03.09.2010
		JP 2007-525913 A	06.09.2007
		JP 4579969 B2	10.11.2010
		KR 10-0831437 B1	21.05.2008
		KR 10-2006-0127229 A	11.12.2006
US 2010-0299525 A1	25.11.2010	WO 2005-101794 A1	27.10.2005
		AU 2006-280301 A1	22.02.2007
		CN 101292233 A0	22.10.2008
		EP 1904931 A2	02.04.2008
		JP 2009-505493 A	05.02.2009
		US 2007-0038653 A1	15.02.2007
		US 2009-0119504 A1	07.05.2009
US 2008-0037793 A1	14.02.2008	WO 2007-021483 A2	22.02.2007
		EP 1484890 A2	08.12.2004
		EP 1484890 A3	11.07.2012
		EP 1484913 A2	08.12.2004
		EP 1484913 A3	15.04.2009
		US 2004-0247131 A1	09.12.2004
		US 2005-0041802 A1	24.02.2005
		US 2010-0296573 A1	25.11.2010
		US 6724335 B1	20.04.2004
		US 7289632 B2	30.10.2007
		US 7768434 B2	03.08.2010
		US 8111183 B2	07.02.2012

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: KELLETT GLEN M. BARNES & THORNBURG, LLP C/O CPA GLOBAL P.O. BOX 52050 MINNEAPOLIS MN 55402 USA

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing (day/month/year) 30 AUGUST 2012 (30.08.2012)	
Applicant's or agent's file reference P41624PCT	FOR FURTHER ACTION See paragraph 2 below
International application No. PCT/US2011/065069	International filing date (day/month/year) 15 DECEMBER 2011 (15.12.2011)
Priority date(day/month/year)	
International Patent Classification (IPC) or both national classification and IPC H04L 9/14(2006.01); H04L 9/32(2006.01);	
Applicant INTEL CORPORATION et al	

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability, citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☒ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/KR  Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Date of completion of this opinion 29 AUGUST 2012 (29.08.2012)	Authorized officer Lee Hyoung Il Telephone No 82-42-481-8199
---	---	--



Form PCT/ISA/237 (cover sheet) (July 2011)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US2011/065069

Box No. 1 Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of :
 - ☒ the international application in the language in which it was filed
 - ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))
3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:
 - a. a sequence listing filed or furnished
 - ☐ on paper
 - ☐ in electronic form
 - b. time of filing or furnishing
 - ☐ contained in the international application as filed.
 - ☐ filed together with the international application in electronic form.
 - ☐ furnished subsequently to this Authority for the purposes of search.
4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5. Additional comments:

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2011/065069

**Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability;
citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-47	YES
	Claims	NONE	NO
Inventive step (IS)	Claims	33-34,37-47	YES
	Claims	1-32,35-36	NO
Industrial applicability (IA)	Claims	1-47	YES
	Claims	NONE	NO

2. Citations and explanations :

Reference is made to the following documents:

D1: US 2011-0231923 A1 (BOLLAY BENN SAPIN et al.) 22 September 2011
D2: US 2005-0213768 A1 (DAVID DURHAM et al.) 29 September 2005
D3: US 2010-0299525 A1 (SHAH PARAS et al.) 25 November 2010
D4: US 2008-0037793 A1 (BUER MARK) 14 February 2008

1. Novelty and Inventive Step

1.1 Independent Claim 1

D1, which is considered to be the closest prior art to the subject matter of claim 1, discloses an apparatus for a client to generate random number, send client hello message for SSL handshake initiation, perform a server key exchange and a client key exchange, generate a session key based on secret data, store the session in a data store, establish an encrypted session between the server and the client using the session key. Claim 1 differs from D1 in that the apparatus uses the secure memory. However, D2 discloses an apparatus storing the cryptographic key in a secure storage. Accordingly, claim 1 would have been obvious over D1 in view of D2. Therefore, claim 1 lacks an inventive step under PCT Article 33(3).

1.2 Dependent Claims 2-15

Claims 2-15, which are dependent on claim 1, lack an inventive step under PCT Article 33(3), because the additional features of claims 2-15 are merely matters of design option when the general technical knowledge about the state of the art is used.

1.3 Independent Claim 16

Claim 16 relates to a method performing the functions of the apparatus according to claim 1. Claim 16 is considered to lack an inventive step under PCT Article 33(3), because the subject matter of claim 1 is considered to lack an inventive step under PCT Article 33(3).

[Continued on Supplemental Box]

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2011/065069

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

Claims 35-36 and 46-47 do not comply with PCT Rule 6.4(a) because the multiple dependent claims don't refer to other claims in the alternative way.

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2011/065069

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

[Box V]

[Box V]

1.4 Dependent Claims 17-32

Claims 17-32, which are dependent on claim 16, lack an inventive step under PCT Article 33(3), because the additional features of claims 17-32 are merely matters of design option when the general technical knowledge about the state of the art is used.

1.5 Dependent Claims 33-34

The additional feature of claim 33 dependent on claim 16 is not disclosed in any of the prior art documents, nor is it obvious to a person skilled in the art by the documents. Accordingly, claim 33 is novel and involves an inventive step under PCT Article 33(2) and (3).

The additional feature of claim 34 dependent on claim 16 is not disclosed in any of the prior art documents, nor is it obvious to a person skilled in the art by the documents. Accordingly, claim 34 is novel and involves an inventive step under PCT Article 33(2) and (3).

1.6 Independent Claim 35

Claim 35 relates to a source device including a plurality of instructions performing the method of claims 16-32. Claim 35 is considered to lack an inventive step under PCT Article 33(3), because the subject matters of claims 16-32 are considered to lack an inventive step under PCT Article 33(3).

1.7 Independent Claim 36

Claim 36 relates to one or more machine readable media comprising a plurality of instructions performing the method of claims 16-32. Claim 36 is considered to lack an inventive step under PCT Article 33(3), because the subject matters of claims 16-32 are considered to lack an inventive step under PCT Article 33(3).

1.8 Claims 37-45

The subject matter of claim 37 differs from these prior art documents in generating a hash code as a function of the session key and sending a client completion message to the server that includes the hash code to indicate the client has completed an initial handshake procedure. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 37 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 38-45 are dependent on claim 37 and therefore meet the requirements of PCT Article 33(2) and (3).

1.9 Claims 46-47

Claim 46 relates to a source device including a plurality of instructions performing the method of claims 37-45. Claim 46 is considered to be novel and to involve an inventive step under PCT Article 33(2) and (3), because the subject matters of claim 37-45 are considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

Claim 47 relates to one or more machine readable media comprising a plurality of instructions performing the method of claims 37-45. Claim 47 is considered to be novel and to involve an inventive step under PCT Article 33(2) and (3), because the subject matters of claim 37-45 are considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

[Continued on Supplemental Box]

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US2011/065069

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

[Box V]

2. Industrial Applicability

Claims 1-47 are industrially applicable under PCT Article 33(4).

Box No. VIII (iv) DECLARATION: INVENTORSHIP (only for the purposes of the designation of the United States of America)
The declaration must conform to the following standardized wording provided for in Section 214; see Notes to Boxes Nos. VIII, VIII (i) to (v) (in general) and the specific Notes to Box No. VIII (iv). If this Box is not used, this sheet should not be included in the request.

**Declaration of Inventorship (Rules 4.17(iv) and 51bis.1(a)(iv))
 for the purposes of the designation of the United States of America:**

I hereby declare that I believe I am the original, first and sole (if only one inventor is listed below) or joint (if more than one inventor is listed below) inventor of the subject matter which is claimed and for which a patent is sought.

This declaration is directed to the international application of which it forms a part (if filing declaration with application).

This declaration is directed to international application No. PCT/... PCT/US2011/065069 ... (if furnishing declaration pursuant to Rule 26ter).

I hereby declare that my residence, mailing address, and citizenship are as stated next to my name.

I hereby state that I have reviewed and understand the contents of the above-identified international application, including the claims of said application. I have identified in the request of said application, in compliance with PCT Rule 4.10, any claim to foreign priority, and I have identified below, under the heading "Prior Applications," by application number, country or Member of the World Trade Organization, day, month and year of filing, any application for a patent or inventor's certificate filed in a country other than the United States of America, including any PCT international application designating at least one country other than the United States of America, having a filing date before that of the application on which foreign priority is claimed.

Prior Applications:

I hereby acknowledge the duty to disclose information that is known by me to be material to patentability as defined by 37 C.F.R. § 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the PCT international filing date of the continuation-in-part application.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Name: KHOSRAVI, Homuzd, M.

Residence: Portland, OR
 (city and either US state, if applicable, or country)

Mailing Address: 2723 NW Kanner Ter Unit
 4816 NW 46th Ave, Portland, OR, US 97229

Citizenship: India

Inventor's Signature: [Signature] Date: 2-22-2012
 (The signature must be that of the inventor, not that of the agent)

Name: EPP, Edward, C.

Residence: Hillsboro, OR
 (city and either US state, if applicable, or country)

Mailing Address: 2111 NE 25th Ave Hillsboro, OR, US 97124
 3035 NE 23rd Av., Portland, OR 97212 ECE

Citizenship: United States of America

Inventor's Signature: [Signature] Date: 2-22-2012
 (The signature must be that of the inventor, not that of the agent)

☐ This declaration is continued on the following sheet, "Continuation of Box No. VIII (iv)".

PCT REQUESTOriginal (for **SUBMISSION**)

0	For receiving Office use only	
0-1	International Application No.	PCT/US11/65069
0-2	International Filing Date	15 DEC 2011 (15.12.11)
0-3	Name of receiving Office and "PCT International Application"	PCT INTERNATIONAL APPLICATION RO/US
0-4	Form PCT/RO/101 PCT Request	
0-4-1	Prepared Using	PCT-SAFE [EASY/EFS-Web mode] Version 3.51.051.227 MT/FOP 20111001/0.20.5.19
0-5	Petition The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	Receiving Office (specified by the applicant)	United States Patent and Trademark Office (USPTO) (RO/US)
0-7	Applicant's or agent's file reference	P41624PCT
I	Title of Invention	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
II	Applicant	
II-1	This person is	Applicant only
II-2	Applicant for	All designated States except US
II-4	Name	INTEL CORPORATION
II-5	Address	2200 Mission College Boulevard Santa Clara, California 95052 United States of America
II-6	State of nationality	US
II-7	State of residence	US
II-8	Telephone No.	317-236-1313
II-10	e-mail	docketing@cpaglobal.com
II-10(a)	E-mail authorization The receiving Office, the International Searching Authority, the International Bureau and the International Preliminary Examining Authority are authorized to use this e-mail address, if the Office or Authority so wishes, to send notifications issued in respect of this international application:	as advance copies followed by paper notifications

PCT REQUEST

Original (for SUBMISSION)

III-1	Applicant and/or inventor	
III-1-1	This person is	Applicant and inventor
III-1-2	Applicant for	US only
III-1-4	Name (LAST, First)	KHOSRAVI, Hormuzd M.
III-1-5	Address	4816 NW 166th Avenue Portland, Oregon 97229 United States of America
III-1-6	State of nationality	IN
III-1-7	State of residence	US
III-2	Applicant and/or inventor	
III-2-1	This person is	Applicant and inventor
III-2-2	Applicant for	US only
III-2-4	Name (LAST, First)	EPP, Edward C.
III-2-5	Address	2111 NE 25th Avenue Hillsboro, Oregon 97124 United States of America
III-2-6	State of nationality	US
III-2-7	State of residence	US
III-3	Applicant and/or inventor	
III-3-1	This person is	Applicant and inventor
III-3-2	Applicant for	US only
III-3-4	Name (LAST, First)	KABIR, Farhana
III-3-5	Address	20021 SE 3rd Circle Camas, Washington 98607 United States of America
III-3-6	State of nationality	US
III-3-7	State of residence	US

PCT REQUEST

Original (for SUBMISSION)

IV-1	Agent or common representative; or address for correspondence The person identified below is hereby/ has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	Agent	
IV-1-1	Name (LAST, First)	KELLETT, Glen M.	
IV-1-2	Address	Barnes & Thornburg, LLP c/o CPA Global P.O. Box 52050 Minneapolis, Minnesota 55402 United States of America	
IV-1-3	Telephone No.	317-236-1313	
IV-1-5	e-mail	docketing@cpaglobal.com	
IV-1-5(a))	E-mail authorization The receiving Office, the International Searching Authority, the International Bureau and the International Preliminary Examining Authority are authorized to use this e-mail address, if the Office or Authority so wishes, to send notifications issued in respect of this international application:	as advance copies followed by paper notifications	
IV-1-6	Agent's registration No.	60202	
V	DESIGNATIONS		
V-1	The filing of this request constitutes under Rule 4.9(a), the designation of all Contracting States bound by the PCT on the international filing date, for the grant of every kind of protection available and, where applicable, for the grant of both regional and national patents.		
VI-1	Priority Claim	NONE	
VII-1	International Searching Authority Chosen	Korean Intellectual Property Office (ISA/KR)	
VIII	Declarations	Number of declarations	
VIII-1	Declaration as to the identity of the inventor	—	
VIII-2	Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent	—	
VIII-3	Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application	—	
VIII-4	Declaration of inventorship (only for the purposes of the designation of the United States of America)	—	
VIII-5	Declaration as to non-prejudicial disclosures or exceptions to lack of novelty	—	

PCT REQUESTOriginal (for **SUBMISSION**)

IX	Check list	Number of sheets	Electronic file(s) attached
IX-1	Request (including declaration sheets)	4	✓
IX-2	Description	15	—
IX-3	Claims	9	—
IX-4	Abstract	1	✓
IX-5	Drawings	4	—
IX-7	TOTAL	33	
	Accompanying Items	Paper document(s) attached	Electronic file(s) attached
IX-8	Fee calculation sheet	✓	—
IX-19	Other	PCT Transmittal	
IX-19	Other	PCT Transmittal	
IX-20	Figure of the drawings which should accompany the abstract	1	
IX-21	Language of filing of the international application	English	
X-1	Signature of applicant, agent or common representative	/Glen M. Kellet, Reg No. 60202/	
X-1-1	Name (LAST, First)	KELLETT, Glen M.	
X-1-2	Name of signatory		
X-1-3	Capacity (if such capacity is not obvious from reading the request)		

FOR RECEIVING OFFICE USE ONLY

15-12-2011

10-1	Date of actual receipt of the purported international application	15 DEC 2011 (15.12.11)
10-2	Drawings:	
10-2-1	Received	
10-2-2	Not received	
10-3	Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application	
10-4	Date of timely receipt of the required corrections under PCT Article 11(2)	
10-5	International Searching Authority	ISA/KR
10-6	Transmittal of search copy delayed until search fee is paid	

FOR INTERNATIONAL BUREAU USE ONLY

11-1	Date of receipt of the record copy by the International Bureau	
-------------	---	--

(51) International Patent Classification:
H04L 9/14 (2006.01) H04L 9/32 (2006.01)(21) International Application Number:
PCT/US2011/065069(22) International Filing Date:
15 December 2011 (15.12.2011)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, California 95052 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): KHOSRAVI, Hormuzd M. [IN/US]; 4816 NW 166th Avenue, Portland, Oregon 97229 (US). EPP, Edward C. [US/US]; 2111 NE 25th Avenue, Hillsboro, Oregon 97124 (US). KABIR, Farhana [US/US]; 20021 SE 3rd Circle, Camas, Washington 98607 (US).

(74) Agent: KELLETT, Glen M.; Barnes & Thornburg, LLP, c/o CPA Global, P.O. Box 52050, Minneapolis, Minnesota 55402 (US).

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

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

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

Declarations under Rule 4.17:

— of inventorship (Rule 4.17(iv))

Published:

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

(54) Title: METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE

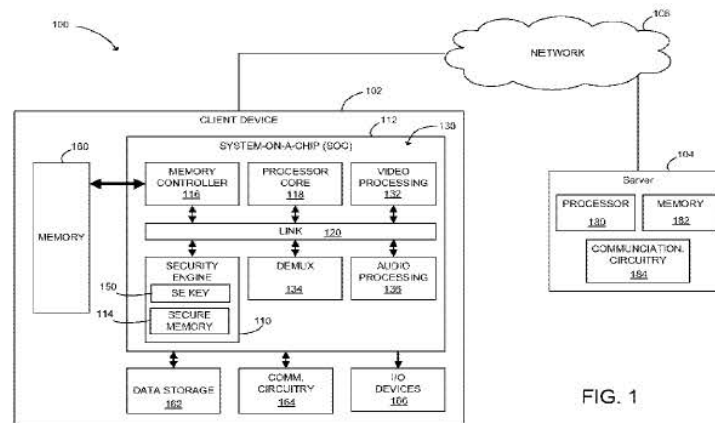


FIG. 1

(57) Abstract: A method, device, and system for establishing a secure communication session with a server includes initiating a request for a secure communication session, such as a Secure Sockets Layer (SSL) communication session with a server using a nonce value generated in a security engine of a system-on-a-chip (SOC) of a client device. Additionally, a cryptographic key exchange is performed between the client and the server to generate a symmetric session key, which is stored in a secure storage of the security engine. The cryptographic key exchange may be, for example, a Rivest-Shamir-Adleman (RSA) key exchange or a Diffie-Hellman key exchange. Private keys and other data generated during the cryptographic key exchange may be generated and/or stored in the security engine.

**METHOD AND DEVICE FOR SECURE COMMUNICATIONS
OVER A NETWORK USING A HARDWARE SECURITY ENGINE**

BACKGROUND

5 Cryptographic communication protocols are used to establish a secure communication session between computing devices over an untrusted network or communication link. One commonly used cryptographic communication protocol is the Secure Sockets Layer (SSL) protocol. The SSL protocol, and the related Transport Layer Security (TLS) protocol, is used for many different types of secure communication sessions including, for example, secure web-browsing, ecommerce, secure upgrades, and other secure communication sessions between two computing devices on an untrusted network such as the Internet. Other communication protocols may utilize the SSL/TLS protocol to provide the underlying security. For example, the Hypertext Transfer Protocol Secure (HTTPS) uses SSL/TLS for encryption of messages between devices. Typically, the cryptographic security offered by the SSL/TLS protocols is done so in-band and performed at the software application level.

15 Some computing and electronic devices utilize system-on-a-chip (SOC) designs due to their relatively small footprint. SOC devices are integrated circuits that incorporate various components, in addition to the processing core, of electronic systems on a single die. For example, an SOC may include a processor core, memory controller, video components, audio components, and/or communication components on a single chip.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention described herein is illustrated by way of example and not by way of limitation in the accompanying figures. For simplicity and clarity of illustration, elements illustrated in the figures are not necessarily drawn to scale. For example, the dimensions of some elements may be exaggerated relative to other elements for clarity. Further, where considered appropriate, reference labels have been repeated among the figures to indicate corresponding or analogous elements.

25 FIG. 1 is a simplified block diagram of at least one embodiment of a system for establishing a secure communication session between a client device having a system-on-a-chip (SOC) and a server over a network;

30 FIG. 2 is a block diagram of at least one embodiment of a security scheme for the system of FIG. 1;

FIG. 3 is a simplified sequence diagram of at least one embodiment of a communication sequence of the client device and server of FIG. 1 to establish a secure communication session; and

5 FIG. 4 is a simplified flow diagram of at least one embodiment of a method for establishing a secure communication session executed by the client device of FIG. 1.

DETAILED DESCRIPTION OF THE DRAWINGS

While the concepts of the present disclosure are susceptible to various modifications and alternative forms, specific exemplary embodiments thereof have been shown by way of example in the drawings and will herein be described in detail. It should be understood,
10 however, that there is no intent to limit the concepts of the present disclosure to the particular forms disclosed, but on the contrary, the intention is to cover all modifications, equivalents, and alternatives consistent with the present disclosure and the appended claims.

In the following description, numerous specific details such as logic implementations, opcodes, means to specify operands, resource partitioning/sharing/duplication
15 implementations, types and interrelationships of system components, and logic partitioning/integration choices are set forth in order to provide a more thorough understanding of the present disclosure. It will be appreciated, however, by one skilled in the art that embodiments of the disclosure may be practiced without such specific details.

20 In other instances, control structures, gate level circuits and full software instruction sequences have not been shown in detail in order not to obscure the invention. Those of ordinary skill in the art, with the included descriptions, will be able to implement appropriate functionality without undue experimentation.

References in the specification to “one embodiment,” “an embodiment,” “an example
25 embodiment,” etc., indicate that the embodiment described may include a particular feature, structure, or characteristic, but every embodiment may not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is
30 within the knowledge of one skilled in the art to effect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described.

Embodiments of the invention may be implemented in hardware, firmware, software, or any combination thereof. Embodiments of the invention implemented in a computer

system may include one or more bus-based interconnects between components and/or one or more point-to-point interconnects between components. Embodiments of the invention may also be implemented as instructions carried by or stored on a machine-readable medium, which may be read and executed by one or more processors. A machine-readable
5 medium may be embodied as any device, mechanism, or physical structure for storing or transmitting information in a form readable by a machine (e.g., a computing device). For example, a machine-readable medium may be embodied as read only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices; mini- or micro-SD cards, memory sticks, electrical signals, and others.

10 In the drawings, specific arrangements or orderings of schematic elements, such as those representing devices, modules, instruction blocks and data elements, may be shown for ease of description. However, it should be understood by those skilled in the art that the specific ordering or arrangement of the schematic elements in the drawings is not meant to imply that a particular order or sequence of processing, or separation of processes, is
15 required. Further, the inclusion of a schematic element in a drawing is not meant to imply that such element is required in all embodiments or that the features represented by such element may not be included in or combined with other elements in some embodiments.

In general, schematic elements used to represent instruction blocks may be implemented using any suitable form of machine-readable instruction, such as software or firmware
20 applications, programs, functions, modules, routines, processes, procedures, plug-ins, applets, widgets, code fragments and/or others, and that each such instruction may be implemented using any suitable programming language, library, application programming interface (API), and/or other software development tools. For example, some embodiments may be implemented using Java, C++, and/or other programming languages.

25 Similarly, schematic elements used to represent data or information may be implemented using any suitable electronic arrangement or structure, such as a register, data store, table, record, array, index, hash, map, tree, list, graph, file (of any file type), folder, directory, database, and/or others.

30 Further, in the drawings, where connecting elements, such as solid or dashed lines or arrows, are used to illustrate a connection, relationship or association between or among two or more other schematic elements, the absence of any such connecting elements is not meant to imply that no connection, relationship or association can exist. In other words, some connections, relationships or associations between elements may not be shown in the drawings so as not to obscure the disclosure. In addition, for ease of illustration, a single

connecting element may be used to represent multiple connections, relationships or associations between elements. For example, where a connecting element represents a communication of signals, data or instructions, it should be understood by those skilled in the art that such element may represent one or multiple signal paths (e.g., a bus), as may be needed, to effect the communication.

Referring now to FIG. 1, a system 100 for establishing a secure communication session includes a client device 102, a server 104, and a network 106. In operation, the client device 102 initiates a request for a secure communication session with the server 104 over the network 106. To establish the secure communication session, the client device 102 and the server 104 perform a cryptographic key exchange, such as a Diffie-Hellman or a Rivest-Shamir-Adleman (RSA) key exchange, to generate a secret symmetric session key. The secret symmetric session key may then be used to encrypt and decrypt messages between the client device 102 and the server 104. To ensure a secure communication session, the various keys and other cryptographic functions generated by the client device 102 are done so within a security engine 110 of a system-on-a chip (SOC) 112 of the client device 102. The client device 102 maintains the keys in secrecy within a secure memory 114 of the security engine 110. For example, the security engine 110 may include a security key 150, as discussed below, used to sign and/or otherwise encrypt other keys and messages. In this way, the client device 102 and server 104 may establish a secure communication session across the network 106 using out-of-band (i.e., not application level), hardware security features of the client device 102. In the illustrative embodiments described herein, the secure communication session is a Secure Sockets Layer (SSL) communication session, but the system 100 and features described herein may be used to establish other types of secure communication sessions in other embodiments.

The client device 102 may be embodied as any type of computing device capable of communicating with the server 104 over the network 106. For example, the client device 102 may be embodied as a set-top box, a digital television, a smartphone, a tablet computer, a laptop computer, a mobile internet device (MID), a desktop computer, or other device capable of communicating with the server 104.

As discussed above, the client device 102 includes the SOC 112, which may be embodied as any type of system-on-a-chip device having various components and structures. In the illustrative embodiment of FIG. 1, the SOC 112 includes the security engine 110, a memory controller 116, a processor core 118, and a plurality of hardware peripherals 130, which are communicatively coupled to each other via a link 120. The link 120 may be

embodied as any type of interconnect such as a bus, point-to-point, or other interconnect capable of facilitating communication between the various components of the SOC 112. The hardware peripherals 130 may include any type of hardware peripheral component depending upon the intended functionality of the SOC 112. For example, in the illustrative embodiment, the hardware peripherals 130 include a demux 132 to separate audio and video content streams, video processing component(s) 134 to process video content, and audio processing component(s) 136 to process audio content. Of course, it should be appreciated that the hardware peripherals 130 of the SOC 112 have been simplified in the illustrative embodiment of FIG. 1 and that the SOC 112 may include additional, different, and/or greater detailed hardware peripherals 130, which are not illustrated in FIG. 1 for clarity of the disclosure.

The security engine 110 may be embodied as a security co-processor or processing circuitry separate from the processor core 118. The security engine 110 includes the security key 150 and the secure memory 114, which is accessible only by the security engine 110. The security engine 110 stores the security key 150, and other cryptographic keys as discussed below, in the secure memory 114. In the illustrative embodiment, the security key 150 is provisioned during the manufacturing of the SOC 112, but may be generated by the SOC 112 during operation in other embodiments. For example, in some embodiments, the security key 150 is based on blown fuses within the security engine 110 itself. Additionally or alternatively, the security engine 110 may include a key-generating module, such as a trusted platform module (TPM), to generate the security key 150. During use, the security engine 110 may use any number of security keys 150, which may be identical or different from each other.

In some embodiments, the client device 102 may include additional components and structures other than the SOC 112 depending on the type and intended use of the client device 102. For example, in the illustrative embodiment of FIG. 1, the client device 102 includes a system memory 160, a data storage 162, a communications output 164, and one or more input/output devices 166. The system memory 160 may be embodied as any type of main memory or data storage locations including, for example, dynamic random access memory devices (DRAM), synchronous dynamic random access memory devices (SDRAM), double-data rate synchronous dynamic random access memory device (DDR SDRAM), mask read-only memory (ROM) devices, erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM) devices, flash memory devices, and/or other volatile and/or non-volatile memory devices.

The data storage 162 may be embodied as any type of device or devices configured for the short-term or long-term storage of data such as, for example, memory devices and circuits, memory cards, hard disk drives, solid-state drives, or other data storage devices. The communications output 164 may be embodied as a simplified output or as various circuits and/or devices to facilitate, for example, communications with the server 104. For example, the communications output 164 (and/or communication circuitry within the SOC 112) may use any suitable communication protocol such as Ethernet (i.e. the IEEE 802.3 standard) or Wi-Fi® (i.e., the IEEE 802.11 standard), and/or other communication protocols or standards. Additionally, the input/output devices 166 may be embodied as any type of I/O device for interacting with the client device 102. For example, the I/O devices 166 may include output devices such as a display for displaying data on the client device 102, speakers for generating audio, and/or input devices such as a remote control receiver, a keyboard, a mouse, and/or the like.

The server 104 may be embodied as any type of data server capable of establishing a secure communication session with the client device 102. As such, the server 104 may include various hardware and software components typically found in a server for communicating, maintaining, and transferring data over a network. For example, the illustrative server 104 includes a processor 180, a memory 182, and communication circuitry 184, which may be similar to such components found in other data servers. For example, the processor 180 may be embodied as any type of processor capable of executing software/firmware, such as a microprocessor, digital signal processor, microcontroller, or the like, and may include one or more processing cores. The memory 182 may be embodied as any type of memory or data storage locations including, for example, dynamic random access memory devices (DRAM), synchronous dynamic random access memory devices (SDRAM), double-data rate synchronous dynamic random access memory device (DDR SDRAM), mask read-only memory (ROM) devices, erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM) devices, flash memory devices, and/or other volatile and/or non-volatile memory devices. The communication circuitry 184 may be embodied any type of circuitry and/or device to facilitate, for example, communications with the client device 102. For example, the communication circuitry 184 may support communication protocols such as Ethernet (i.e. the IEEE 802.3 standard) and/or Wi-Fi® (i.e., the IEEE 802.11 standard), and/or other communication protocols or standards.

The network 106 may be embodied as any number of various wired and/or wireless networks. For example, the network 106 may be embodied as or otherwise include a local area network (LAN), a wide area network (WAN), and/or a publicly accessible, global network such as the Internet. Additionally, the network 106 may include any number of
5 additional devices to facilitate communication between the client device 102 and the server 104. As discussed above, in the illustrative embodiment, the client device 102 and the server 104 establish a SSL communication session over the network 106. However, other types of secure communication sessions may be established in other embodiments.

Referring now to FIG. 2, as discussed in more detail below, the use of the security engine
10 110 of the client device 102 to perform the cryptographic functions and store keying data associated with the establishment of the secure communication session allows the system 100 to offer several different levels of security. The particular level of security used in the system 100 may depend upon various criteria such as the nature of the network 106, the importance of the data being transferred between the client device 102 and the server 104,
15 and/or the like. For example, one illustrative security scheme 200 includes three different levels of security as shown in FIG. 2. At level 0 security, the client device 102 is configured to protect the client private device key (i.e., the security key 150), which is used for encrypting, signing, and verification functions as discussed in more detail below.

At level 1 security, the client device 102 is configured to protect the session keys and
20 related keys used for data encryption. For example, if an RSA key exchange is performed, the pre-master key and the master key (i.e., the session key) may be stored in the secure memory 114 of the security engine 110 of the SOC 112. Additionally, in some embodiments as discussed below, the master key may be stored in an encrypted or wrapped form (e.g., encrypted using the security key 150). In embodiments in which a
25 Diffie-Hellman key exchange is used, the private Diffie-Hellman client key and/or shared secret key (i.e., the session key) may be stored in the secure memory 114 of the security engine 110 of the SOC 112. Again, in some embodiments, the private Diffie-Hellman client key and/or session key may be stored in an encrypted or wrapped form (e.g., encrypted using the security key 150).

30 Additionally, at level 2 security, the client device 102 may be configured to protect the data of the host application. For example, if the host application is being used to perform an e-commerce transaction, the bank account information used in such transaction may be encrypted using the security key 150 and stored in the secure memory 114. In this way, the bank account information is not available to the host application. Of course, it should

be appreciated that, in other embodiments, security schemes having more or fewer security levels may be used.

Referring now to FIG. 3, in operation, the client device 102 and the server 104 establish a secure communication session using the security engine 110 of the client device 102 to perform various cryptographic functions and store keying data therein. To do so, the client device 102 and server 104 may perform a handshake session as shown in the communication sequence 300 of FIG. 3. To establish the secure communication session, a security engine driver 302 of the security engine 110 communicates with a firmware of the security engine 110 and a client secure communication application 304 executed on the client device 102. The client secure communication application 304 also communicates with a corresponding server secure communication application 306 executed on the server 104.

The communication sequence 300 begins with block 310 in which the client secure communication application 304 sends a ClientHello message to the server secure communication application 306 to request the initiation of a secure communication session. As discussed above, the secure communication session is a SSL session in the illustrative embodiment. To facilitate the request, the security engine driver 302 communicates with security engine 110 of the SOC 112 to request a random nonce from the security engine 110 in block 312. The security engine 110 may use any suitable random number-generating algorithm to generate the random nonce in block 312. The nonce is embodied as random or pseudo-random number intended to be used only once in cryptographic functions to thwart, for example, replay attacked. In the illustrative embodiment, the random nonce includes a 32-bit timestamp and a 28-byte random number. Of course, other numeric formats for the random nonce may be used in other embodiments. Regardless, it should be appreciated that because the random nonce is generated in the security engine 110, the generation and storage of the random nonce is protected compared to generation of the nonce at, for example, the application level.

The random nonce generated in block 312 is included in the ClientHello message sent to the server secure communication application 306 in block 310. Additionally, the ClientHello message may include a list of cipher suites, compression methods, and other cryptographic protocols or algorithms from which the server 104 may make a selection for use in establishing the secure communication session. In response to the secure communication session request, the server secure communication application 306 sends a ServerHello message in block 314. The ServerHello message may be substantially similar

to the ClientHello message. For example, in the illustrative embodiment, the ServerHello message includes a server random nonce generated by the server 104. Additionally, the ServerHello message includes the selection(s) of the cryptographic protocols and/or other options made by the server 104 from the list included in the ClientHello message. The
5 ServerHello message completes the session initiation phase (Phase 1) of the illustrative handshake session.

In block 316, the server secure communication application 306 sends a server certificate to the client secure communication application 304. The server certificate, like the client certificate discussed below, is typically generated by a certification authority organization,
10 which acts as a third-party verifier of the authentication of the server 104. The server certificate may include unique identifier or number assigned to the server 104 by the certification authority organization to verify the server 104 to other devices on the network 106. As such, in block 318, the client device 102 may verify the server certificate. In some embodiments, the client device 102 verifies the server certificate using a public
15 certificate key issued by the certification authority organization. In such embodiments, the security engine 110 may store the public certificate key in the secure memory 114 in an unencrypted or encrypted state (e.g., using the security key 150).

To establish the secure communication session, the client device 102 and the server 104 perform a key exchange to establish a shared secret key (i.e., a master or session key) in
20 each of the client device 102 and server 104. The client device 102 and the server 104 may use any appropriate key exchange algorithm to effect the establishment of the shared secret. In the illustrative embodiment, the key exchange may be embodied as an RSA key exchange or a Diffie-Hellman key exchange. In embodiments wherein a RSA key exchange is used, the server secure communication application 306 performs a server RSA
25 key exchange in block 320. In such embodiments, the server 104 may generate a temporary RSA public/private key pair and send the RSA public key to the client device 102 in block 320. Such message may be signed by the server 104 and verified by the client device 102 using a public server key, which may be stored in the secure memory 114 as discussed above.

Alternatively, the server secure communication application 306 may perform a server
30 Diffie-Hellman key exchange in block 320. In such embodiments, the server 104 selects or otherwise generates the Diffie-Hellman global values (e.g., a prime number and a primitive root of the prime number), generates a private and public Diffie-Hellman server key, and sends the Diffie-Hellman global values and public Diffie-Hellman server key to the client

device 102 in block 320. Again, such message may be signed by the server 104 and verified by the client device 102 using a public server key.

5 In some embodiments, the sever secure communication application 306 may send a client certification request in block 322. If so, the request may specify the types of certificates accepted by the server 104 (e.g., the public key algorithm used), acceptable certificate authorities, and/or other certificate parameters. Subsequently, in block 324, the server secure communication application 306 sends a server completion message (a “ServerHelloDone” message) to the client secure communication application 304 to indicate that the server 104 has completed this phase of the handshake session. In the
10 illustrative embodiment, no parameters or other data are required for the server completion message. The ServerHelloDone message completes the server authentication and key exchange phase (Phase 2) of the illustrative handshake session.

After receiving the server completion message, the client secure communication application 304 initiates the client authentication and key exchange phase (Phase 3) of the
15 handshake session by sending the client certificate in block 326. As discussed above, the client certificate is typically generated by the certification authority organization and may include a unique identifier or number assigned to the client device 102 by the certification authority organization to verify the client device 102 to other devices on the network 106. In some embodiments, the client certificate may be stored in the secure memory 114 of the
20 security engine 110 of the SOC 112 in an unencrypted or encrypted state. Additionally, the client device 102 may use a private device key issued by the certification authority organization to sign the certificate prior to sending it to the server 104.

In block 328, the client secure communication application 304 performs a client key exchange. Again, the client device 102 and the server 104 may use any appropriate key
25 exchange algorithm to effect the establishment of the shared secret as discussed above. In embodiments wherein an RSA key exchange is used, the security engine 110 of the SOC 112 of the client device 102 generates a random pre-master key in block 330. Illustratively, the pre-master key is embodied as a 48-byte random number, but other numeric formats may be used in other embodiments. In block 332, the pre-master key generated in block 330 is encrypted or otherwise wrapped using the server public key
30 provided by the server in server authentication and key exchange phase (Phase 2). The encrypted pre-master key may be stored in the secure memory 114 of the security engine 110 of the SOC 112 and sent to the server 104 in block 328.

Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 generates, in block 334, a private Diffie-Hellman client key and a public Diffie-Hellman client key using the Diffie-Hellman global values received from the server 104 in block 320. The private Diffie-Hellman client key may be embodied as a random value generated by the security engine 110, while the public Diffie-Hellman client key is generated by the security engine 110 using the Diffie-Hellman global values received from the server 104. The private Diffie-Hellman client key may be stored in the secure memory 114 of the security engine 110. Of course, in some embodiments, the client device 102 may generate the Diffie-Hellman global values in block 334 and send such global values to the server 104 in block 328 to allow the server 104 to generate the public Diffie-Hellman server key based thereon. Regardless, in block 336, the security engine 110 of the SOC 112 signs the public Diffie-Hellman client key (and Diffie-Hellman global values if generated by the client device 102) in block 336 using the security key 150 or other private client key of the security engine 110. The signed Diffie-Hellman parameters may be further encrypted using the public server key and sent to the server 104 in block 328.

In some embodiments, the client secure communication application 304 may send a client certification verification message to the sever secure communication application 306 in block 338. To do so, the security engine 110 generates a hash code based on the preceding message and signs the hash code using the security key 150 of the security engine 110 in block 340. The client device 102 sends the signed hash code to the server 104 in block 338 as verification of the preceding message. It should be appreciated that such client certification verification messages may be used subsequent to any message sent to the server 104 from the client device 102 to provide an added level of security and verification to the secure communication session. The client certification verification message in block 338 completes the client authentication and key exchange phase (Phase 3) of the illustrative handshake session.

In block 342, the client secure communication application 304 sends a change cipher specification message to the server secure communication application 306 to inform the server 104 that subsequent communications will use the agreed-upon cipher (e.g., the generated session key). In block 344, the security engine 110 of the client device 102 generates a session key (i.e., the “master” key). In embodiments wherein an RSA key exchange is used, the security engine 110 generates the session key as a function of the pre-master key generated in block 330. To do so, the security engine 110 calculates a hash

function of the pre-master key, the client random nonce generated in block 312, and the server random nonce received in block 314. Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 generates the session key as a function of the Diffie-Hellman global values, the public Diffie-Hellman server key, and the private Diffie-Hellman client key. As discussed above, the session key is stored in the secure memory 114 of the security engine 110.

In block 346, the security engine 110 generates a hash code of the session key, which may include additional padding depending on the type of hash function used. The hash code of the session key is sent to the server 104 for verification in a client-finished message in block 348. The hash code of the session key may be encrypted by the security engine 110 using the public server key as discussed above.

In response to the client-finished message, the server 104 sends a change cipher specification message that acknowledges the use of the agreed-upon cipher (e.g., the session key) in block 350. The server 104 also sends a server-finished message in block 352 that includes a similar hash code of the session key for verification by the client device 102. Assuming that the client device 102 and the server 104 verify the hash code of the session key, the handshake session is complete and each of the client device 102 and server 104 have a shared secret session key that is used to encrypt and decrypt subsequent messages. Again, it should be appreciated that the security engine 110 of the SOC 112 of the client device 102 is used for all cryptographic functions and storage of sensitive keying data to provide hardware-based protection of the cryptographic keys and certificate keys used during the communication sequence 300.

Referring now to FIG. 4, in use, the client device 102 may execute a method 400 to establish a secure communication session with the server 104. The method 400 begins with block 402 in which the security engine 110 of the SOC 112 of the client device 102 is provisioned. To do so, in one embodiment, the security engine 110 receives a client device certificate, a private client device key, and a public certification key. The client device certificate, the private client device key, and the public certification key are typically generated by the certification authority organization, which acts as a third-party verifier of the authentication of the client device 102 as discussed above. The client device certificate may include a unique device identifier or number assigned to the client device 102 by the certification authority organization to verify the client device 102 to other devices on the network 106. The private client device key may be used by the client device 102 to sign the client device certificate so as to authenticate the client device 102 to other devices as

discussed in more detail below. Conversely, the public certification key may be used by the client device 102 to verify certification of other devices on the network 106 by the certification authority organization.

5 The security engine 110 encrypts the private client device key using the security key 150 and stores the encrypted private client device key in the secure memory 114. The security engine 110 may also store the client device certificate and/or the public certification key in the secure memory 114. Additionally, in some embodiments, the security engine 110 may encrypt the client device certificate and/or the public certification key using the security key 150 stored in the security engine 110.

10 After the security engine 110 has been provisioned in block 402, the client device 102 determines whether to establish a secure communication session (e.g., an SSL session) with the server 104 in block 404. If so, in block 406, the security engine 110 generates a random nonce value. As discussed above, the security engine 110 may use any suitable random number-generating algorithm to generate the random nonce. In block 408, the
15 client device 102 sends a request (a ClientHello message) to initiate the secure communication session to the server 104. The request includes the random nonce generated in block 406 along with a list of cipher protocols, compression methods, and/or other cryptographic choices from which the server 104 may select.

In block 410, the client device 102 completes the server authentication and server key
20 exchange. In so doing, the client device 102 may receive a corresponding ServerHello message including a server random nonce, the server's 104 public key, and the server's 104 selection of cryptographic choices presented in the ClientHello message. As discussed above, the server random nonce, along with the client random nonce, is used to generate the session key. As such, the security engine 110 may store the server random nonce in the
25 secure memory 114. Additionally, in some embodiments, the security engine 110 may store the server certificate and/or other keying data in the secure memory 114. For example, in embodiments wherein an RSA key exchange is used, the security engine 110 may store the public RSA key received from the server in the secure memory 114. Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the
30 security engine 110 may store the Diffie-Hellman global values and/or public Diffie-Hellman server key in the secure memory 114.

In block 414, the client 104 determines whether the server 104 is successfully authenticated. If not, the method 400 loops back to block 404 in which the client device 102 may reattempt to establish a secure communication session with the server 104.

However, if the server 104 is successfully authenticated, the method 400 advances to block 416 in which the client device 102 sends the server 104 the client certificate. If the client certificate has been encrypted (e.g., using the secure key 150), the security engine 110 decrypts the client certificate and signs the client certificate using the private client device key.

In block 418, the client 104 completes the client key exchange using the security engine 110 to maintain the security of the keying functions. For example, if a RSA key exchange was selected, the security engine 110 generates the pre-master key and encrypts the pre-master key using the server public key received in block 410 prior to sending the encrypted pre-master key to the server 104 in block 420. Alternatively, if a Diffie-Hellman key exchange was selected, the security engine 110 generates the public and private Diffie-Hellman client keys using the Diffie-Hellman global values received from the server 104 in block 410. The security engine 110 may sign the public Diffie-Hellman client key using the security key 150 or the public client device key provisioned in block 402. The client device 102 sends the signed public Diffie-Hellman client key to the server 104 in block 422. The keys and related keying data generated during the client key exchange may be stored in the secure memory 114 in an encrypted state (using the security key 150) or an unencrypted state.

In block 424, the client device 102 determines whether the client device 102 has been successfully authenticated by the server 104. If not, the method 400 loops back to block 404 in which the client device 102 may reattempt to establish a secure communication session with the server 104. However, if the client device 102 is successfully authenticated, the method 400 advances to block 426 in which the client device 102 confirms the cipher suite with the server 104 by informing the server 104 that subsequent messages will use the agreed-upon cryptographic protocols. In so doing, the security engine 110 may generate the master or session key. To do so, in embodiments wherein an RSA key exchange is used, the security engine 110 calculates a hash function of the pre-master key, the client random nonce generated in block 406, and the server random nonce received in block 410. Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 generates the session key as a function of the Diffie-Hellman global values, the public Diffie-Hellman server key, and the private Diffie-Hellman client key. Once generated, the security engine 110 of the SOC 112 may store the session key in the secure memory 114 of the security engine 110. In some embodiments,

the session key may be encrypted using the security key 150 while stored in the secure memory 114.

5 In block 428, the security engine 110 generates a hash function of the session key, which is sent to the server 104 for verification in a client finished message. Again, the hash code of the session key may be encrypted by the security engine 110 using the public server key as discussed above. In response, the server 104 confirms the cipher suite with the client device 102 to acknowledge the agreed-upon cipher (e.g., the session key). The server 104 also sends a server finished message that includes a similar hash code of the session key for verification by the client device 102. Assuming that the client device 102 and the server 104 verify the hash code of the session key, the handshake session is complete and each of the client device 102 and server 104 have a shared secret session key that is used to encrypt and decrypt subsequent messages.

10 While the disclosure has been illustrated and described in detail in the drawings and foregoing description, such an illustration and description is to be considered as exemplary and not restrictive in character, it being understood that only illustrative embodiments have been shown and described and that all changes and modifications consistent with the disclosure and recited claims are desired to be protected.

CLAIMS:

1. A system-on-a-chip apparatus comprising:
a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, the security engine to:
5 generate a random nonce for initiating a request for a secure communication session with a server over a network using the nonce;
perform a cryptographic key exchange with the server to generate a symmetric session key to encrypt messages sent to the server and decrypt messages received from the server during the secure communication session;
10 store the session key in the secure memory,
the system-on-a-chip to establish the secure communication session with the server over the network using the session key.
2. The system-on-a-chip apparatus of claim 1, wherein the system-on-a-chip
15 to establish a Secure Sockets Layer communication session with the server over the network using the session key.
3. The system-on-a-chip apparatus of claim 1, wherein the security engine to receive a server nonce from the server in response to the request for the secure communication session, the response message including a server nonce and store the server nonce in the secure
20 memory.
4. The system-on-a-chip apparatus of claim 1, wherein the security engine to receive a server certificate from the server and store the server certificate in the secure memory.
25
5. The system-on-a-chip apparatus of claim 1, wherein the security engine to perform a Rivest-Shamir-Adleman key exchange with the server to generate the symmetric session key.
- 30 6. The system-on-a-chip apparatus of claim 5, wherein the security engine to generate a pre-master key, encrypt the pre-master key using a security key of the security engine, and send the encrypted pre-master key to the server.

7. The system-on-a-chip apparatus of claim 6, wherein the security engine to wrap the pre-master key using a server public key and store the wrapped pre-master key in the secure storage.
- 5 8. The system-on-a-chip apparatus of claim 6, wherein the security engine to generate the session key as a function of the pre-master key.
9. The system-on-a-chip apparatus of claim 8, wherein the security engine to calculate a hash function as a function of the random nonce generated by the security engine and
10 a nonce received from the server.
10. The system-on-a-chip apparatus of claim 5, wherein the security engine to receive a public Rivest-Shamir-Adleman server key from the server and store the public Rivest-Shamir-Adleman server key in the secure memory.
15
11. The system-on-a-chip apparatus of claim 1, wherein the security engine to perform a Diffie-Hellman key exchange with the server to generate the symmetric session key.
12. The system-on-a-chip apparatus of claim 11, wherein the security engine
20 to generate a public Diffie-Hellman client key and a private Diffie-Hellman client key, sign the public Diffie-Hellman client key using a security key of the security engine, and send the signed public Diffie-Hellman key to the server.
13. The system-on-a-chip apparatus of claim 12, wherein the security engine
25 to receive a public Diffie-Hellman server key from the server and generate the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.
14. The system-on-a-chip apparatus of claim 13, wherein the security engine
30 to use the session key to encrypt a subsequent message sent from the client device to the server.
15. The system-on-a-chip apparatus of claim 11, wherein the security engine to receive Diffie-Hellman global values and a public Diffie-Hellman server key from the server and store at least one of the Diffie-Hellman global values and the public Diffie-Hellman server key in the secure storage.

16. A method comprising:
generating a random nonce in a security engine of a system-on-a-chip of a client device;
initiating, using the client device, a request for a secure communication session
5 with a server over a network, the request including the random nonce;
performing a cryptographic key exchange, using the security engine of the system-on-a-chip, with the server to generate a symmetric session key to encrypt messages sent to the server and decrypt messages received from the server during the secure communication session;
10 storing the session key in a secure memory of the security engine of the system-on-a-chip; and
establishing, using the client device, the secure communication session with the server using the session key.
17. The method of claim 16, wherein initiating a request for a secure communication session comprises initiating a request for a Secure Sockets Layer communication session.
18. The method of claim 16, further comprising:
20 receiving a response message from the server in response to the request for a secure communication session, the response message including a server nonce, and
storing the server nonce in the secure memory of the security engine of the system-on-a-chip.
19. The method of claim 16, wherein initiating a request for a secure communication session comprises sending a ClientHello message, including the nonce, to the server; and further comprising:
25 receiving a ServerHello message from the server, the ServerHello message including a server nonce; and
30 storing the server nonce in the secure memory of the security engine of the system-on-a-chip.

20. The method of claim 16, further comprising receiving a server certificate from the server and storing the server certificate in the secure memory of the security engine of the system-on-a-chip of the client device.
- 5 21. The method of claim 16, wherein performing the cryptographic key exchange with the server comprises performing a Rivest-Shamir-Adleman key exchange, using the security engine of the system-on-a-chip, with the server.
- 10 22. The method of claim 21, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises:
generating a pre-master key in the security engine;
encrypting the pre-master key using a security key of the security engine; and
sending the encrypted pre-master key to the server.
- 15 23. The method of claim 22, further comprising:
wrapping the pre-master key in the security engine of the system-on-a-chip using a server public key, and
storing the wrapped pre-master key in the secure storage of the security engine of the system-on-a-chip.
- 20 24. The method of claim 22, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises generating the session key in the security engine of the system-on-a-chip as a function of the pre-master key.
- 25 25. The method of claim 24, wherein generating the session key in the security engine comprises calculating, using the security engine of the system-on-a-chip, a hash function as a function of the random nonce generated by the security engine and a nonce received from the server.
- 30 26. The method of claim 21, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises:
receiving a public Rivest-Shamir-Adleman server key from the server; and
storing the public Rivest-Shamir-Adleman server key in the secure memory of the security engine of the system-on-a-chip.

27. The method of claim 16, wherein performing the cryptographic key exchange with the server comprises performing a Diffie-Hellman key exchange, using the security engine of the system-on-a-chip, with the server.

5

28. The method of claim 27, wherein performing a Diffie-Hellman key exchange with the server comprises:

generating, in the security engine of the system-on-a-chip, a public Diffie-Hellman client key and a private Diffie-Hellman client key;

10 signing the public Diffie-Hellman client key using a security key of the security engine of the system-on-a-chip; and

sending the signed public Diffie-Hellman key to the server.

29. The method of claim 28, wherein performing a Diffie-Hellman key
15 exchange with the server comprises:

receiving a public Diffie-Hellman server key from the server;

generating, in the security engine of the system-on-a-chip, the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

20 30. The method of claim 29, wherein performing a Diffie-Hellman key exchange with the server comprises using the session key to encrypt a subsequent message sent from the client device to the server.

31. The method of claim 27, wherein performing a Diffie-Hellman key exchange with the server comprises:

receiving Diffie-Hellman global values and a public Diffie-Hellman server key from the server, and

5 storing at least one of the Diffie-Hellman global values and the public Diffie-Hellman server key in the secure storage of the security engine of the system-on-a-chip.

32. The method of claim 16, further comprising:

retrieving a client certificate stored on the client device;

10 signing a client certificate using a security key stored in a secure memory of the security engine of the system-on-a-chip; and

sending the client certificate to the server.

33. The method of claim 16, further comprising:

15 generating, in the security engine of the system-on-a-chip, a hash code of a preceding message sent from the client to the server;

signing the hash code using a security key stored in a secure memory of the security engine; and

20 sending a client certificate verification message to the server, the client certificate verification message including the signed hash code.

34. The method of claim 16, wherein establishing the secure communication session comprises:

generating, in the security engine, a hash code as a function of the session key;

and

5 sending a client completion message that includes the hash code to the server to indicate the client has completed an initial handshake procedure.

35. A source device comprising:

10 a system-on-a-chip having a security engine, the system-on-a-chip including a plurality of instructions that when executed results in the system-on-a-chip performing the method of claim 16-34.

36. One or more machine readable media comprising a plurality of instructions that in response to being executed by a client device result in the client device
15 performing the method of claims 16-34.

37. A method comprising:

generating a random nonce in a security engine of a system-on-a-chip of a client device;

20 initiating, using the client device, a request for a Secure Sockets Layer communication session with a server over a network, the request including the random nonce;

performing a cryptographic key exchange, using the security engine of the system-on-a-chip, with the server to generate a symmetric session key to encrypt messages sent to the server and decrypt messages received from the server during the Secure Sockets Layer
25 communication session;

storing the session key in a secure memory of the security engine of the system-on-a-chip; and

generating, in the security engine, a hash code as a function of the session key;

and

30 sending a client completion message to the server that includes the hash code to indicate the client has completed an initial handshake procedure.

38. The method of claim 37, wherein performing the cryptographic key exchange with the server comprises performing a Rivest-Shamir-Adleman key exchange, using the security engine of the system-on-a-chip, with the server.

5 39. The method of claim 38, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises:

generating a pre-master key in the security engine;
encrypting the pre-master key using a security key of the security engine; and
sending the encrypted pre-master key to the server.

10

40. The method of claim 39, further comprising:
wrapping the pre-master key in the security engine using a server public key, and
storing the wrapped pre-master key in the secure storage of the security engine of
the system-on-a-chip.

15

41. The method of claim 39, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises generating the session key in the security engine of the system-on-a-chip as a function of the pre-master key.

20

42. The method of claim 41, wherein generating the session key in the security engine comprises calculating, using the security engine of the system-on-a-chip, a hash function as a function of the random nonce generated by the security engine and a nonce received from the server.

25

43. The method of claim 37, wherein performing the cryptographic key exchange with the server comprises performing a Diffie-Hellman key exchange, using the security engine of the system-on-a-chip, with the server.

30

44. The method of claim 43, wherein performing a Diffie-Hellman key exchange with the server comprises:
generating, in the security engine of the system-on-a-chip, a public Diffie-Hellman client key and a private Diffie-Hellman client key;
signing the public Diffie-Hellman client key using a security key of the security engine of the system-on-a-chip; and

sending the signed public Diffie-Hellman key to the server.

45. The method of claim 44, wherein performing a Diffie-Hellman key exchange with the server comprises:

- 5 receiving a public Diffie-Hellman server key from the server;
 generating, in the security engine of the system-on-a-chip, the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

46. A source device comprising:

- 10 a system-on-a-chip having a security engine, the system-on-a-chip including a plurality of instructions that when executed results in the system-on-a-chip performing the method of claim 37-45.

47. One or more machine readable media comprising a plurality of
15 instructions that in response to being executed by a client device result in the client device performing the method of claims 37-45.

1/4

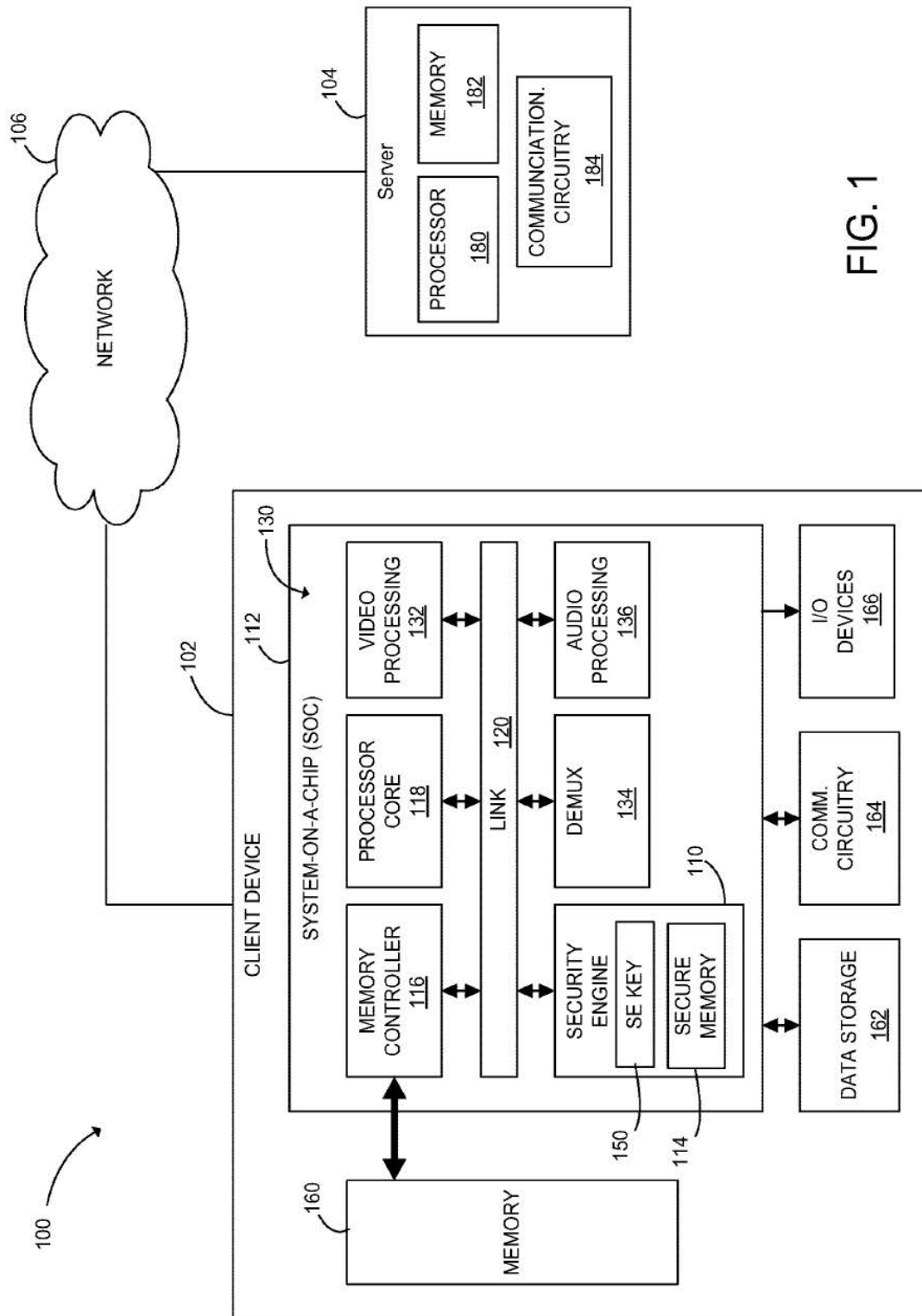


FIG. 1

2/4

200

LEVEL 0	PROTECTION OF CLIENT PRIVATE DEVICE KEY USED FOR SIGNING & VERIFICATION	
LEVEL 1	PROTECTION OF SESSION KEYS USED FOR DATA ENCRYPTION	
	RSA KEY EXCHANGE	DIFFIE-HELLMAN KEY EXCHANGE
	PROTECTION OF PRE-MASTER KEY	PROTECTION OF CLIENT PRIVATE DH KEY
LEVEL 2	PROTECTION OF APPLICATION DATA	

FIG. 2

3/4

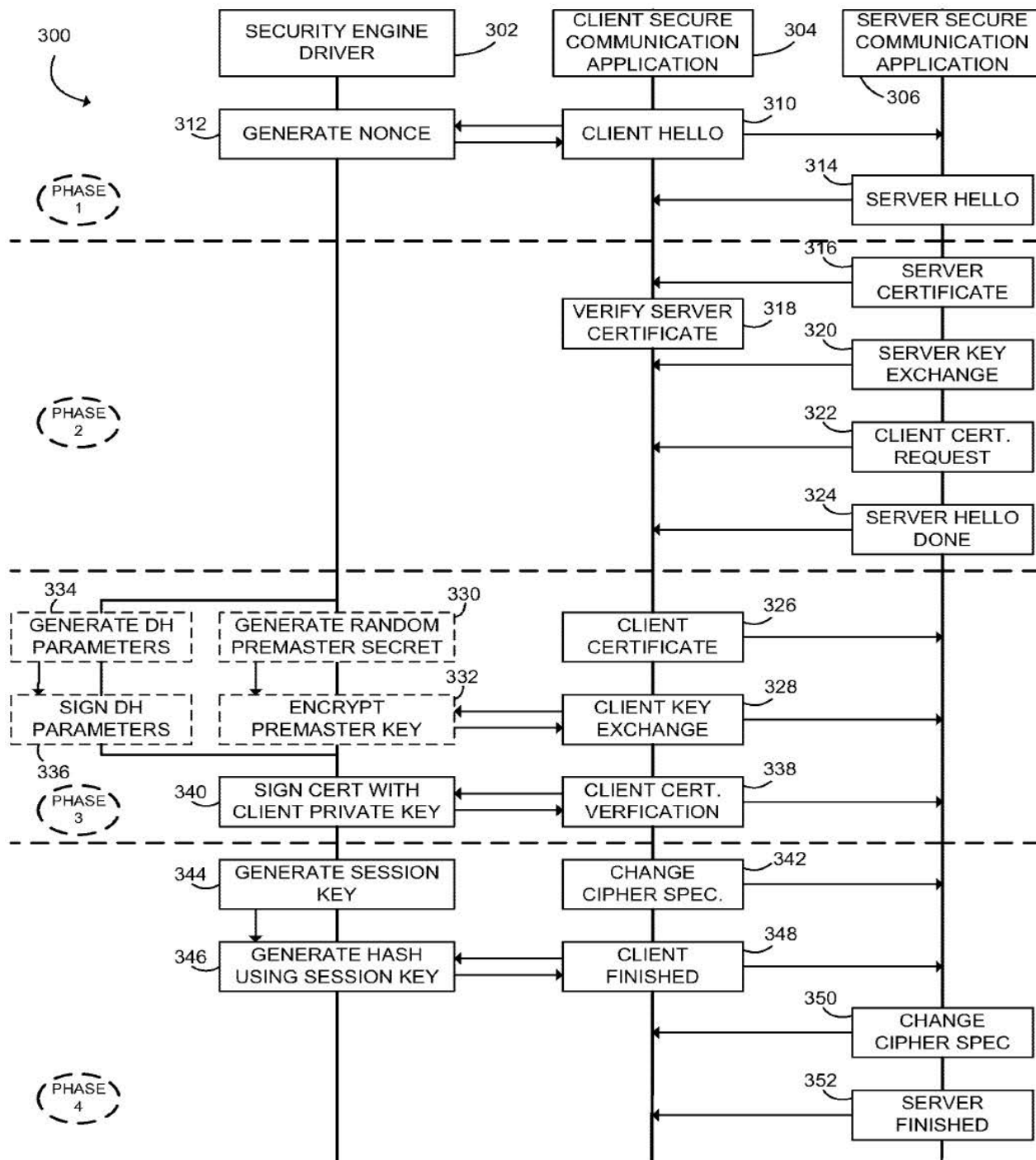


FIG. 3

4/4

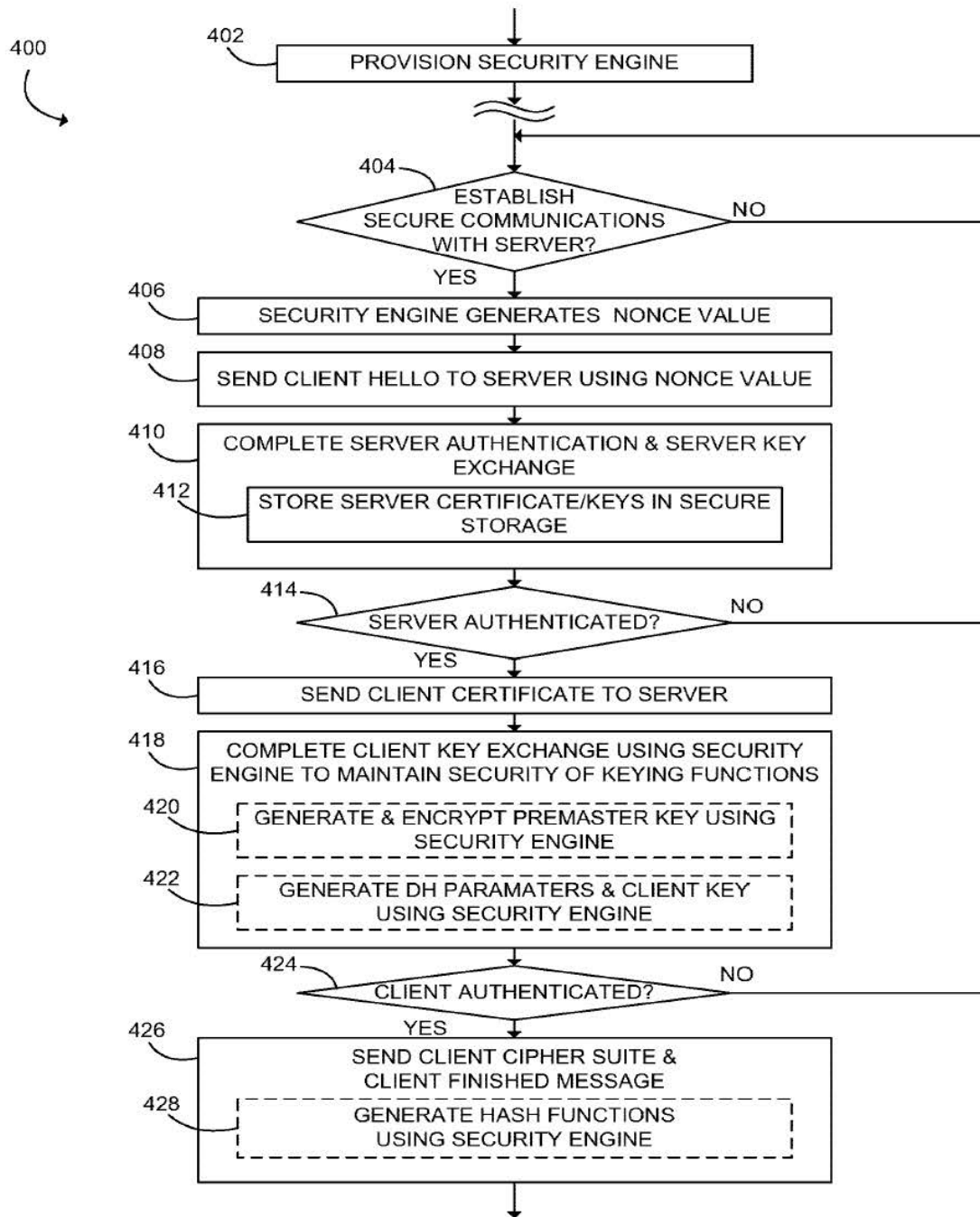


FIG. 4

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875				Application or Docket Number 13/997,412		Filing Date 04/03/2014		☐ To be Mailed	
ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO									
APPLICATION AS FILED – PART I									
(Column 1)		(Column 2)							
FOR		NUMBER FILED	NUMBER EXTRA			RATE (\$)	FEE (\$)		
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))		N/A	N/A			N/A			
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))		N/A	N/A			N/A			
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))		N/A	N/A			N/A			
TOTAL CLAIMS (37 CFR 1.16(i))		minus 20 =	*			X \$	=		
INDEPENDENT CLAIMS (37 CFR 1.16(h))		minus 3 =	*			X \$	=		
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))		If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).							
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))									
						TOTAL			
APPLICATION AS AMENDED – PART II									
(Column 1)		(Column 2)		(Column 3)					
AMENDMENT	06/24/2013	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	* 24	Minus	** 24	= 0	X \$80 =		0	
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0	X \$420 =		0	
	☐ Application Size Fee (37 CFR 1.16(s))								
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
							TOTAL ADD'L FEE		0
(Column 1)		(Column 2)		(Column 3)					
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	*	Minus	**	=	X \$		=	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X \$		=	
	☐ Application Size Fee (37 CFR 1.16(s))								
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
							TOTAL ADD'L FEE		
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.									

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

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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

U.S. APPLICATION NUMBER NO.	FIRST NAMED APPLICANT	ATTY. DOCKET NO.
13/997,412	Hormuzd M. Khosravi	P41624US
73486 Barnes & Thornburg LLP (Intel) c/o CPA Global P.O. Box 52050 Minneapolis, MN 55402		INTERNATIONAL APPLICATION NO. PCT/US11/65069
		L.A. FILING DATE 12/15/2011
		PRIORITY DATE

CONFIRMATION NO. 1045
371 FORMALITIES LETTER



Date Mailed: 07/23/2013

**NOTIFICATION OF MISSING REQUIREMENTS UNDER 35 U.S.C. 371
IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US)**

The following items have been submitted by the applicant or the IB to the United States Patent and Trademark Office as a Designated Office (37 CFR 1.494):

- Copy of the International Application filed on 06/24/2013
- Copy of the International Search Report filed on 06/24/2013
- Oath or Declaration filed on 06/24/2013
- U.S. Basic National Fees filed on 06/24/2013

The following items **MUST** be furnished within the period set forth below in order to complete the requirements for acceptance under 35 U.S.C. 371:

- Oath or declaration of the inventors, in compliance with 37 CFR 1.497(a) and (b), identifying the application by the International application number and international filing date. The current oath or declaration does not comply with 37 CFR 1.497(a) and (b) in that it:
 - is not executed in accordance with either 37 CFR 1.66 or 37 CFR 1.68.
 - Inventor Kabir has not signed OATH

ALL OF THE ITEMS SET FORTH ABOVE MUST BE SUBMITTED WITHIN TWO (2) MONTHS FROM THE DATE OF THIS NOTICE OR BY 32 MONTHS FROM THE PRIORITY DATE FOR THE APPLICATION, WHICHEVER IS LATER. FAILURE TO PROPERLY RESPOND WILL RESULT IN ABANDONMENT.

The time period set above may be extended by filing a petition and fee for extension of time under the provisions of 37 CFR 1.136(a).

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
<https://portal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html>

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

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

BRIAN A HARDEN

Telephone: (703) 756-1815

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 13/997,412				
APPLICATION AS FILED - PART I										
(Column 1)		(Column 2)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY				
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)			
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	280			
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A	480			
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	720			
TOTAL CLAIMS (37 CFR 1.16(i))	24	minus 20 = *	4			x 80 =	320			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3	minus 3 = *				x 420 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL		TOTAL	1800			
APPLICATION AS AMENDED - PART II										
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY		
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=		x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=		x	=
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
TOTAL ADD'L FEE								TOTAL ADD'L FEE		
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x	=		x	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x	=		x	=
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
TOTAL ADD'L FEE								TOTAL ADD'L FEE		
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.										

MULTIPLE DEPENDENT CLAIM FEE CALCULATION SHEET Substitute for Form PTO-1360 (For use with Form PTO/SB/06)							Application Number 13997412		Filing Date	
							Applicant(s) Hormuzd Khosravi			
							* May be used for additional claims or amendments			
CLAIMS	AS FILED		AFTER FIRST AMENDMENT		AFTER SECOND AMENDMENT			*	*	*
	Indep	Depend	Indep	Depend	Indep	Depend				
1	1		---	---						
2		1	---	---						
3		1	---	---						
4		1	---	---						
5		1	---	---						
6		1	---	---						
7		1	---	---						
8		1	---	---						
9		1	---	---						
10		1	---	---						
11		1	---	---						
12		1	---	---						
13		1	---	---						
14		1	---	---						
15		1	---	---						
16	1		---	---						
17		1	---	---						
18		1	---	---						
19		1	---	---						
20		1	---	---						
21		1	---	---						
22		1	---	---						
23		1	---	---						
24		1	---	---						
25		1	---	---						
26		1	---	---						
27		1	---	---						
28		1	---	---						
29		1	---	---						
30		1	---	---						
31		1	---	---						
32		1	---	---						
33		1	---	---						
34		1	---	---						
35		29	---	---						
36		29	---	---						
37	1		---	---						
38		1	---	---						
39		1	---	---						
40		1	---	---						
41		1	---	---						
42		1	---	---						
43		1	---	---						
44		1	---	---						
45		1	---	---						
46		9	---	---						
47		9	---	---						
48			1							
49				1						
50				1						
Total Indep	3		3		0					
Total Depend	116	←	21	←	0	←				
Total Claims	119		24		0					

51				1		
52				1		
53				1		
54				1		
55				1		
56			1			
57				1		
58				1		
59				1		
60				1		
61				1		
62				1		
63				1		
64			1			
65				1		
66				1		
67				1		
68				1		
69				1		
70				1		
71				1		
72						
73						
74						
75						
76						
77						
78						
79						
80						
81						
82						
83						
84						
85						
86						
87						
88						
89						
90						
91						
92						
93						
94						
95						
96						
97						
98						
99						
100						

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)

Approved for use through 07/31/2012. OMB 0651-0031

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13997412	
	Filing Date		2013-06-24	
	First Named Inventor	Hormuzd M. Khosravi		
	Art Unit	UNK		
	Examiner Name	UNK		
	Attorney Docket Number	P41624US/45631-225521		

U.S. PATENTS							Remove	
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1							
If you wish to add additional U.S. Patent citation information please click the Add button.							Add	
U.S. PATENT APPLICATION PUBLICATIONS							Remove	
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1	20110231923	A1	2011-09-22	Bollay et al.			
	2	20100299525	A1	2010-11-25	Shah et al.			
	3	20080037793	A1	2008-02-14	Buer			
	4	20050213768	A1	2005-09-29	Durham et al.			
If you wish to add additional U.S. Published Application citation information please click the Add button.							Add	
FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13997412	
	Filing Date		2013-06-24	
	First Named Inventor	Hormuzd M. Khosravi		
	Art Unit	UNK		
	Examiner Name	UNK		
	Attorney Docket Number	P41624US/45631-225521		

	1	2013089725	WO	A1	2013-06-20	Intel Corporation		☐
--	---	------------	----	----	------------	-------------------	--	--------------------------

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

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	International Search Report and Written Opinion received for International Application No. PCT/US2011/065069, mailed August 30, 2012, 11 pages.	☐
	2	"Transport Layer Security," Wikipedia, The Free Encyclopedia, available: [http://en.wikipedia.org/w/index.php?title=Transport_Layer_Security&oldid=464220022], edited December 5, 2011, 19 pages.	☐
	3	"HTTP Secure," Wikipedia, The Free Encyclopedia, available: [http://en.wikipedia.org/w/index.php?title=HTTP_Secure&oldid=465003157], edited December 9, 2011, 6 pages.	☐

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

EXAMINER SIGNATURE

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

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	13997412
	Filing Date	2013-06-24
	First Named Inventor	Hormuzd M. Khosravi
	Art Unit	UNK
	Examiner Name	UNK
	Attorney Docket Number	P41624US/45631-225521

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/CHRISTOPHER A. SINGH/	Date (YYYY-MM-DD)	2013-07-26
Name/Print	CHRISTOPHER A. SINGH	Registration Number	61236

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

Privacy Act Statement

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

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

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



- (51) **International Patent Classification:**
H04L 9/14 (2006.01) *H04L 9/32* (2006.01)
- (21) **International Application Number:**
PCT/US2011/065069
- (22) **International Filing Date:**
15 December 2011 (15.12.2011)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (71) **Applicant (for all designated States except US):** **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, California 95052 (US).
- (72) **Inventors; and**
- (75) **Inventors/Applicants (for US only):** **KHOSRAVI, Hormuzd M.** [IN/US]; 4816 NW 166th Avenue, Portland, Oregon 97229 (US). **EPP, Edward C.** [US/US]; 2111 NE 25th Avenue, Hillsboro, Oregon 97124 (US). **KABIR, Farhana** [US/US]; 20021 SE 3rd Circle, Camas, Washington 98607 (US).
- (74) **Agent:** **KELLETT, Glen M.**; Barnes & Thornburg, LLP, c/o CPA Global, P.O. Box 52050, Minneapolis, Minnesota 55402 (US).
- (81) **Designated States (unless otherwise indicated, for every kind of national protection available):** AE, AG, AL, AM,

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

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

Declarations under Rule 4.17:

— of inventorship (Rule 4.17(iv))

Published:

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

(54) **Title:** METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE

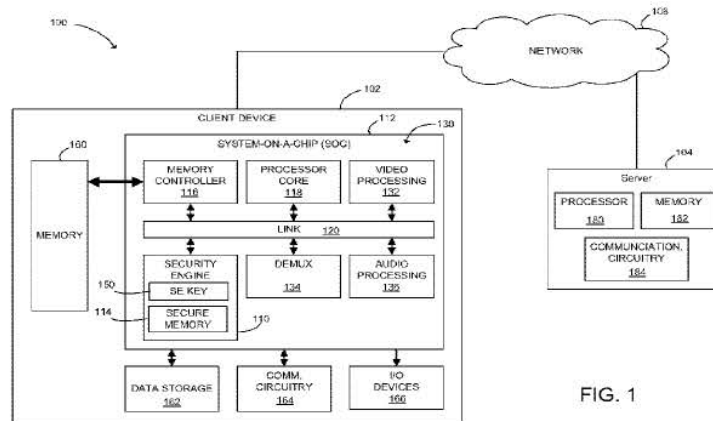


FIG. 1

(57) **Abstract:** A method, device, and system for establishing a secure communication session with a server includes initiating a request for a secure communication session, such as a Secure Sockets Layer (SSL) communication session with a server using a nonce value generated in a security engine of a system-on-a-chip (SOC) of a client device. Additionally, a cryptographic key exchange is performed between the client and the server to generate a symmetric session key, which is stored in a secure storage of the security engine. The cryptographic key exchange may be, for example, a Rivest-Shamir-Adleman (RSA) key exchange or a Diffie-Hellman key exchange. Private keys and other data generated during the cryptographic key exchange may be generated and/or stored in the security engine.

**METHOD AND DEVICE FOR SECURE COMMUNICATIONS
OVER A NETWORK USING A HARDWARE SECURITY ENGINE**

BACKGROUND

5 Cryptographic communication protocols are used to establish a secure communication session between computing devices over an untrusted network or communication link. One commonly used cryptographic communication protocol is the Secure Sockets Layer (SSL) protocol. The SSL protocol, and the related Transport Layer Security (TLS) protocol, is used for many different types of secure communication sessions including, for example, secure web-browsing, ecommerce, secure upgrades, and other secure communication sessions between two computing devices on an untrusted network such as the Internet. Other communication protocols may utilize the SSL/TLS protocol to provide the underlying security. For example, the Hypertext Transfer Protocol Secure (HTTPS) uses SSL/TLS for encryption of messages between devices. Typically, the cryptographic security offered by the SSL/TLS protocols is done so in-band and performed at the software application level.

15 Some computing and electronic devices utilize system-on-a-chip (SOC) designs due to their relatively small footprint. SOC devices are integrated circuits that incorporate various components, in addition to the processing core, of electronic systems on a single die. For example, an SOC may include a processor core, memory controller, video components, audio components, and/or communication components on a single chip.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention described herein is illustrated by way of example and not by way of limitation in the accompanying figures. For simplicity and clarity of illustration, elements illustrated in the figures are not necessarily drawn to scale. For example, the dimensions of some elements may be exaggerated relative to other elements for clarity. Further, where considered appropriate, reference labels have been repeated among the figures to indicate corresponding or analogous elements.

25 FIG. 1 is a simplified block diagram of at least one embodiment of a system for establishing a secure communication session between a client device having a system-on-a-chip (SOC) and a server over a network;

30 FIG. 2 is a block diagram of at least one embodiment of a security scheme for the system of FIG. 1;

FIG. 3 is a simplified sequence diagram of at least one embodiment of a communication sequence of the client device and server of FIG. 1 to establish a secure communication session; and

5 FIG. 4 is a simplified flow diagram of at least one embodiment of a method for establishing a secure communication session executed by the client device of FIG. 1.

DETAILED DESCRIPTION OF THE DRAWINGS

While the concepts of the present disclosure are susceptible to various modifications and alternative forms, specific exemplary embodiments thereof have been shown by way of example in the drawings and will herein be described in detail. It should be understood,
10 however, that there is no intent to limit the concepts of the present disclosure to the particular forms disclosed, but on the contrary, the intention is to cover all modifications, equivalents, and alternatives consistent with the present disclosure and the appended claims.

In the following description, numerous specific details such as logic implementations, opcodes, means to specify operands, resource partitioning/sharing/duplication
15 implementations, types and interrelationships of system components, and logic partitioning/integration choices are set forth in order to provide a more thorough understanding of the present disclosure. It will be appreciated, however, by one skilled in the art that embodiments of the disclosure may be practiced without such specific details.

20 In other instances, control structures, gate level circuits and full software instruction sequences have not been shown in detail in order not to obscure the invention. Those of ordinary skill in the art, with the included descriptions, will be able to implement appropriate functionality without undue experimentation.

References in the specification to “one embodiment,” “an embodiment,” “an example embodiment,” etc., indicate that the embodiment described may include a particular
25 feature, structure, or characteristic, but every embodiment may not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is within the knowledge of one skilled in the art to effect such feature, structure, or
30 characteristic in connection with other embodiments whether or not explicitly described.

Embodiments of the invention may be implemented in hardware, firmware, software, or any combination thereof. Embodiments of the invention implemented in a computer

system may include one or more bus-based interconnects between components and/or one or more point-to-point interconnects between components. Embodiments of the invention may also be implemented as instructions carried by or stored on a machine-readable medium, which may be read and executed by one or more processors. A machine-readable
5 medium may be embodied as any device, mechanism, or physical structure for storing or transmitting information in a form readable by a machine (e.g., a computing device). For example, a machine-readable medium may be embodied as read only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices; mini- or micro-SD cards, memory sticks, electrical signals, and others.

10 In the drawings, specific arrangements or orderings of schematic elements, such as those representing devices, modules, instruction blocks and data elements, may be shown for ease of description. However, it should be understood by those skilled in the art that the specific ordering or arrangement of the schematic elements in the drawings is not meant to imply that a particular order or sequence of processing, or separation of processes, is
15 required. Further, the inclusion of a schematic element in a drawing is not meant to imply that such element is required in all embodiments or that the features represented by such element may not be included in or combined with other elements in some embodiments.

In general, schematic elements used to represent instruction blocks may be implemented using any suitable form of machine-readable instruction, such as software or firmware
20 applications, programs, functions, modules, routines, processes, procedures, plug-ins, applets, widgets, code fragments and/or others, and that each such instruction may be implemented using any suitable programming language, library, application programming interface (API), and/or other software development tools. For example, some embodiments may be implemented using Java, C++, and/or other programming languages.

25 Similarly, schematic elements used to represent data or information may be implemented using any suitable electronic arrangement or structure, such as a register, data store, table, record, array, index, hash, map, tree, list, graph, file (of any file type), folder, directory, database, and/or others.

30 Further, in the drawings, where connecting elements, such as solid or dashed lines or arrows, are used to illustrate a connection, relationship or association between or among two or more other schematic elements, the absence of any such connecting elements is not meant to imply that no connection, relationship or association can exist. In other words, some connections, relationships or associations between elements may not be shown in the drawings so as not to obscure the disclosure. In addition, for ease of illustration, a single

connecting element may be used to represent multiple connections, relationships or associations between elements. For example, where a connecting element represents a communication of signals, data or instructions, it should be understood by those skilled in the art that such element may represent one or multiple signal paths (e.g., a bus), as may be needed, to effect the communication.

Referring now to FIG. 1, a system 100 for establishing a secure communication session includes a client device 102, a server 104, and a network 106. In operation, the client device 102 initiates a request for a secure communication session with the server 104 over the network 106. To establish the secure communication session, the client device 102 and the server 104 perform a cryptographic key exchange, such as a Diffie-Hellman or a Rivest-Shamir-Adleman (RSA) key exchange, to generate a secret symmetric session key. The secret symmetric session key may then be used to encrypt and decrypt messages between the client device 102 and the server 104. To ensure a secure communication session, the various keys and other cryptographic functions generated by the client device 102 are done so within a security engine 110 of a system-on-a chip (SOC) 112 of the client device 102. The client device 102 maintains the keys in secrecy within a secure memory 114 of the security engine 110. For example, the security engine 110 may include a security key 150, as discussed below, used to sign and/or otherwise encrypt other keys and messages. In this way, the client device 102 and server 104 may establish a secure communication session across the network 106 using out-of-band (i.e., not application level), hardware security features of the client device 102. In the illustrative embodiments described herein, the secure communication session is a Secure Sockets Layer (SSL) communication session, but the system 100 and features described herein may be used to establish other types of secure communication sessions in other embodiments.

The client device 102 may be embodied as any type of computing device capable of communicating with the server 104 over the network 106. For example, the client device 102 may be embodied as a set-top box, a digital television, a smartphone, a tablet computer, a laptop computer, a mobile internet device (MID), a desktop computer, or other device capable of communicating with the server 104.

As discussed above, the client device 102 includes the SOC 112, which may be embodied as any type of system-on-a-chip device having various components and structures. In the illustrative embodiment of FIG. 1, the SOC 112 includes the security engine 110, a memory controller 116, a processor core 118, and a plurality of hardware peripherals 130, which are communicatively coupled to each other via a link 120. The link 120 may be

embodied as any type of interconnect such as a bus, point-to-point, or other interconnect capable of facilitating communication between the various components of the SOC 112. The hardware peripherals 130 may include any type of hardware peripheral component depending upon the intended functionality of the SOC 112. For example, in the illustrative embodiment, the hardware peripherals 130 include a demux 132 to separate audio and video content streams, video processing component(s) 134 to process video content, and audio processing component(s) 136 to process audio content. Of course, it should be appreciated that the hardware peripherals 130 of the SOC 112 have been simplified in the illustrative embodiment of FIG. 1 and that the SOC 112 may include additional, different, and/or greater detailed hardware peripherals 130, which are not illustrated in FIG. 1 for clarity of the disclosure.

The security engine 110 may be embodied as a security co-processor or processing circuitry separate from the processor core 118. The security engine 110 includes the security key 150 and the secure memory 114, which is accessible only by the security engine 110. The security engine 110 stores the security key 150, and other cryptographic keys as discussed below, in the secure memory 114. In the illustrative embodiment, the security key 150 is provisioned during the manufacturing of the SOC 112, but may be generated by the SOC 112 during operation in other embodiments. For example, in some embodiments, the security key 150 is based on blown fuses within the security engine 110 itself. Additionally or alternatively, the security engine 110 may include a key-generating module, such as a trusted platform module (TPM), to generate the security key 150. During use, the security engine 110 may use any number of security keys 150, which may be identical or different from each other.

In some embodiments, the client device 102 may include additional components and structures other than the SOC 112 depending on the type and intended use of the client device 102. For example, in the illustrative embodiment of FIG. 1, the client device 102 includes a system memory 160, a data storage 162, a communications output 164, and one or more input/output devices 166. The system memory 160 may be embodied as any type of main memory or data storage locations including, for example, dynamic random access memory devices (DRAM), synchronous dynamic random access memory devices (SDRAM), double-data rate synchronous dynamic random access memory device (DDR SDRAM), mask read-only memory (ROM) devices, erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM) devices, flash memory devices, and/or other volatile and/or non-volatile memory devices.

The data storage 162 may be embodied as any type of device or devices configured for the short-term or long-term storage of data such as, for example, memory devices and circuits, memory cards, hard disk drives, solid-state drives, or other data storage devices. The communications output 164 may be embodied as a simplified output or as various circuits and/or devices to facilitate, for example, communications with the server 104. For example, the communications output 164 (and/or communication circuitry within the SOC 112) may use any suitable communication protocol such as Ethernet (i.e. the IEEE 802.3 standard) or Wi-Fi® (i.e., the IEEE 802.11 standard), and/or other communication protocols or standards. Additionally, the input/output devices 166 may be embodied as any type of I/O device for interacting with the client device 102. For example, the I/O devices 166 may include output devices such as a display for displaying data on the client device 102, speakers for generating audio, and/or input devices such as a remote control receiver, a keyboard, a mouse, and/or the like.

The server 104 may be embodied as any type of data server capable of establishing a secure communication session with the client device 102. As such, the server 104 may include various hardware and software components typically found in a server for communicating, maintaining, and transferring data over a network. For example, the illustrative server 104 includes a processor 180, a memory 182, and communication circuitry 184, which may be similar to such components found in other data servers. For example, the processor 180 may be embodied as any type of processor capable of executing software/firmware, such as a microprocessor, digital signal processor, microcontroller, or the like, and may include one or more processing cores. The memory 182 may be embodied as any type of memory or data storage locations including, for example, dynamic random access memory devices (DRAM), synchronous dynamic random access memory devices (SDRAM), double-data rate synchronous dynamic random access memory device (DDR SDRAM), mask read-only memory (ROM) devices, erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM) devices, flash memory devices, and/or other volatile and/or non-volatile memory devices. The communication circuitry 184 may be embodied any type of circuitry and/or device to facilitate, for example, communications with the client device 102. For example, the communication circuitry 184 may support communication protocols such as Ethernet (i.e. the IEEE 802.3 standard) and/or Wi-Fi® (i.e., the IEEE 802.11 standard), and/or other communication protocols or standards.

The network 106 may be embodied as any number of various wired and/or wireless networks. For example, the network 106 may be embodied as or otherwise include a local area network (LAN), a wide area network (WAN), and/or a publicly accessible, global network such as the Internet. Additionally, the network 106 may include any number of
5 additional devices to facilitate communication between the client device 102 and the server 104. As discussed above, in the illustrative embodiment, the client device 102 and the server 104 establish a SSL communication session over the network 106. However, other types of secure communication sessions may be established in other embodiments.

Referring now to FIG. 2, as discussed in more detail below, the use of the security engine
10 110 of the client device 102 to perform the cryptographic functions and store keying data associated with the establishment of the secure communication session allows the system 100 to offer several different levels of security. The particular level of security used in the system 100 may depend upon various criteria such as the nature of the network 106, the importance of the data being transferred between the client device 102 and the server 104,
15 and/or the like. For example, one illustrative security scheme 200 includes three different levels of security as shown in FIG. 2. At level 0 security, the client device 102 is configured to protect the client private device key (i.e., the security key 150), which is used for encrypting, signing, and verification functions as discussed in more detail below.

At level 1 security, the client device 102 is configured to protect the session keys and
20 related keys used for data encryption. For example, if an RSA key exchange is performed, the pre-master key and the master key (i.e., the session key) may be stored in the secure memory 114 of the security engine 110 of the SOC 112. Additionally, in some embodiments as discussed below, the master key may be stored in an encrypted or wrapped form (e.g., encrypted using the security key 150). In embodiments in which a
25 Diffie-Hellman key exchange is used, the private Diffie-Hellman client key and/or shared secret key (i.e., the session key) may be stored in the secure memory 114 of the security engine 110 of the SOC 112. Again, in some embodiments, the private Diffie-Hellman client key and/or session key may be stored in an encrypted or wrapped form (e.g., encrypted using the security key 150).

30 Additionally, at level 2 security, the client device 102 may be configured to protect the data of the host application. For example, if the host application is being used to perform an e-commerce transaction, the bank account information used in such transaction may be encrypted using the security key 150 and stored in the secure memory 114. In this way, the bank account information is not available to the host application. Of course, it should

be appreciated that, in other embodiments, security schemes having more or fewer security levels may be used.

Referring now to FIG. 3, in operation, the client device 102 and the server 104 establish a secure communication session using the security engine 110 of the client device 102 to perform various cryptographic functions and store keying data therein. To do so, the client device 102 and server 104 may perform a handshake session as shown in the communication sequence 300 of FIG. 3. To establish the secure communication session, a security engine driver 302 of the security engine 110 communicates with a firmware of the security engine 110 and a client secure communication application 304 executed on the client device 102. The client secure communication application 304 also communicates with a corresponding server secure communication application 306 executed on the server 104.

The communication sequence 300 begins with block 310 in which the client secure communication application 304 sends a ClientHello message to the server secure communication application 306 to request the initiation of a secure communication session. As discussed above, the secure communication session is a SSL session in the illustrative embodiment. To facilitate the request, the security engine driver 302 communicates with security engine 110 of the SOC 112 to request a random nonce from the security engine 110 in block 312. The security engine 110 may use any suitable random number-generating algorithm to generate the random nonce in block 312. The nonce is embodied as random or pseudo-random number intended to be used only once in cryptographic functions to thwart, for example, replay attacked. In the illustrative embodiment, the random nonce includes a 32-bit timestamp and a 28-byte random number. Of course, other numeric formats for the random nonce may be used in other embodiments. Regardless, it should be appreciated that because the random nonce is generated in the security engine 110, the generation and storage of the random nonce is protected compared to generation of the nonce at, for example, the application level.

The random nonce generated in block 312 is included in the ClientHello message sent to the server secure communication application 306 in block 310. Additionally, the ClientHello message may include a list of cipher suites, compression methods, and other cryptographic protocols or algorithms from which the server 104 may make a selection for use in establishing the secure communication session. In response to the secure communication session request, the server secure communication application 306 sends a ServerHello message in block 314. The ServerHello message may be substantially similar

to the ClientHello message. For example, in the illustrative embodiment, the ServerHello message includes a server random nonce generated by the server 104. Additionally, the ServerHello message includes the selection(s) of the cryptographic protocols and/or other options made by the server 104 from the list included in the ClientHello message. The
5 ServerHello message completes the session initiation phase (Phase 1) of the illustrative handshake session.

In block 316, the server secure communication application 306 sends a server certificate to the client secure communication application 304. The server certificate, like the client certificate discussed below, is typically generated by a certification authority organization,
10 which acts as a third-party verifier of the authentication of the server 104. The server certificate may include unique identifier or number assigned to the server 104 by the certification authority organization to verify the server 104 to other devices on the network 106. As such, in block 318, the client device 102 may verify the server certificate. In some embodiments, the client device 102 verifies the server certificate using a public
15 certificate key issued by the certification authority organization. In such embodiments, the security engine 110 may store the public certificate key in the secure memory 114 in an unencrypted or encrypted state (e.g., using the security key 150).

To establish the secure communication session, the client device 102 and the server 104 perform a key exchange to establish a shared secret key (i.e., a master or session key) in
20 each of the client device 102 and server 104. The client device 102 and the server 104 may use any appropriate key exchange algorithm to effect the establishment of the shared secret. In the illustrative embodiment, the key exchange may be embodied as an RSA key exchange or a Diffie-Hellman key exchange. In embodiments wherein a RSA key exchange is used, the server secure communication application 306 performs a server RSA
25 key exchange in block 320. In such embodiments, the server 104 may generate a temporary RSA public/private key pair and send the RSA public key to the client device 102 in block 320. Such message may be signed by the server 104 and verified by the client device 102 using a public server key, which may be stored in the secure memory 114 as discussed above.

Alternatively, the server secure communication application 306 may perform a server
30 Diffie-Hellman key exchange in block 320. In such embodiments, the server 104 selects or otherwise generates the Diffie-Hellman global values (e.g., a prime number and a primitive root of the prime number), generates a private and public Diffie-Hellman server key, and sends the Diffie-Hellman global values and public Diffie-Hellman server key to the client

device 102 in block 320. Again, such message may be signed by the server 104 and verified by the client device 102 using a public server key.

In some embodiments, the sever secure communication application 306 may send a client certification request in block 322. If so, the request may specify the types of certificates
5 accepted by the server 104 (e.g., the public key algorithm used), acceptable certificate authorities, and/or other certificate parameters. Subsequently, in block 324, the server secure communication application 306 sends a server completion message (a “ServerHelloDone” message) to the client secure communication application 304 to indicate that the server 104 has completed this phase of the handshake session. In the
10 illustrative embodiment, no parameters or other data are required for the server completion message. The ServerHelloDone message completes the server authentication and key exchange phase (Phase 2) of the illustrative handshake session.

After receiving the server completion message, the client secure communication application 304 initiates the client authentication and key exchange phase (Phase 3) of the
15 handshake session by sending the client certificate in block 326. As discussed above, the client certificate is typically generated by the certification authority organization and may include a unique identifier or number assigned to the client device 102 by the certification authority organization to verify the client device 102 to other devices on the network 106. In some embodiments, the client certificate may be stored in the secure memory 114 of the
20 security engine 110 of the SOC 112 in an unencrypted or encrypted state. Additionally, the client device 102 may use a private device key issued by the certification authority organization to sign the certificate prior to sending it to the server 104.

In block 328, the client secure communication application 304 performs a client key exchange. Again, the client device 102 and the server 104 may use any appropriate key
25 exchange algorithm to effect the establishment of the shared secret as discussed above. In embodiments wherein an RSA key exchange is used, the security engine 110 of the SOC 112 of the client device 102 generates a random pre-master key in block 330. Illustratively, the pre-master key is embodied as a 48-byte random number, but other numeric formats may be used in other embodiments. In block 332, the pre-master key generated in block 330 is encrypted or otherwise wrapped using the server public key
30 provided by the server in server authentication and key exchange phase (Phase 2). The encrypted pre-master key may be stored in the secure memory 114 of the security engine 110 of the SOC 112 and sent to the server 104 in block 328.

Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 generates, in block 334, a private Diffie-Hellman client key and a public Diffie-Hellman client key using the Diffie-Hellman global values received from the server 104 in block 320. The private Diffie-Hellman client key may be embodied as a random value generated by the security engine 110, while the public Diffie-Hellman client key is generated by the security engine 110 using the Diffie-Hellman global values received from the server 104. The private Diffie-Hellman client key may be stored in the secure memory 114 of the security engine 110. Of course, in some embodiments, the client device 102 may generate the Diffie-Hellman global values in block 334 and send such global values to the server 104 in block 328 to allow the server 104 to generate the public Diffie-Hellman server key based thereon. Regardless, in block 336, the security engine 110 of the SOC 112 signs the public Diffie-Hellman client key (and Diffie-Hellman global values if generated by the client device 102) in block 336 using the security key 150 or other private client key of the security engine 110. The signed Diffie-Hellman parameters may be further encrypted using the public server key and sent to the server 104 in block 328.

In some embodiments, the client secure communication application 304 may send a client certification verification message to the sever secure communication application 306 in block 338. To do so, the security engine 110 generates a hash code based on the preceding message and signs the hash code using the security key 150 of the security engine 110 in block 340. The client device 102 sends the signed hash code to the server 104 in block 338 as verification of the preceding message. It should be appreciated that such client certification verification messages may be used subsequent to any message sent to the server 104 from the client device 102 to provide an added level of security and verification to the secure communication session. The client certification verification message in block 338 completes the client authentication and key exchange phase (Phase 3) of the illustrative handshake session.

In block 342, the client secure communication application 304 sends a change cipher specification message to the server secure communication application 306 to inform the server 104 that subsequent communications will use the agreed-upon cipher (e.g., the generated session key). In block 344, the security engine 110 of the client device 102 generates a session key (i.e., the “master” key). In embodiments wherein an RSA key exchange is used, the security engine 110 generates the session key as a function of the pre-master key generated in block 330. To do so, the security engine 110 calculates a hash

function of the pre-master key, the client random nonce generated in block 312, and the server random nonce received in block 314. Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 generates the session key as a function of the Diffie-Hellman global values, the public Diffie-Hellman server key, and the private Diffie-Hellman client key. As discussed above, the session key is stored in the secure memory 114 of the security engine 110.

In block 346, the security engine 110 generates a hash code of the session key, which may include additional padding depending on the type of hash function used. The hash code of the session key is sent to the server 104 for verification in a client-finished message in block 348. The hash code of the session key may be encrypted by the security engine 110 using the public server key as discussed above.

In response to the client-finished message, the server 104 sends a change cipher specification message that acknowledges the use of the agreed-upon cipher (e.g., the session key) in block 350. The server 104 also sends a server-finished message in block 352 that includes a similar hash code of the session key for verification by the client device 102. Assuming that the client device 102 and the server 104 verify the hash code of the session key, the handshake session is complete and each of the client device 102 and server 104 have a shared secret session key that is used to encrypt and decrypt subsequent messages. Again, it should be appreciated that the security engine 110 of the SOC 112 of the client device 102 is used for all cryptographic functions and storage of sensitive keying data to provide hardware-based protection of the cryptographic keys and certificate keys used during the communication sequence 300.

Referring now to FIG. 4, in use, the client device 102 may execute a method 400 to establish a secure communication session with the server 104. The method 400 begins with block 402 in which the security engine 110 of the SOC 112 of the client device 102 is provisioned. To do so, in one embodiment, the security engine 110 receives a client device certificate, a private client device key, and a public certification key. The client device certificate, the private client device key, and the public certification key are typically generated by the certification authority organization, which acts as a third-party verifier of the authentication of the client device 102 as discussed above. The client device certificate may include a unique device identifier or number assigned to the client device 102 by the certification authority organization to verify the client device 102 to other devices on the network 106. The private client device key may be used by the client device 102 to sign the client device certificate so as to authenticate the client device 102 to other devices as

discussed in more detail below. Conversely, the public certification key may be used by the client device 102 to verify certification of other devices on the network 106 by the certification authority organization.

The security engine 110 encrypts the private client device key using the security key 150 and stores the encrypted private client device key in the secure memory 114. The security engine 110 may also store the client device certificate and/or the public certification key in the secure memory 114. Additionally, in some embodiments, the security engine 110 may encrypt the client device certificate and/or the public certification key using the security key 150 stored in the security engine 110.

After the security engine 110 has been provisioned in block 402, the client device 102 determines whether to establish a secure communication session (e.g., an SSL session) with the server 104 in block 404. If so, in block 406, the security engine 110 generates a random nonce value. As discussed above, the security engine 110 may use any suitable random number-generating algorithm to generate the random nonce. In block 408, the client device 102 sends a request (a ClientHello message) to initiate the secure communication session to the server 104. The request includes the random nonce generated in block 406 along with a list of cipher protocols, compression methods, and/or other cryptographic choices from which the server 104 may select.

In block 410, the client device 102 completes the server authentication and server key exchange. In so doing, the client device 102 may receive a corresponding ServerHello message including a server random nonce, the server's 104 public key, and the server's 104 selection of cryptographic choices presented in the ClientHello message. As discussed above, the server random nonce, along with the client random nonce, is used to generate the session key. As such, the security engine 110 may store the server random nonce in the secure memory 114. Additionally, in some embodiments, the security engine 110 may store the server certificate and/or other keying data in the secure memory 114. For example, in embodiments wherein an RSA key exchange is used, the security engine 110 may store the public RSA key received from the server in the secure memory 114. Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 may store the Diffie-Hellman global values and/or public Diffie-Hellman server key in the secure memory 114.

In block 414, the client 104 determines whether the server 104 is successfully authenticated. If not, the method 400 loops back to block 404 in which the client device 102 may reattempt to establish a secure communication session with the server 104.

However, if the server 104 is successfully authenticated, the method 400 advances to block 416 in which the client device 102 sends the server 104 the client certificate. If the client certificate has been encrypted (e.g., using the secure key 150), the security engine 110 decrypts the client certificate and signs the client certificate using the private client device key.

In block 418, the client 104 completes the client key exchange using the security engine 110 to maintain the security of the keying functions. For example, if a RSA key exchange was selected, the security engine 110 generates the pre-master key and encrypts the pre-master key using the server public key received in block 410 prior to sending the encrypted pre-master key to the server 104 in block 420. Alternatively, if a Diffie-Hellman key exchange was selected, the security engine 110 generates the public and private Diffie-Hellman client keys using the Diffie-Hellman global values received from the server 104 in block 410. The security engine 110 may sign the public Diffie-Hellman client key using the security key 150 or the public client device key provisioned in block 402. The client device 102 sends the signed public Diffie-Hellman client key to the server 104 in block 422. The keys and related keying data generated during the client key exchange may be stored in the secure memory 114 in an encrypted state (using the security key 150) or an unencrypted state.

In block 424, the client device 102 determines whether the client device 102 has been successfully authenticated by the server 104. If not, the method 400 loops back to block 404 in which the client device 102 may reattempt to establish a secure communication session with the server 104. However, if the client device 102 is successfully authenticated, the method 400 advances to block 426 in which the client device 102 confirms the cipher suite with the server 104 by informing the server 104 that subsequent messages will use the agreed-upon cryptographic protocols. In so doing, the security engine 110 may generate the master or session key. To do so, in embodiments wherein an RSA key exchange is used, the security engine 110 calculates a hash function of the pre-master key, the client random nonce generated in block 406, and the server random nonce received in block 410. Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 generates the session key as a function of the Diffie-Hellman global values, the public Diffie-Hellman server key, and the private Diffie-Hellman client key. Once generated, the security engine 110 of the SOC 112 may store the session key in the secure memory 114 of the security engine 110. In some embodiments,

the session key may be encrypted using the security key 150 while stored in the secure memory 114.

5 In block 428, the security engine 110 generates a hash function of the session key, which is sent to the server 104 for verification in a client finished message. Again, the hash code of the session key may be encrypted by the security engine 110 using the public server key as discussed above. In response, the server 104 confirms the cipher suite with the client device 102 to acknowledge the agreed-upon cipher (e.g., the session key). The server 104 also sends a server finished message that includes a similar hash code of the session key for verification by the client device 102. Assuming that the client device 102 and the server 104 verify the hash code of the session key, the handshake session is complete and each of the client device 102 and server 104 have a shared secret session key that is used to encrypt and decrypt subsequent messages.

10 While the disclosure has been illustrated and described in detail in the drawings and foregoing description, such an illustration and description is to be considered as exemplary and not restrictive in character, it being understood that only illustrative embodiments have been shown and described and that all changes and modifications consistent with the disclosure and recited claims are desired to be protected.

CLAIMS:

1. A system-on-a-chip apparatus comprising:
a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, the security engine to:
5 generate a random nonce for initiating a request for a secure communication session with a server over a network using the nonce;
perform a cryptographic key exchange with the server to generate a symmetric session key to encrypt messages sent to the server and decrypt messages received from the server during the secure communication session;
10 store the session key in the secure memory,
the system-on-a-chip to establish the secure communication session with the server over the network using the session key.
2. The system-on-a-chip apparatus of claim 1, wherein the system-on-a-chip
15 to establish a Secure Sockets Layer communication session with the server over the network using the session key.
3. The system-on-a-chip apparatus of claim 1, wherein the security engine to receive a server nonce from the server in response to the request for the secure communication session, the response message including a server nonce and store the server nonce in the secure
20 memory.
4. The system-on-a-chip apparatus of claim 1, wherein the security engine to receive a server certificate from the server and store the server certificate in the secure memory.
25
5. The system-on-a-chip apparatus of claim 1, wherein the security engine to perform a Rivest-Shamir-Adleman key exchange with the server to generate the symmetric session key.
- 30 6. The system-on-a-chip apparatus of claim 5, wherein the security engine to generate a pre-master key, encrypt the pre-master key using a security key of the security engine, and send the encrypted pre-master key to the server.

7. The system-on-a-chip apparatus of claim 6, wherein the security engine to wrap the pre-master key using a server public key and store the wrapped pre-master key in the secure storage.

5 8. The system-on-a-chip apparatus of claim 6, wherein the security engine to generate the session key as a function of the pre-master key.

9. The system-on-a-chip apparatus of claim 8, wherein the security engine to calculate a hash function as a function of the random nonce generated by the security engine and a nonce received from the server.

10

10. The system-on-a-chip apparatus of claim 5, wherein the security engine to receive a public Rivest-Shamir-Adleman server key from the server and store the public Rivest-Shamir-Adleman server key in the secure memory.

15

11. The system-on-a-chip apparatus of claim 1, wherein the security engine to perform a Diffie-Hellman key exchange with the server to generate the symmetric session key.

12. The system-on-a-chip apparatus of claim 11, wherein the security engine to generate a public Diffie-Hellman client key and a private Diffie-Hellman client key, sign the public Diffie-Hellman client key using a security key of the security engine, and send the signed public Diffie-Hellman key to the server.

20

13. The system-on-a-chip apparatus of claim 12, wherein the security engine to receive a public Diffie-Hellman server key from the server and generate the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

25

14. The system-on-a-chip apparatus of claim 13, wherein the security engine to use the session key to encrypt a subsequent message sent from the client device to the server.

30

15. The system-on-a-chip apparatus of claim 11, wherein the security engine to receive Diffie-Hellman global values and a public Diffie-Hellman server key from the server and store at least one of the Diffie-Hellman global values and the public Diffie-Hellman server key in the secure storage.

16. A method comprising:
generating a random nonce in a security engine of a system-on-a-chip of a client device;
initiating, using the client device, a request for a secure communication session
5 with a server over a network, the request including the random nonce;
performing a cryptographic key exchange, using the security engine of the system-on-a-chip, with the server to generate a symmetric session key to encrypt messages sent to the server and decrypt messages received from the server during the secure communication session;
10 storing the session key in a secure memory of the security engine of the system-on-a-chip; and
establishing, using the client device, the secure communication session with the server using the session key.
17. The method of claim 16, wherein initiating a request for a secure communication session comprises initiating a request for a Secure Sockets Layer communication session.
18. The method of claim 16, further comprising:
20 receiving a response message from the server in response to the request for a secure communication session, the response message including a server nonce, and
storing the server nonce in the secure memory of the security engine of the system-on-a-chip.
19. The method of claim 16, wherein initiating a request for a secure communication session comprises sending a ClientHello message, including the nonce, to the server; and further comprising:
25 receiving a ServerHello message from the server, the ServerHello message including a server nonce; and
30 storing the server nonce in the secure memory of the security engine of the system-on-a-chip.

20. The method of claim 16, further comprising receiving a server certificate from the server and storing the server certificate in the secure memory of the security engine of the system-on-a-chip of the client device.
- 5 21. The method of claim 16, wherein performing the cryptographic key exchange with the server comprises performing a Rivest-Shamir-Adleman key exchange, using the security engine of the system-on-a-chip, with the server.
22. The method of claim 21, wherein performing the Rivest-Shamir-Adleman
10 key exchange with the server comprises:
generating a pre-master key in the security engine;
encrypting the pre-master key using a security key of the security engine; and
sending the encrypted pre-master key to the server.
- 15 23. The method of claim 22, further comprising:
wrapping the pre-master key in the security engine of the system-on-a-chip using a server public key, and
storing the wrapped pre-master key in the secure storage of the security engine of the system-on-a-chip.
- 20 24. The method of claim 22, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises generating the session key in the security engine of the system-on-a-chip as a function of the pre-master key.
- 25 25. The method of claim 24, wherein generating the session key in the security engine comprises calculating, using the security engine of the system-on-a-chip, a hash function as a function of the random nonce generated by the security engine and a nonce received from the server.
- 30 26. The method of claim 21, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises:
receiving a public Rivest-Shamir-Adleman server key from the server; and
storing the public Rivest-Shamir-Adleman server key in the secure memory of the security engine of the system-on-a-chip.

27. The method of claim 16, wherein performing the cryptographic key exchange with the server comprises performing a Diffie-Hellman key exchange, using the security engine of the system-on-a-chip, with the server.

5

28. The method of claim 27, wherein performing a Diffie-Hellman key exchange with the server comprises:

generating, in the security engine of the system-on-a-chip, a public Diffie-Hellman client key and a private Diffie-Hellman client key;

10 signing the public Diffie-Hellman client key using a security key of the security engine of the system-on-a-chip; and

sending the signed public Diffie-Hellman key to the server.

29. The method of claim 28, wherein performing a Diffie-Hellman key
15 exchange with the server comprises:

receiving a public Diffie-Hellman server key from the server;

generating, in the security engine of the system-on-a-chip, the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

20 30. The method of claim 29, wherein performing a Diffie-Hellman key exchange with the server comprises using the session key to encrypt a subsequent message sent from the client device to the server.

31. The method of claim 27, wherein performing a Diffie-Hellman key exchange with the server comprises:

receiving Diffie-Hellman global values and a public Diffie-Hellman server key from the server, and

5 storing at least one of the Diffie-Hellman global values and the public Diffie-Hellman server key in the secure storage of the security engine of the system-on-a-chip.

32. The method of claim 16, further comprising:

retrieving a client certificate stored on the client device;

10 signing a client certificate using a security key stored in a secure memory of the security engine of the system-on-a-chip; and

sending the client certificate to the server.

33. The method of claim 16, further comprising:

15 generating, in the security engine of the system-on-a-chip, a hash code of a preceding message sent from the client to the server;

signing the hash code using a security key stored in a secure memory of the security engine; and

20 sending a client certificate verification message to the server, the client certificate verification message including the signed hash code.

34. The method of claim 16, wherein establishing the secure communication session comprises:

generating, in the security engine, a hash code as a function of the session key;

and

5 sending a client completion message that includes the hash code to the server to indicate the client has completed an initial handshake procedure.

35. A source device comprising:

10 a system-on-a-chip having a security engine, the system-on-a-chip including a plurality of instructions that when executed results in the system-on-a-chip performing the method of claim 16-34.

36. One or more machine readable media comprising a plurality of instructions that in response to being executed by a client device result in the client device
15 performing the method of claims 16-34.

37. A method comprising:

generating a random nonce in a security engine of a system-on-a-chip of a client device;

20 initiating, using the client device, a request for a Secure Sockets Layer communication session with a server over a network, the request including the random nonce;

performing a cryptographic key exchange, using the security engine of the system-on-a-chip, with the server to generate a symmetric session key to encrypt messages sent to the server and decrypt messages received from the server during the Secure Sockets Layer
25 communication session;

storing the session key in a secure memory of the security engine of the system-on-a-chip; and

generating, in the security engine, a hash code as a function of the session key;

and

30 sending a client completion message to the server that includes the hash code to indicate the client has completed an initial handshake procedure.

38. The method of claim 37, wherein performing the cryptographic key exchange with the server comprises performing a Rivest-Shamir-Adleman key exchange, using the security engine of the system-on-a-chip, with the server.

5 39. The method of claim 38, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises:

generating a pre-master key in the security engine;
encrypting the pre-master key using a security key of the security engine; and
sending the encrypted pre-master key to the server.

10

40. The method of claim 39, further comprising:
wrapping the pre-master key in the security engine using a server public key, and
storing the wrapped pre-master key in the secure storage of the security engine of
the system-on-a-chip.

15

41. The method of claim 39, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises generating the session key in the security engine of the system-on-a-chip as a function of the pre-master key.

20

42. The method of claim 41, wherein generating the session key in the security engine comprises calculating, using the security engine of the system-on-a-chip, a hash function as a function of the random nonce generated by the security engine and a nonce received from the server.

25

43. The method of claim 37, wherein performing the cryptographic key exchange with the server comprises performing a Diffie-Hellman key exchange, using the security engine of the system-on-a-chip, with the server.

30 44. The method of claim 43, wherein performing a Diffie-Hellman key exchange with the server comprises:

generating, in the security engine of the system-on-a-chip, a public Diffie-Hellman client key and a private Diffie-Hellman client key;
signing the public Diffie-Hellman client key using a security key of the security engine of the system-on-a-chip; and

sending the signed public Diffie-Hellman key to the server.

45. The method of claim 44, wherein performing a Diffie-Hellman key exchange with the server comprises:

- 5 receiving a public Diffie-Hellman server key from the server;
 generating, in the security engine of the system-on-a-chip, the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

46. A source device comprising:

- 10 a system-on-a-chip having a security engine, the system-on-a-chip including a plurality of instructions that when executed results in the system-on-a-chip performing the method of claim 37-45.

47. One or more machine readable media comprising a plurality of
15 instructions that in response to being executed by a client device result in the client device performing the method of claims 37-45.

1/4

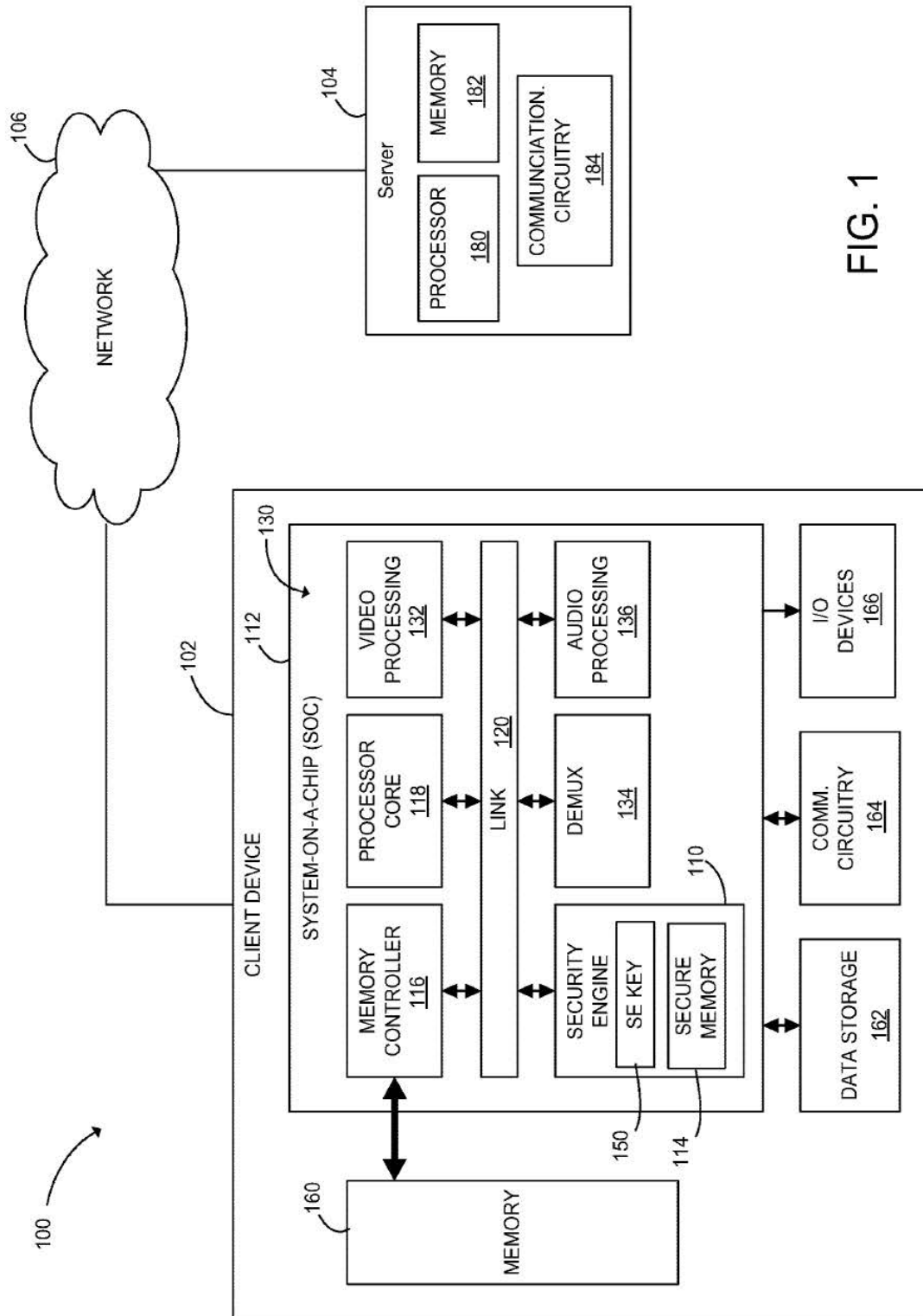


FIG. 1

2/4

200

LEVEL 0	PROTECTION OF CLIENT PRIVATE DEVICE KEY USED FOR SIGNING & VERIFICATION	
LEVEL 1	PROTECTION OF SESSION KEYS USED FOR DATA ENCRYPTION	
	RSA KEY EXCHANGE	DIFFIE-HELLMAN KEY EXCHANGE
	PROTECTION OF PRE-MASTER KEY	PROTECTION OF CLIENT PRIVATE DH KEY
LEVEL 2	PROTECTION OF APPLICATION DATA	

FIG. 2

3/4

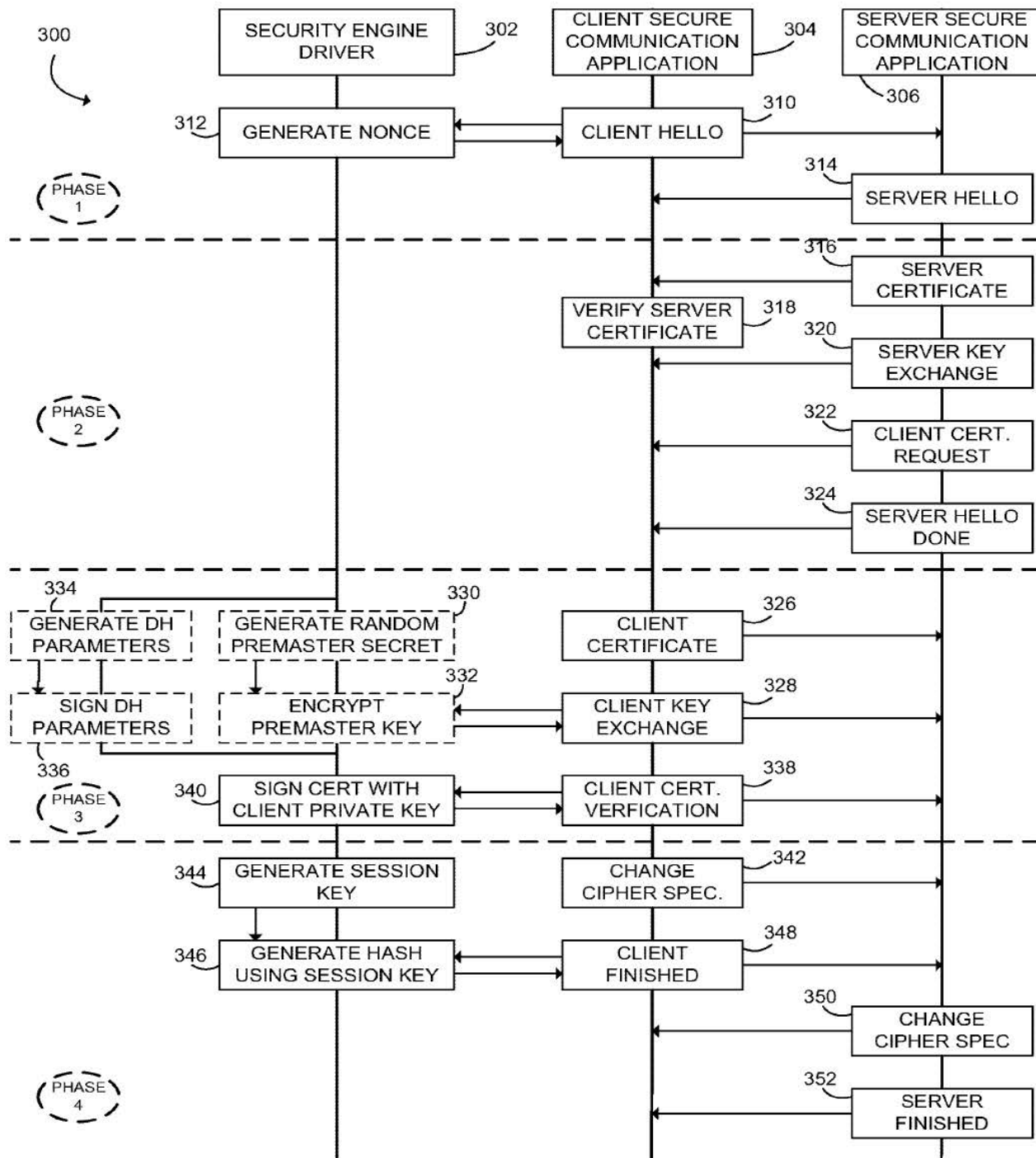


FIG. 3

4/4

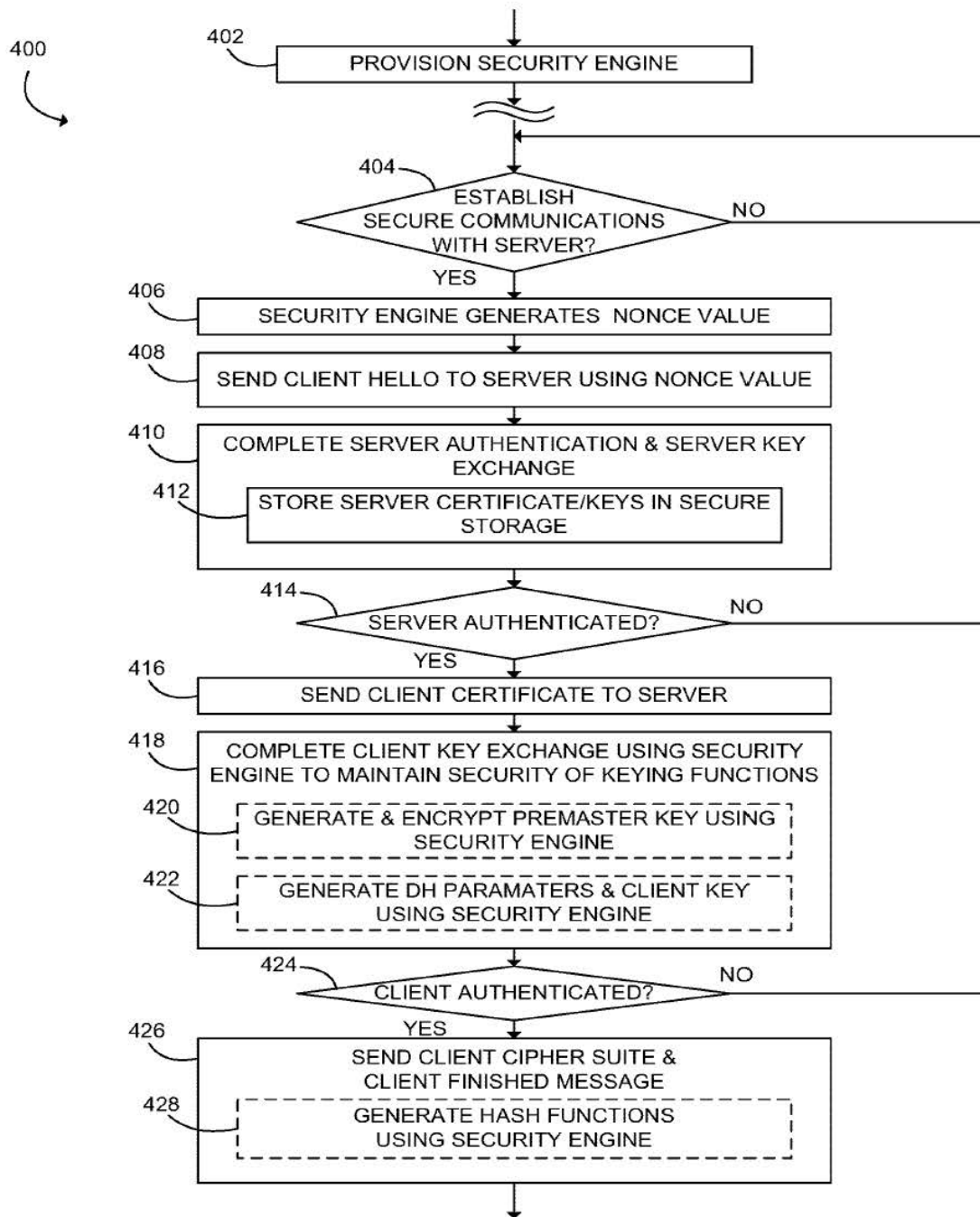


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/065069**A. CLASSIFICATION OF SUBJECT MATTER****H04L 9/14(2006.01)i, H04L 9/32(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 9/14; H04L 9/08; H04L 9/32; H04L 9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: secure communication, secure socket layer, SSL, transport layer security, IPSec, random nonce, handshake initiate, key exchange, session key, secure memory, hash code, handshake completion

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2011-0231923 A1 (BOLLAY BENN SAPIN et al.) 22 September 2011 See Claims 1,6; Paragraphs [27],[63],[70],[89]-[93],[95],[123]-[126]; Figures 2,5,8	1-32,35-36
A		33-34,37-47
Y	US 2005-0213768 A1 (DAVID DURHAM et al.) 29 September 2005 See Claims 1-4; Paragraphs [14],[15],[17],[20],[21],[26],[28],[33],[45],[49],[53],[54]; Figures 1,2,5	1-32,35-36
A		33-34,37-47
A	US 2010-0299525 A1 (SHAH PARAS et al.) 25 November 2010 See Claims 1,8; Paragraphs [47],[50],[54]-[56],[59],[60]; Figures 2,3	1-47
A	US 2008-0037793 A1 (BUER MARK) 14 February 2008 See Claims 11-17; Paragraphs [35],[39]-[43]; Figures 4,7-9	1-47

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

29 AUGUST 2012 (29.08.2012)

Date of mailing of the international search report

30 AUGUST 2012 (30.08.2012)

Name and mailing address of the ISA/KR


 Korean Intellectual Property Office
 189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan
 City, 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Lee Hyoung Il

Telephone No. 82-42-481-8199



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2011/065069

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011-0231923 A1	22.09.2011	CN 102195878 A	21.09.2011
		US 2011-231649 A1	22.09.2011
		US 2011-231651 A1	22.09.2011
		US 2011-231652 A1	22.09.2011
		US 2011-231653 A1	22.09.2011
		US 2011-231655 A1	22.09.2011
		WO 2011-116342 A2	22.09.2011
		WO 2011-116342 A3	22.12.2011
US 2005-0213768 A1	29.09.2005	CN 1926837 A	07.03.2007
		CN 1926837 B	06.04.2011
		EP 1728376 A1	06.12.2006
		EP 1728376 B1	15.07.2009
		JP 04-579969 B2	03.09.2010
		JP 2007-525913 A	06.09.2007
		JP 4579969 B2	10.11.2010
		KR 10-0831437 B1	21.05.2008
		KR 10-2006-0127229 A	11.12.2006
US 2010-0299525 A1	25.11.2010	WO 2005-101794 A1	27.10.2005
		AU 2006-280301 A1	22.02.2007
		CN 101292233 A0	22.10.2008
		EP 1904931 A2	02.04.2008
		JP 2009-505493 A	05.02.2009
		US 2007-0038853 A1	15.02.2007
		US 2009-0119504 A1	07.05.2009
		WO 2007-021483 A2	22.02.2007
US 2008-0037793 A1	14.02.2008	EP 1484890 A2	08.12.2004
		EP 1484890 A3	11.07.2012
		EP 1484913 A2	08.12.2004
		EP 1484913 A3	15.04.2009
		US 2004-0247131 A1	09.12.2004
		US 2005-0041802 A1	24.02.2005
		US 2010-0296573 A1	25.11.2010
		US 6724335 B1	20.04.2004
		US 7289632 B2	30.10.2007
		US 7768434 B2	03.08.2010
		US 8111183 B2	07.02.2012

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To: KELLETT GLEN M. BARNES & THORNBURG, LLP C/O CPA GLOBAL P.O. BOX 52050 MINNEAPOLIS MN 55402 USA		PCT NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION (PCT Rule 44.1)
		Date of mailing (day/month/year) 30 AUGUST 2012 (30.08.2012)
Applicant's or agent's file reference P41624PCT	FOR FURTHER ACTION See paragraphs 1 and 4 below	
International application No. PCT/US2011/065069	International filing date (day/month/year) 15 DECEMBER 2011 (15.12.2011)	
Applicant INTEL CORPORATION et al		

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.
Filing of amendments and statement under Article 19:
 The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):
When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.
Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes
 1211 Geneva 20, Switzerland, Facsimile No.: +41 22 338 82 70
For more detailed instructions, see PCT Applicant's Guide, International Phase, paragraphs 9.004 - 9.011.
2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.
3. ☐ **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:
☐ the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.
☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.
4. **Reminders**
 The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.
 Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90bis.1 and 90bis.3).
 Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.
 In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.
 For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the PCT Applicant's Guide, National Chapters.

Name and mailing address of the ISA/KR  Korean Intellectual Property Office 189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer COMMISSIONER Telephone No. 82-42-481-8754	CPA GLOBAL SEP 11 2012 RECEIVED Coded _____ Verified _____
--	--	---

Form PCT/ISA/220 (July 2010)

* Attention

Copies of the documents cited in the international search report can be searched in the following Korean Intellectual Property Office English website for three months from the date of mailing of the international search report.

<http://www.kipo.go.kr/en/> => PCT Services => PCT Services

ID : PCT international application number

PW : **CZKLKWRL**

Inquiries related to PCT International Search Report or Written Opinion prepared by KIPO as an International Searching Authority can be answered not only by KIPO but also through IPKC (Intellectual Property Korea Center), located in Vienna, VA, which functions as a PCT Help Desk for PCT applicants.

Homepage: <http://www.ipkcenter.com>

Email: ipkc@ipkcenter.com

Phone: +1 703 388 1066

Fax: +1 703 388 1084

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference P41624PCT	FOR FURTHER ACTION see Form PCT/ISA/220 as well as, where applicable, item 5 below.	
International application No. PCT/US2011/065069	International filing date (<i>day/month/year</i>) 15 DECEMBER 2011 (15.12.2011)	(Earliest) Priority Date (<i>day/month/year</i>)
Applicant INTEL CORPORATION et al		

This International search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

a. With regard to the **language**, the international search was carried out on the basis of:

- ☒ the international application in the language in which it was filed
☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6bis(a)).

c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. ☐ **Certain claims were found unsearchable** (See Box No. II)

3. ☐ **Unity of invention is lacking** (See Box No. III)

4. With regard to the **title**,

- ☒ the text is approved as submitted by the applicant.
☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

- ☒ the text is approved as submitted by the applicant.
☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,

- a. the figure of the **drawings** to be published with the abstract is Figure No. 1
☒ as suggested by the applicant.
☐ as selected by this Authority, because the applicant failed to suggest a figure.
☐ as selected by this Authority, because this figure better characterizes the invention.
b. ☐ none of the figure is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/065069**A. CLASSIFICATION OF SUBJECT MATTER***H04L 9/14(2006.01)i, H04L 9/32(2006.01)i*

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 9/14; H04L 9/08; H04L 9/32; H04L 9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: secure communication, secure socket layer, SSL, transport layer security, IPSec, random nonce, handshake initiate, key exchange, session key, secure memory, hash code, handshake completion

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2011-0231923 A1 (BOLLAY BENN SAPIN et al.) 22 September 2011	1-32,35-36
A	See Claims 1,6; Paragraphs [27],[63],[70],[89]-[93],[95],[123]-[126]; Figures 2,5,8	33-34,37-47
Y	US 2005-0213768 A1 (DAVID DURHAM et al.) 29 September 2005	1-32,35-36
A	See Claims 1-4; Paragraphs [14],[15],[17],[20],[21],[26],[28],[33],[45],[49],[53],[54]; Figures 1,2,5	33-34,37-47
A	US 2010-0299525 A1 (SHAH PARAS et al.) 25 November 2010	1-47
	See Claims 1,8; Paragraphs [47],[50],[54]-[56],[59],[60]; Figures 2,3	
A	US 2008-0037793 A1 (BUER MARK) 14 February 2008	1-47
	See Claims 11-17; Paragraphs [35],[39]-[43]; Figures 4,7-9	



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

29 AUGUST 2012 (29.08.2012)

Date of mailing of the international search report

30 AUGUST 2012 (30.08.2012)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan
City, 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Lee Hyoung Il

Telephone No. 82-42-481-8199



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2011/065069

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011-0231923 A1	22.09.2011	CN 102195878 A	21.09.2011
		US 2011-231649 A1	22.09.2011
		US 2011-231651 A1	22.09.2011
		US 2011-231652 A1	22.09.2011
		US 2011-231653 A1	22.09.2011
		US 2011-231655 A1	22.09.2011
		WO 2011-116342 A2	22.09.2011
		WO 2011-116342 A3	22.12.2011
US 2005-0213768 A1	29.09.2005	CN 1926837 A	07.03.2007
		CN 1926837 B	06.04.2011
		EP 1728376 A1	06.12.2006
		EP 1728376 B1	15.07.2009
		JP 04-579969 B2	03.09.2010
		JP 2007-525913 A	06.09.2007
		JP 4579969 B2	10.11.2010
		KR 10-0831437 B1	21.05.2008
		KR 10-2006-0127229 A	11.12.2006
US 2010-0299525 A1	25.11.2010	WO 2005-101794 A1	27.10.2005
		AU 2006-280301 A1	22.02.2007
		CN 101292233 A0	22.10.2008
		EP 1904931 A2	02.04.2008
		JP 2009-505493 A	05.02.2009
		US 2007-0038853 A1	15.02.2007
		US 2009-0119504 A1	07.05.2009
		WO 2007-021483 A2	22.02.2007
US 2008-0037793 A1	14.02.2008	EP 1484890 A2	08.12.2004
		EP 1484890 A3	11.07.2012
		EP 1484913 A2	08.12.2004
		EP 1484913 A3	15.04.2009
		US 2004-0247131 A1	09.12.2004
		US 2005-0041802 A1	24.02.2005
		US 2010-0296573 A1	25.11.2010
		US 6724335 B1	20.04.2004
		US 7289632 B2	30.10.2007
		US 7768434 B2	03.08.2010
		US 8111183 B2	07.02.2012

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: KELLETT GLEN M. BARNES & THORNBURG, LLP C/O CPA GLOBAL P.O. BOX 52050 MINNEAPOLIS MN 55402 USA

PCT

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

(PCT Rule 43bis.1)

Date of mailing (day/month/year) 30 AUGUST 2012 (30.08.2012)	
Applicant's or agent's file reference P41624PCT	FOR FURTHER ACTION See paragraph 2 below
International application No. PCT/US2011/065069	International filing date (day/month/year) 15 DECEMBER 2011 (15.12.2011)
Priority date(day/month/year)	
International Patent Classification (IPC) or both national classification and IPC H04L 9/14(2006.01)i, H04L 9/32(2006.01)i	
Applicant INTEL CORPORATION et al	

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
☐ Box No. II Priority
☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐ Box No. IV Lack of unity of invention
☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐ Box No. VI Certain documents cited
☒ Box No. VII Certain defects in the international application
☐ Box No. VIII Certain observations on the international application

2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/KR Korean Intellectual Property Office 189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Date of completion of this opinion 29 AUGUST 2012 (29.08.2012)	Authorized officer Lee Hyoung Il Telephone No. 82-42-481-8199
---	---	---

Form PCT/ISA/237 (cover sheet) (July 2011)

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2011/065069

Box No. 1 Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of :

- ☒ the international application in the language in which it was filed
- ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:

a. a sequence listing filed or furnished

- ☐ on paper
- ☐ in electronic form

b. time of filing or furnishing

- ☐ contained in the international application as filed.
- ☐ filed together with the international application in electronic form.
- ☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2011/065069

**Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability;
citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-47	YES
	Claims	NONE	NO
Inventive step (IS)	Claims	33-34,37-47	YES
	Claims	1-32,35-36	NO
Industrial applicability (IA)	Claims	1-47	YES
	Claims	NONE	NO

2. Citations and explanations :

Reference is made to the following documents:

D1: US 2011-0231923 A1 (BOLLAY BENN SAPIN et al.) 22 September 2011
D2: US 2005-0213768 A1 (DAVID DURHAM et al.) 29 September 2005
D3: US 2010-0299525 A1 (SHAH PARAS et al.) 25 November 2010
D4: US 2008-0037793 A1 (BUER MARK) 14 February 2008

1. Novelty and Inventive Step

1.1 Independent Claim 1

D1, which is considered to be the closest prior art to the subject matter of claim 1, discloses an apparatus for a client to generate random number, send client hello message for SSL handshake initiation, perform a server key exchange and a client key exchange, generate a session key based on secret data, store the session in a data store, establish an encrypted session between the server and the client using the session key. Claim 1 differs from D1 in that the apparatus uses the secure memory. However, D2 discloses an apparatus storing the cryptographic key in a secure storage. Accordingly, claim 1 would have been obvious over D1 in view of D2. Therefore, claim 1 lacks an inventive step under PCT Article 33(3).

1.2 Dependent Claims 2-15

Claims 2-15, which are dependent on claim 1, lack an inventive step under PCT Article 33(3), because the additional features of claims 2-15 are merely matters of design option when the general technical knowledge about the state of the art is used.

1.3 Independent Claim 16

Claim 16 relates to a method performing the functions of the apparatus according to claim 1. Claim 16 is considered to lack an inventive step under PCT Article 33(3), because the subject matter of claim 1 is considered to lack an inventive step under PCT Article 33(3).

[Continued on Supplemental Box]

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2011/065069

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

Claims 35-36 and 46-47 do not comply with PCT Rule 6.4(a) because the multiple dependent claims don't refer to other claims in the alternative way.

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2011/065069

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

[Box V]

[Box V]

1.4 Dependent Claims 17-32

Claims 17-32, which are dependent on claim 16, lack an inventive step under PCT Article 33(3), because the additional features of claims 17-32 are merely matters of design option when the general technical knowledge about the state of the art is used.

1.5 Dependent Claims 33-34

The additional feature of claim 33 dependent on claim 16 is not disclosed in any of the prior art documents, nor is it obvious to a person skilled in the art by the documents. Accordingly, claim 33 is novel and involves an inventive step under PCT Article 33(2) and (3).

The additional feature of claim 34 dependent on claim 16 is not disclosed in any of the prior art documents, nor is it obvious to a person skilled in the art by the documents. Accordingly, claim 34 is novel and involves an inventive step under PCT Article 33(2) and (3).

1.6 Independent Claim 35

Claim 35 relates to a source device including a plurality of instructions performing the method of claims 16-32. Claim 35 is considered to lack an inventive step under PCT Article 33(3), because the subject matters of claims 16-32 are considered to lack an inventive step under PCT Article 33(3).

1.7 Independent Claim 36

Claim 36 relates to one or more machine readable media comprising a plurality of instructions performing the method of claims 16-32. Claim 36 is considered to lack an inventive step under PCT Article 33(3), because the subject matters of claims 16-32 are considered to lack an inventive step under PCT Article 33(3).

1.8 Claims 37-45

The subject matter of claim 37 differs from these prior art documents in generating a hash code as a function of the session key and sending a client completion message to the server that includes the hash code to indicate the client has completed an initial handshake procedure. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 37 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 38-45 are dependent on claim 37 and therefore meet the requirements of PCT Article 33(2) and (3).

1.9 Claims 46-47

Claim 46 relates to a source device including a plurality of instructions performing the method of claims 37-45. Claim 46 is considered to be novel and to involve an inventive step under PCT Article 33(2) and (3), because the subject matters of claim 37-45 are considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

Claim 47 relates to one or more machine readable media comprising a plurality of instructions performing the method of claims 37-45. Claim 47 is considered to be novel and to involve an inventive step under PCT Article 33(2) and (3), because the subject matters of claim 37-45 are considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

[Continued on Supplemental Box]

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2011/065069

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

[Box V]

2. Industrial Applicability

Claims 1-47 are industrially applicable under PCT Article 33(4).

Electronic Acknowledgement Receipt	
EFS ID:	16431576
Application Number:	13997412
International Application Number:	
Confirmation Number:	1045
Title of Invention:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor/Applicant Name:	Hormuzd M. Khosravi
Customer Number:	73486
Filer:	Christopher A. Singh/Jenny Kathman
Filer Authorized By:	Christopher A. Singh
Attorney Docket Number:	P41624US/45631-225521
Receipt Date:	26-JUL-2013
Filing Date:	
Time Stamp:	17:34:18
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P41624US_IDS.pdf	612529 d1252053a2f5862f53cab17042ff94031ea243fa	no	4

Warnings:

Information:

2	Foreign Reference	FR1.pdf	1414117 2001cf96b8116eb778bdc2ed624e2199833dedb9	no	31
Warnings:					
Information:					
3	Non Patent Literature	NPL1.pdf	403207 55c54ca63faa05b6910359efa1077d8c913180d6	no	11
Warnings:					
Information:					
4	Non Patent Literature	NPL2.pdf	3104183 08aea302b1c155c2b18eeea6cca27818f8699a78	no	19
Warnings:					
Information:					
5	Non Patent Literature	NPL3.pdf	919669 0b6a539cc93664667a9281043edd26694e2e1922	no	6
Warnings:					
Information:					
Total Files Size (in bytes):			6453705		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

(51) International Patent Classification:
G06F 21/24 (2006.01)(21) International Application Number:
PCT/US2011/065094(22) International Filing Date:
15 December 2011 (15.12.2011)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): **INTEL CORPORATION** [US/US]; 2200 Mission College Blvd, Santa Clara, CA 95052 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **KHOSRAVI, Hormuzd** [IN/US]; 4816 NW 166th Ave, Portland, OR 97229 (US). **AGRAWAL, Sachin** [IN/US]; 2111 NE 25th Ave, Hillsboro, OR 97229 (US). **VENKATARAMANAN, Anirudh** [IN/US]; 2111 NE 25th Avenue, Hillsboro, OR 97214 (US).(74) Agent: **KELLET, Glen M.**; Barnes & Thornburg, LLP, c/o CPA Global, PO Box 52050, Minneapolis, MN 55402 (US).

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

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

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

Declarations under Rule 4.17:

— of inventorship (Rule 4.17(iv))

Published:

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

(54) Title: METHOD, DEVICE, AND SYSTEM FOR SECURELY SHARING MEDIA CONTENT FROM A SOURCE DEVICE

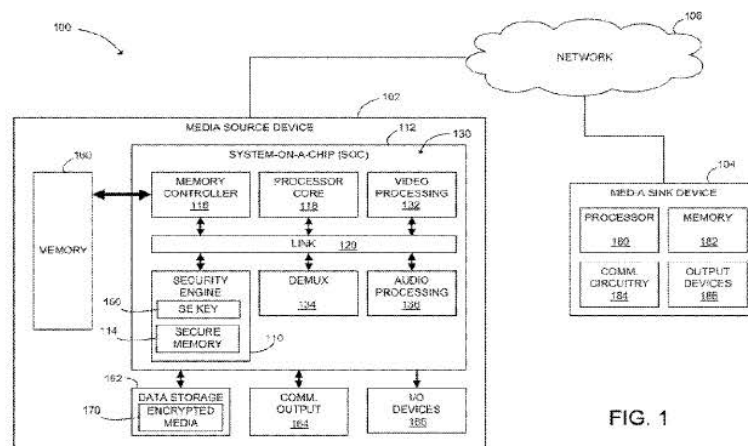


FIG. 1

(57) Abstract: A method, device, and system for sharing media content with a sink device includes performing a cryptographic key exchange with the sink device and generating an authorization key in a security engine of a system-on-a-chip (SOC) of a source device. The method may also include generating an exchange key as a function of the authorization key and a packet key as a function of the exchange key. Such key generation occurs in the security engine of the SOC, and the keys are stored in a secure memory of the security engine.

METHOD, DEVICE, AND SYSTEM FOR SECURELY SHARING MEDIA CONTENT FROM A SOURCE DEVICE

BACKGROUND

The generation, sharing, and consumption of digital media content continue to grow as consumer devices capable of interacting with such content become ubiquitous. The desire to share digital media content between consumer devices, especially in the home environment, is increasing in unison with the increased exposure to digital media content. To ensure that two media devices can properly share digital media content while also ensuring the digital rights of such content remain protected, digital media content delivery protocols have been developed by various authority organizations. One such organization is the Digital Living Network Alliance (DLNA), which has established various interoperability protocols and standards for sharing media content between media devices. For example the Digital Transmission Content Protection (DTCP) protocol is a security protocol that defines security guidelines and compliance requirements for securely sharing media content between media devices. Digital Transmission Content Protection over Internet Protocol (DTCP-IP) is a sub-set protocol of the DTCP protocol directed to sharing media content between media devices over a network.

Some media devices utilize system-on-a-chip (SOC) designs due to their relatively small footprint. SOC devices are integrated circuits that incorporate various components, in addition to the processing core, of electronic systems on a single die. For example, an SOC may include a processor core, memory controller, video components, audio components, and/or communication components on a single chip.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention described herein is illustrated by way of example and not by way of limitation in the accompanying figures. For simplicity and clarity of illustration, elements illustrated in the figures are not necessarily drawn to scale. For example, the dimensions of some elements may be exaggerated relative to other elements for clarity. Further, where considered appropriate, reference labels have been repeated among the figures to indicate corresponding or analogous elements.

FIG. 1 is a simplified block diagram of at least one embodiment of a system for sharing media content from a media source device having a system-on-a-chip (SOC) to a media sink device;

FIG. 2 is a simplified flow diagram of at least one embodiment of a method for provisioning a security engine of the SOC of the media source device;

FIG. 3 is a simplified flow diagram of at least one embodiment of a method for authenticating the media sink device of FIG. 1; and

FIG. 4 is a simplified flow diagram of at least one embodiment of a method for securely sharing media content with the media sink device of FIG. 1.

5 DETAILED DESCRIPTION OF THE DRAWINGS

While the concepts of the present disclosure are susceptible to various modifications and alternative forms, specific exemplary embodiments thereof have been shown by way of example in the drawings and will herein be described in detail. It should be understood, however, that there is no intent to limit the concepts of the present disclosure to the particular forms disclosed, but on the contrary, the intention is to cover all modifications, equivalents, and alternatives
10 consistent with the present disclosure and the appended claims.

In the following description, numerous specific details such as logic implementations, opcodes, means to specify operands, resource partitioning/sharing/duplication implementations, types and interrelationships of system components, and logic partitioning/integration choices are set forth in order to provide a more thorough understanding of the present disclosure. It will be appreciated, however, by one skilled in the art that embodiments of the disclosure may be practiced without such specific details. In other instances, control structures, gate level circuits and full software instruction sequences have not been shown in detail in order not to obscure the invention. Those of ordinary skill in the art, with the included descriptions, will be able to
15 implement appropriate functionality without undue experimentation.

References in the specification to “one embodiment,” “an embodiment,” “an example embodiment,” etc., indicate that the embodiment described may include a particular feature, structure, or characteristic, but every embodiment may not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is within the knowledge of one skilled in the art to effect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described.
25

Embodiments of the invention may be implemented in hardware, firmware, software, or any combination thereof. Embodiments of the invention implemented in a computer system may include one or more bus-based interconnects or links between components and/or one or more point-to-point interconnects between components. Embodiments of the invention may also be implemented as instructions carried by or stored on a machine-readable medium, which may be
30

read and executed by one or more processors. A machine-readable medium may be embodied as any device, mechanism, or physical structure for storing or transmitting information in a form readable by a machine (e.g., a computing device). For example, a machine-readable medium may be embodied as read only memory (ROM); random access memory (RAM); magnetic disk
5 storage media; optical storage media; flash memory devices; mini- or micro-SD cards, memory sticks, electrical signals, and others.

In the drawings, specific arrangements or orderings of schematic elements, such as those representing devices, modules, instruction blocks and data elements, may be shown for ease of description. However, it should be understood by those skilled in the art that the specific
10 ordering or arrangement of the schematic elements in the drawings is not meant to imply that a particular order or sequence of processing, or separation of processes, is required. Further, the inclusion of a schematic element in a drawing is not meant to imply that such element is required in all embodiments or that the features represented by such element may not be included in or combined with other elements in some embodiments.

In general, schematic elements used to represent instruction blocks may be implemented using any suitable form of machine-readable instruction, such as software or firmware applications, programs, functions, modules, routines, processes, procedures, plug-ins, applets, widgets, code fragments and/or others, and that each such instruction may be implemented using any suitable programming language, library, application programming interface (API), and/or other software
15 development tools. For example, some embodiments may be implemented using Java, C++, and/or other programming languages. Similarly, schematic elements used to represent data or information may be implemented using any suitable electronic arrangement or structure, such as a register, data store, table, record, array, index, hash, map, tree, list, graph, file (of any file type), folder, directory, database, and/or others.

Further, in the drawings, where connecting elements, such as solid or dashed lines or arrows, are used to illustrate a connection, relationship or association between or among two or more other schematic elements, the absence of any such connecting elements is not meant to imply that no connection, relationship or association can exist. In other words, some connections, relationships or associations between elements may not be shown in the drawings so as not to
25 obscure the disclosure. In addition, for ease of illustration, a single connecting element may be used to represent multiple connections, relationships or associations between elements. For example, where a connecting element represents a communication of signals, data or instructions, it should be understood by those skilled in the art that such element may represent one or multiple signal paths (e.g., a bus), as may be needed, to effect the communication.

Referring now to FIG. 1, a system 100 for sharing digital media content includes a media source device 102, a media sink device 104, and a network 106. In operation, the media source device 102 may share digital media content with the media sink device 104 over the network 106 using a security protocol. In the illustrative embodiment, a Digital Transmission Content Protection
5 (DTCP) security protocol is used, such as the Digital Transmission Content Protection over Internet Protocol (DTCP-IP). However, other security protocols may be used in other embodiments.

The media source device 102 initially authenticates the media sink device 104. If the media sink device 104 is successfully authenticated, the media source device 102 and sink device 104
10 perform a key exchange to generate a shared secret key. The media source device 102 generates a packet encryption key based on the shared key and encrypts the media content using the packet encryption key. The media sink device 104 may decrypt the media content using a shared exchange key. To ensure the security and protection of the media content, the keys and other cryptographic functions generated by the media source device 102 are done so within a security
15 engine 110 of a system-on-a chip (SOC) 112 of the media source device 102. The media source device 102 maintains the keys in secrecy within a secure memory 114 of the security engine 110. In this way, digital media content may be shared with the media sink device 104 while ensuring the security of the digital media content and the encryption keys used to facilitate such secured sharing.

The media source device 102 may be embodied as any type of device capable of delivering digital media content to the media sink device 104. For example, the media source device 102 may be embodied as a set-top box, a digital television, a smartphone, a tablet computer, a laptop computer, a mobile internet device (MID), a desktop computer, or other device capable of delivery of media content. The media source device 102 may be configured to deliver any type
25 of digital media content to the media sink device 104 including, for example, movies, pictures, images, songs, audio and/or video recordings, and/or any other type of audio, video, and/or audio and video content.

As discussed above, the media source device 102 includes the SOC 112, which may be embodied as any type of system-on-a-chip device having various components and structures. In the illustrative embodiment of FIG. 1, the SOC 112 includes the security engine 110, a memory controller 116, a processor core 118, and bus a plurality of hardware peripherals 130, which are communicatively coupled to each other a link 120. The link 120 may be embodied as any type
30 of interconnect such as a bus, point-to-point, or other interconnect capable of facilitating communication between the various components of the SOC 122. The hardware peripherals 130

may include any type of hardware peripheral component depending upon the intended functionality of the SOC 112. For example, in the illustrative embodiment, the hardware peripherals 130 include a demux 132 to separate audio and video content streams, video processing component(s) 134 to process video content, and audio processing component(s) 136 to process audio content. Of course, it should be appreciated that the hardware peripherals 130 of the SOC 112 have been simplified in the illustrative embodiment of FIG. 1 and that the SOC 112 may include additional, different, and/or greater detailed hardware peripherals 130, which are not illustrated in FIG. 1 for clarity of the disclosure.

The security engine 110 may be embodied as a security co-processor or processing circuitry separate from the processor core 118. The security engine 110 includes a security key 150 and the secure memory 114, which is accessible only by the security engine 110. The security engine 110 stores the security key 150, and other cryptographic keys as discussed below, in the secure memory 114. In the illustrative embodiment, the security key 150 is provisioned during the manufacturing of the SOC 112, but may be generated by the SOC 112 during operation in other embodiments. For example, in some embodiments, the security key 150 is based on blown fuses within the security engine 110 itself. Additionally or alternatively, the security engine 110 may include a key-generating module, such as a trusted platform module (TPM), to generate the security key 150. During use, the security engine 110 may use any number of security keys 150, which may be identical or different from each other.

In some embodiments, the media source device 102 may include additional components and structures other than the SOC 112 depending on the type and intended use of the media source device 102. For example, in the illustrative embodiment of FIG. 1, the media source device 102 includes a system memory 160, a data storage 162, a communications output 164, and one or more input/output devices 166. The system memory 160 may be embodied as any type of main memory or data storage locations including, for example, dynamic random access memory devices (DRAM), synchronous dynamic random access memory devices (SDRAM), double-data rate synchronous dynamic random access memory device (DDR SDRAM), mask read-only memory (ROM) devices, erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM) devices, flash memory devices, and/or other volatile and/or non-volatile memory devices.

The data storage 162 may be embodied as any type of device or devices configured for the short-term or long-term storage of data such as, for example, memory devices and circuits, memory cards, hard disk drives, solid-state drives, or other data storage devices. In the illustrative

embodiment of FIG. 1, encrypted media content 170 may be stored in the data storage 162, which may be subsequently shared with the media sink device 104 as discussed below.

The communications output 164 may be embodied as a simplified output or as various circuits and/or devices to facilitate, for example, communications with the media sink device 104. For example, the communications output 164 (and/or communication circuitry within the SOC 112) may any suitable communication protocol such as Ethernet (i.e. the IEEE 802.3 standard) or Wi-Fi® (i.e., the IEEE 802.11 standard), and/or other communication protocols or standards.

The input/output devices 166 may be embodied as any type of I/O device for interacting with the media source device 102. For example, the I/O devices 166 may include output devices such as a display for displaying media on the media source device 102 and speakers for playing audio content, and/or input devices such as a remote control receiver, a keyboard, a mouse, and/or the like.

The media sink device 104 may be embodied as any type of media device capable of communicating with and receiving media content from the media source device 102. For example, the media sink device 104 may be embodied as a digital television, a smartphone, a tablet computer, a laptop computer, a mobile internet device (MID), a desktop computer, or other electronic device capable of receiving of media content from the media source device 102.

The illustrative media sink device 104 includes a processor 180, a memory 182, communication circuitry 184, and one or more output devices 186, which may be similar to such components found in other media devices. For example, the processor 180 may be embodied as any type of processor capable of executing software/firmware, such as a microprocessor, digital signal processor, microcontroller, or the like, and may include one or more processing cores. The memory 182 may be embodied as any type of memory or data storage locations including, for example, dynamic random access memory devices (DRAM), synchronous dynamic random access memory devices (SDRAM), double-data rate synchronous dynamic random access memory device (DDR SDRAM), mask read-only memory (ROM) devices, erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM) devices, flash memory devices, and/or other volatile and/or non-volatile memory devices. The communication circuitry

The communication circuitry 184 may be embodied any type of circuitry and/or device to facilitate, for example, communications with the media source device 102. For example, the communication circuitry 184 may support communication protocols such as Ethernet (i.e. the IEEE 802.3 standard) or Wi-Fi® (i.e., the IEEE 802.11 standard), and/or other communication protocols or standards. The output devices 186 may be embodied as any type of output device

for playing, rendering, or otherwise delivering the media content to a user. For example, the output devices 186 may include a display for displaying media on the media sink device 104 and speakers for playing audio content.

The network 106 may be embodied as any number of various wired and/or wireless networks. In the illustrative embodiment, the network 106 is a local area network (LAN) such as a home network, but may be embodied as or otherwise include other networks in other embodiments. For example, in some embodiments, the network 106 may be embodied as an ad-hoc or point-to-point network or a wide area network (WAN). As discussed in more detail below, the media source device 102 is configured to share media content with the media sink device 104 over the network 106.

Referring now to FIG. 2, in use, the security engine 110 of the SOC 112 of the media source device 102 may be provisioned with key material for facilitating the delivery of media content to various sink devices. To do so, the media source device 102 may execute a method 200 for provisioning the security engine 110. The method 200 begins with block 202 in which the security engine 110 receives a source device certificate, a private device key, and a public certification key. The source device certificate, the private device key, and the public certification key are typically generated by a certification authority organization, which acts as a third-party verifier of the authentication of the particular device. The source device certificate includes a unique device identifier or number assigned to the media source device 102 by the certification authority organization to verify the media source device 102 to other media devices. The unique device identifier may also be used to revoke the authorization of the media source device 102 via distribution of a System Renewability Message (SRM) revocation list. The private device key may be used by the media source device 102 to sign the packets so as to authenticate the media source device 102 to other media devices as discussed in more detail below. Conversely, the public certification key may be used by the media sink device 104 to verify the packets received from the media source device 102 during authentication.

In block 204, the security engine 110 stores the source device certificate and the public certification key in the secure memory 114. In some embodiments, the security engine 110 may encrypt the source device certificate and/or the public certification key using the security key 150 stored in the security engine 110. In such embodiments, the security engine 110 may store the encrypted source device certificate and/or the encrypted public certification key in the secure memory 114, in the memory 160, or in the data storage 162.

In block 206, the security engine 110 encrypts the private device key using the security key 150 stored in the security engine 110. In some embodiments, the security engine 110 may also

secure the encrypted private device key in block 208. To do so, for example, the security engine may perform a Cipher Block Chaining Message Authentication Code (CBC-MAC) on the encrypted private device key. Alternatively, the security engine 110 may use some other cryptographic methodology to secure the encrypted private device key. Regardless, in block 5 210, the security engine 110 stores the secured, encrypted private device key in the secure memory 114. In this way, the security engine 110 of the SOC 112 of the media source device 102 is provisioned with initial key material to facilitate delivering media to sink devices in a secure manner.

Referring now to FIG. 3, the media source device 102 may use a Digital Transmission Content 10 Protection (DTCP) protocol to share media content with the sink device 104 as discussed above. Prior to the actual sharing of media content with the media sink device 104, the media source device 102 is configured to authenticate the media sink device 104 and negotiate cryptographic keys with the media sink device 104 to facilitate the delivery of media content thereto. To do so, the media source device 102 may execute a method 300 for authenticating the media sink device 15 104. The method 300 begins with block 302 in which the media source device 102 determines whether a request for authorization has been received from the media sink device 104. If so, in block 304, the media source device 102 receives the sink device certificate and sink public cryptographic key. Similar to the source device certificate of the media source device 102, the sink device certificate is issued by the certification authority organization to verify the media 20 sink device 104. The sink device certificate includes a unique device identifier assigned by the certification authority organization, which uniquely identifies the media sink device 104 from other media devices. The sink public key may be used by the security engine 110 in subsequent communications to verify that received messages were originated by the media sink device 104. In block 306, the media source device 102 verifies the sink device certificate using the public 25 certification key. In embodiments in which the public certification key is stored in an encrypted form, the security engine 110 of the SOC 112 of the media source device 102 retrieves the encrypted public certification key and decrypts the key using the security key 150. The public certification key is used to verify that the sink device certificate has been properly signed by an authorized media device. As such, in block 308, the media source device 102 determines 30 whether the media sink device 104 is properly certified using the public certification key. If not, the method 300 advances to block 310 in which the media source device 102 rejects the authorization request from the media sink device 104.

However, if the sink device certificate is verified in block 308, the media source device 102 further verifies that the certification of the media sink device 104 has not been revoked. To do

so, the media source device 102 may utilize an SRM list, which includes identifiers of devices whose certification has been previously revoked. The SRM list of the media source device 102 may be stored in the secure memory 114 of the SOC 112 in some embodiments. Alternately, the SRM list may be stored in the memory 160 or the data storage 162 in an encrypted or unencrypted form. As new devices are added to the local network of media devices, the SRM list is updated on each device. As such, in block 312, the media source device 102 compares the unique device identifier of the media sink device 104, which was received with the sink device certification, against the current SRM list. If, in block 314, the certification of the media sink device 104 is determined to have been revoked, the method 300 advances to block 310 in which the media source device 102 rejects the authorization request from the media sink device 104. If, however, the certification of the media sink device is not revoked, the method 300 advances to block 316 in which the security engine 110 of the SOC 112 stores the sink public key in the secure memory 114 of the security engine 110. In block 318, the security engine 110 of the SOC 112 retrieves the source device certificate and private source key from the secure memory 114. Additionally, in block 318, the media source device 102 may retrieve a source public key and a source certificate and send the key and certificate to the media sink device 104. The source public key may be used by the media sink device 104 in subsequent communications to verify that received messages were originated by the media source device 102. If the media source device is not verified in block 320, the method 300 advances to block 310 in which the media source device 102 rejects the authorization request from the media sink device 104. Alternatively, in some embodiments, the media source device 102 may attempt to resend the source certificate and source public key to the media sink device 104. However, if the source certificate is verified in block 320, the method 300 advances to block 322 (see FIG. 3B) in which the media source device 102 and the media sink device 104 perform a key exchange. The key exchange is used to establish a shared secret key in the media source device 102 and the media sink device 104 without prior provisioning of the devices 102, 104 with corresponding keys. The media source device 102 may use any appropriate key exchange algorithm to effect the establishment of a shared secret. In the illustrative embodiment, the media source device 102 uses an elliptic curve Diffie-Hellman (ECDH) key exchange in block 322. To do so, the media source device 102 provisions the media sink device 104 for the Diffie-Hellman key exchange in block 324. For example, media source device 102 may select the elliptic curve, E, and the base point, G, to be used in generating the shared secret. The domain parameters associated with the elliptic curve and base point selections are sent to the media sink device 104 in block 324. Of course, in other

embodiments, other Diffie-Hellman key exchanges may be used such as, for example, Rivest-Shamir-Adleman (RSA) Diffie-Hellman key exchange. In such embodiments, the media source device 102 generates the domain parameters (e.g., selects a prime number and a primitive root) and transmits the domain parameters to the media sink device 104 in block 324.

- 5 The security engine 110 of the SOC 112 of the media source device 102 may sign the transmission of block 324, and other subsequent transmissions, with the private source key corresponding to the public source key provided to the media sink device 104 in block 318. In some embodiments, the private source key may be the security key 150 or other key stored in the secure memory 114 of the security engine 110.
- 10 In block 326, the security engine 110 of the SOC 112 generates a source Diffie-Hellman public and private key based on the domain parameters generated or otherwise determined in block 324. The media source device 102 sends the public Diffie-Hellman key to the media sink device 104 in block 326. Again, such transmission may be signed by the security engine using the private source key (e.g., security key 150).
- 15 In block 328, the media source device 102 receives the sink Diffie-Hellman public key from the media sink device 104, which may be calculated in a similar manner as described above in regard to the media source device 102. The media source device 102 stores the sink Diffie-Hellman public key in the secure memory 114 of the security engine 110. Additionally, in block 328, the media source device 102 verifies the signature of the sink Diffie-Hellman public key
- 20 message, and other subsequent messages received from the media sink device 104, using the sink public key stored in the secure memory 114. If the media source device 102 determines that the message, or other message, is not properly signed, the method 300 advances to block 310 in which the media source device 102 rejects the authorization request from the media sink device 104.
- 25 In block 332, the security engine 110 of the SOC 112 of generates an authentication key, K_{AUTH} , using the source Diffie-Hellman private key and the sink Diffie-Hellman public key. The security engine 110 may store the authentication key, K_{AUTH} , in the secure memory 114. In the illustrative embodiment, for example, the security engine 110 performs an elliptic curve scalar multiplication using the source Diffie-Hellman private key and the sink Diffie-Hellman public to
- 30 generate the authentication key, K_{AUTH} . Of course, other cryptographic calculations may be performed in block 332 in other embodiments to generate the authentication key, K_{AUTH} . However, any such calculations occur in the security engine 110 to maintain the security of the authentication process.

In block 334, the security engine 110 generates an exchange key, K_X . In the illustrative embodiments, the exchange key, K_X , is embodied as a random nonce, but may be generated using other methodologies or calculations in other embodiments. The nonce is a random or pseudo-random number intended to be used only once in cryptographic functions to thwart, for example, replay attacked.

In block 336, the security engine 110 of the SOC 112 scrambles the exchange key, K_X , using the authentication key, K_{AUTH} . The security engine 110 may use any suitable cryptographic calculation or scrambling algorithm/methodology to scramble the exchange key, K_X . Subsequently, in block 338, the media source device 102 sends the scrambled exchange key to the media sink device 104. Again, as discussed above, such message may be signed by the security engine 110 of the SOC 112 using the private device key (e.g., the security key 150). The media sink device 104 may generate the exchange key, K_X , using the shared authentication key, K_{AUTH} . In this way, a shared secret key is established between the media source device 102 and the media sink device 104 using the security engine 110 of the SOC 112 of the media source device 102.

After the media source device 102 and the media sink device 104 have established the shared secret key via the method 300, the media source device 102 may share media content with the media sink device 104 using the shared secret key. To do so, the media source device 102 may execute a method 400 for sharing media content with the media sink device 104. The method 400 begins with block 402 in which the media source device 102 obtains media content to be shared with the media sink device 104. Such media content may be stored in the media source device 102 as encrypted media content 170 or may be received by the media source device 102 from an external source (e.g., streamed or transmitted to the media source device 102 such as digital cable TV).

In block 404, the security engine 110 of the media source device 102 generates a random nonce, which is used to combat replay attacks. In block 406, the security engine 110 generates a packet encryption key, K_C , using the exchange key, K_X , the random nonce generated in block 404, and an encryption mode indicator (EMI), which is used for copy control of media content. In the illustrative embodiment, the security engine 110 utilizes an Advanced Encryption Standard – Cipher Block Chaining (AES-CBC) algorithm to generate the packet encryption key, K_C . However, other encryption algorithms may be used in other embodiments. It should be appreciated that a new packet encryption key, K_C , is generated in the security engine for each packet of media content sent to the media sink device 104.

In block 408, the security engine 110 encrypts the media content, or a portion thereof, to be sent to the media sink device 104 using the packet encryption key, K_C . Of course, if the media content is stored on the media source device 102 in an encrypted format (which would be encrypted using an encryption key other than the packet encryption key, K_C), the media source
5 device 102 decrypts the media content before re-encrypting the media content with the packet encryption key, K_C .

In block 410, the media source device 102 encapsulates the encrypted media content, the random nonce generated in block 404, and the EMI into a Protected Content Packet (PCP) packet. Of course, other encapsulation methodologies may be used in other embodiments. Subsequently, in
10 block 412, the media source device 102 sends the encapsulated packet to the media sink device 104. It should be appreciated that the media source device 102 may send multiple packets to the media sink device 104 to effect the secure delivery of the media content to the media sink device 104. The media sink device 104 may decrypt the media content using the exchange key, K_X , as discussed above.

15 While the disclosure has been illustrated and described in detail in the drawings and foregoing description, such an illustration and description is to be considered as exemplary and not restrictive in character, it being understood that only illustrative embodiments have been shown and described and that all changes and modifications consistent with the disclosure and recited claims are desired to be protected.

20

CLAIMS:

1. A system-on-a-chip apparatus comprising:
a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, the security engine to:
5 perform a cryptographic key exchange with a sink device;
generate an authorization key as a function of the cryptographic key exchange;
and
generate an exchange key using the authorization key;
store the authorization key and the exchange key in the secure memory; and
10 encrypt media content as a function of the exchange key to share the encrypted media content with the sink device using a Digital Transmission Content Protection security protocol.
2. The system-on-a-chip apparatus of claim 1, wherein the security engine to
15 perform a Diffie-Hellman cryptographic key exchange with the sink device to generate the authorization key.
3. The system-on-a-chip apparatus of claim 2, wherein the Diffie-Hellman cryptographic key exchange is an elliptic curve Diffie-Hellman cryptographic key exchange.
20
4. The system-on-a-chip apparatus of claim 3, wherein the security engine to generate a source Diffie-Hellman public key and a source Diffie-Hellman private key.
5. The system-on-a-chip apparatus of claim 3, wherein the security engine to
25 receive a sink Diffie-Hellman public key from the sink device.
6. The system-on-a-chip apparatus of claim 5, wherein the security engine to perform an elliptic curve scalar multiplication as a function of the source Diffie-Hellman private key and the sink Diffie-Hellman public key.
30
7. The system-on-a-chip apparatus of claim 1, wherein the security engine to generate a first exchange key and generate a scrambled exchange key using the first exchange key and the authorization key.

8. The system-on-a-chip apparatus of claim 1, wherein the security engine to obtain media content to share with the sink device, generate a packet encryption key as a function of the exchange key, and encrypt the content media using the packet encryption key.

5

9. The system-on-a-chip apparatus of claim 8, wherein the security engine to generate a random number in the security engine and generate the packet encryption key as a function of the exchange key and the random number.

10

10. The system-on-a-chip apparatus of claim 9, wherein the security engine to encapsulate the encrypted content media, the random number, and an encryption mode indicator.

15

11. The system-on-a-chip apparatus of claim 1, wherein the security engine to receive a certificate from the sink device, retrieve a public certification key from the secure memory, and verify certificate received from the sink device using the public certification key.

20

12. The system-on-a-chip apparatus of claim 11, wherein the security engine to receive a sink public key from the sink device and store the sink public key in the secured memory, the sink public key to authenticate communications received from the sink device.

13. The system-on-a-chip apparatus of claim 1, wherein the security engine to generate a security key and store the security key in the secured memory of the security engine.

25

14. A method comprising:
performing, on a source device, a cryptographic key exchange with a sink device;
generating an authorization key in a security engine of a system-on-a-chip of the source device as a function of the cryptographic key exchange;

storing the authorization key in a secure memory of the security engine of the system-on-a-chip;

30

generating an exchange key in the security engine of the system-on-a-chip using the authorization key;

storing the exchange key in the secure memory of the security engine of the system-on-a-chip, the exchange key to encrypt media content for sharing with the sink device.

15. The method of claim 14, further comprising:
receiving, on the source device, an authorization request from the sink device to
share media content with the sink device; and
sharing the media content with the sink device using a Digital Transmission
5 Content Protection security protocol by performing the method of claim 1.

16. The method of claim 1, wherein performing a cryptographic key exchange
comprises performing a Diffie-Hellman cryptographic key exchange with the sink device.

10 17. The method of claim 16, wherein performing the Diffie-Hellman
cryptographic key exchange comprises performing an elliptic curve Diffie-Hellman
cryptographic key exchange.

18. The method of claim 17, wherein performing the elliptic curve Diffie-
15 Hellman cryptographic key exchange comprises generating a source Diffie-Hellman public key
and a source Diffie-Hellman private key in the security engine of the system-on-a-chip.

19. The method of claim 17, wherein performing the Diffie-Hellman
cryptographic key exchange comprises receiving a sink Diffie-Hellman public key from the sink
20 device.

20. The method of claim 19, wherein generating the authorization key
comprises performing an elliptic curve scalar multiplication in the security engine of the system-
on-a-chip as a function of the source Diffie-Hellman private key and the sink Diffie-Hellman
25 public key.

21. The method of claim 14, wherein generating the exchange key in the
security engine comprises:
generating a first exchange key in the security engine, and
30 generating a scrambled exchange key in the security engine of the system-on-a-
chip using the first exchange key and the authorization key.

22. The method of claim 21, wherein generating an exchange key comprises
generating a random number in the security engine of the system-on-a-chip.

23. The method of claim 14, further comprising:
obtaining content media to share with the sink device;
generating a packet encryption key in the security engine of the system-on-a-chip
5 as a function of the exchange key; and
encrypting the content media using the packet encryption key.

24. The method of claim 23, wherein generating a packet encryption key
comprises:
10 generating a random number in the security engine; and
generating a packet encryption key as a function of the exchange key and the
random number.

25. The method of claim 24, further comprising:
15 encapsulating the encrypted content media, the random number, and an
encryption mode indicator in the security engine of the system-on-a-chip; and
transmitting the encapsulated packet to the sink device.

26. The method of claim 14, further comprising:
20 receiving a certificate from the sink device;
retrieving a public certification key from a secure memory of the security engine
of the system-on-a-chip; and
verifying the certificate received from the sink device using the public
certification key.

27. The method of claim 26, further comprising:
receiving a sink public key from the sink device; and
storing the sink public key in the secured memory of the security engine of the
system-on-a-chip, the sink public key to authenticate communications received from the sink
30 device.

28. The method of claim 14, further comprising:
receiving a public certification key with the security engine of the system-on-a-
chip; and

storing the public certification key in secure memory of the security engine, the public certification key to verify certificates received from the sink device.

29. The method of claim 14, further comprising:
5 generating a security key in the security engine of the system-on-a-chip; and
storing the security key in the secured memory of the security engine.
30. The method of claim 29, further comprising:
10 receiving a source private device key with the security engine of the system-on-a-
chip;
encrypting the source private device key using the security key; and
storing the encrypted source private device key in the secure memory of the
security engine of the system-on-a-chip.
31. The method of claim 30, further comprising generating a source certificate
15 in the security engine of the system-on-a-chip using the source private device key.
32. A source device comprising:
a system-on-a-chip having a security engine, the system-on-a-chip including a
20 plurality of instructions that when executed results in the system-on-a-chip performing the
method of any of claims 14-30.
33. One or more machine readable media comprising a plurality of
instructions stored thereon that in response to being executed by a source device result in the
25 source device performing the method of any of claims 14-30.
34. A method comprising:
sharing media content with a sink device using a Digital Transmission Content
Protection protocol by:
30 generating a source Diffie-Hellman private key in a security engine of a
system-on-a-chip of a source device;
receiving a sink Diffie-Hellman public key from a sink device;

generating an authorization key in the security engine of the system-on-a-chip as a function of the source Diffie-Hellman private key and the sink Diffie-Hellman public key;

5 generating an exchange key in the security engine of the system-on-a-chip;

generating a scrambled exchange key in the security engine of the system-on-a-chip using the exchange key and the authorization key;

generating a random number in the security engine of the system-on-a-chip;

10 generating a packet encryption key in the security engine of the system-on-a-chip as a function of the exchange key and the random number; and

encrypting media content using the packet encryption key.

35. The method of claim 34, wherein generating the authorization key
15 comprises performing an elliptic curve scalar multiplication in the security engine of the system-on-a-chip as a function of the source Diffie-Hellman private key and the sink Diffie-Hellman public key.

36. The method of claim 34, wherein generating an exchange key comprises
20 generating a random number in the security engine of the system-on-a-chip.

37. The method of claim 34, further comprising:
 encapsulating the encrypted content media, the random number, and an
encryption mode indicator in the security engine of the system-on-a-chip; and
25 transmitting the encapsulated packet to the sink device.

38. A source device comprising:
 a system-on-a-chip having a security engine, the system-on-a-chip including a
plurality of instructions that when executed results in the system-on-a-chip performing the
30 method of any of claims 34-37.

39. One or more machine readable media comprising a plurality of
instructions stored thereon that in response to being executed by a source device result in the
source device performing the method of any of claims 34-27.

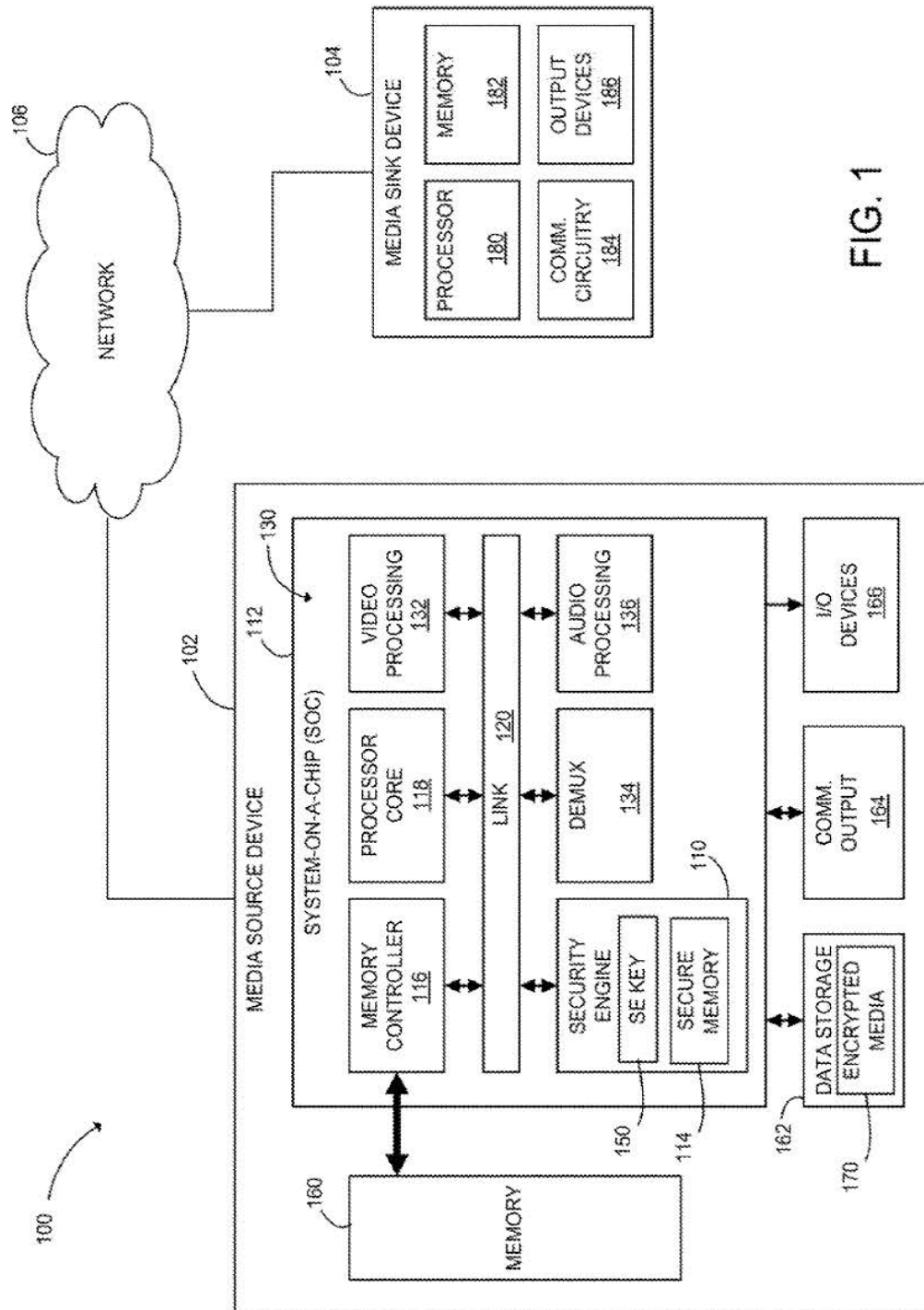


FIG. 1

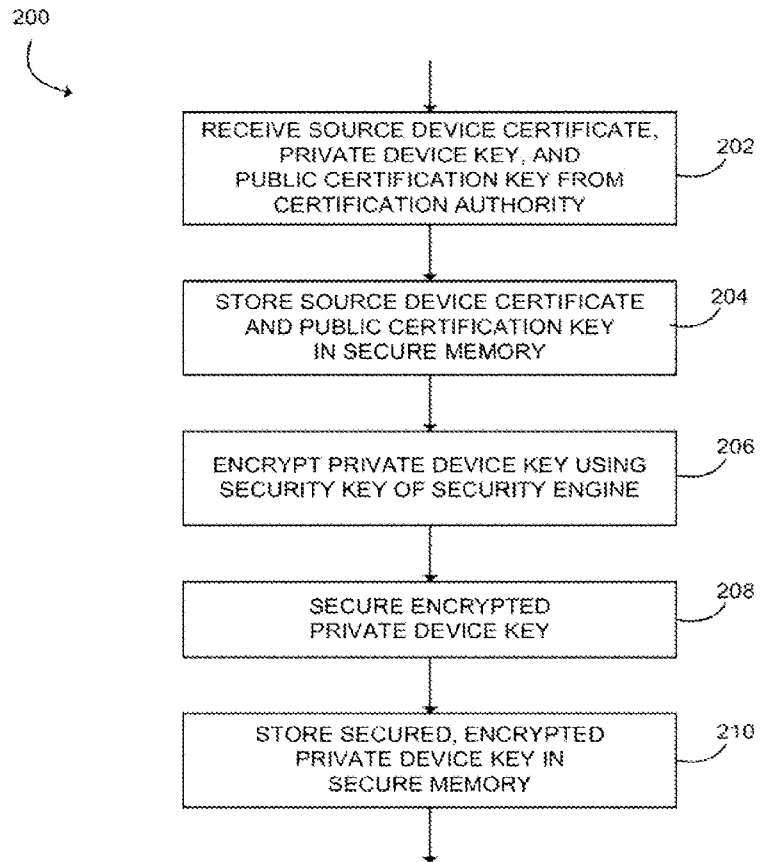


FIG. 2

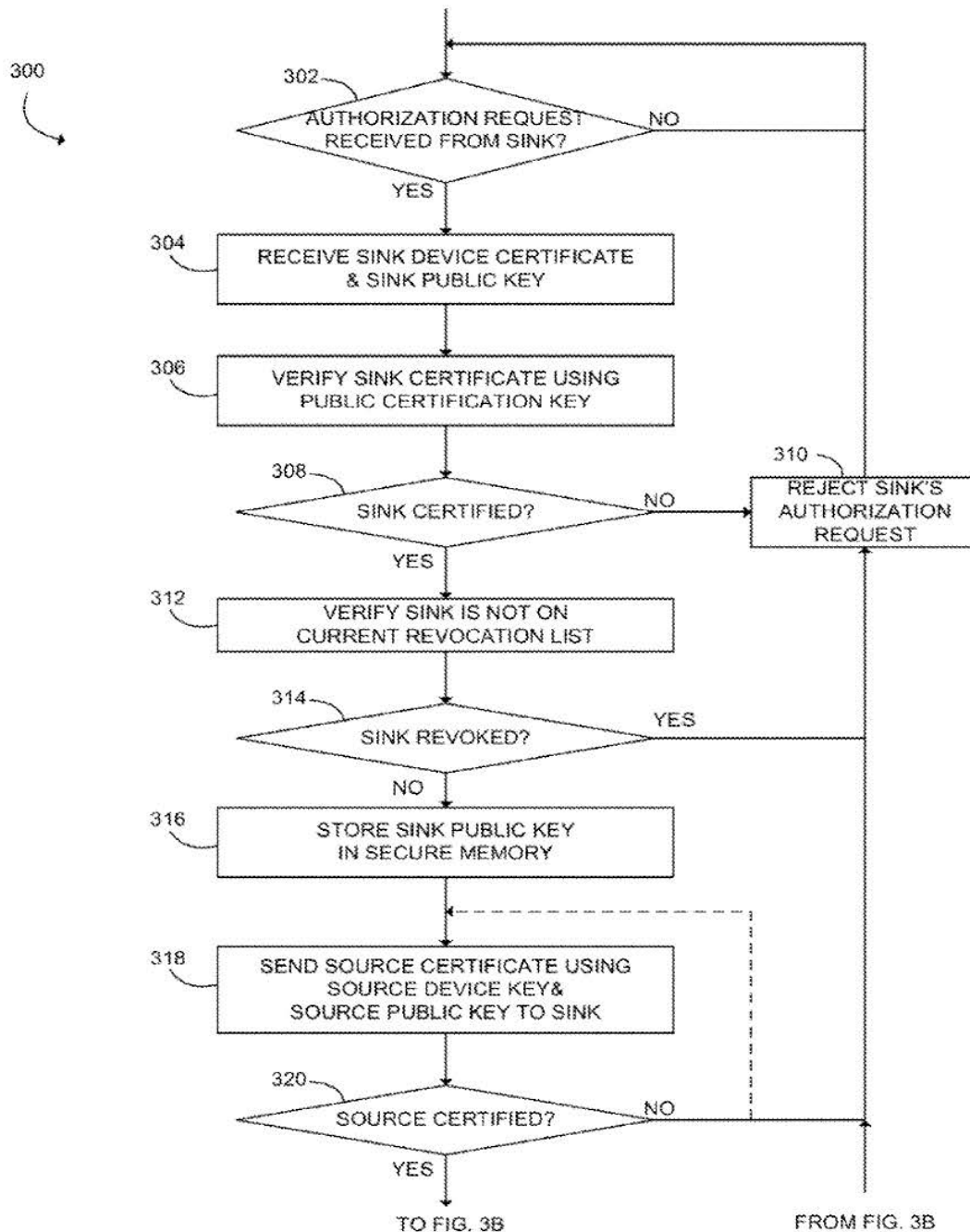


FIG. 3A

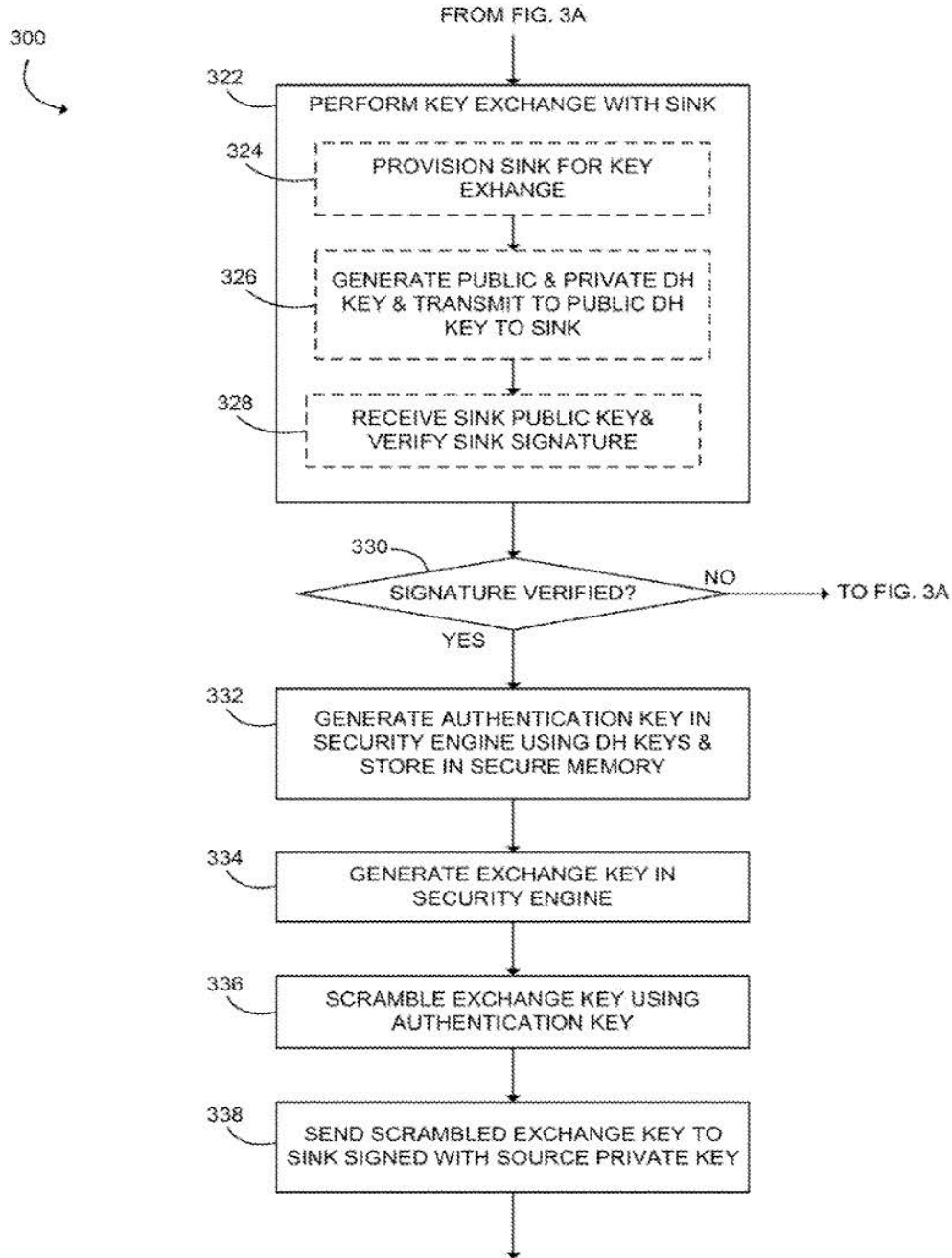


FIG. 3B

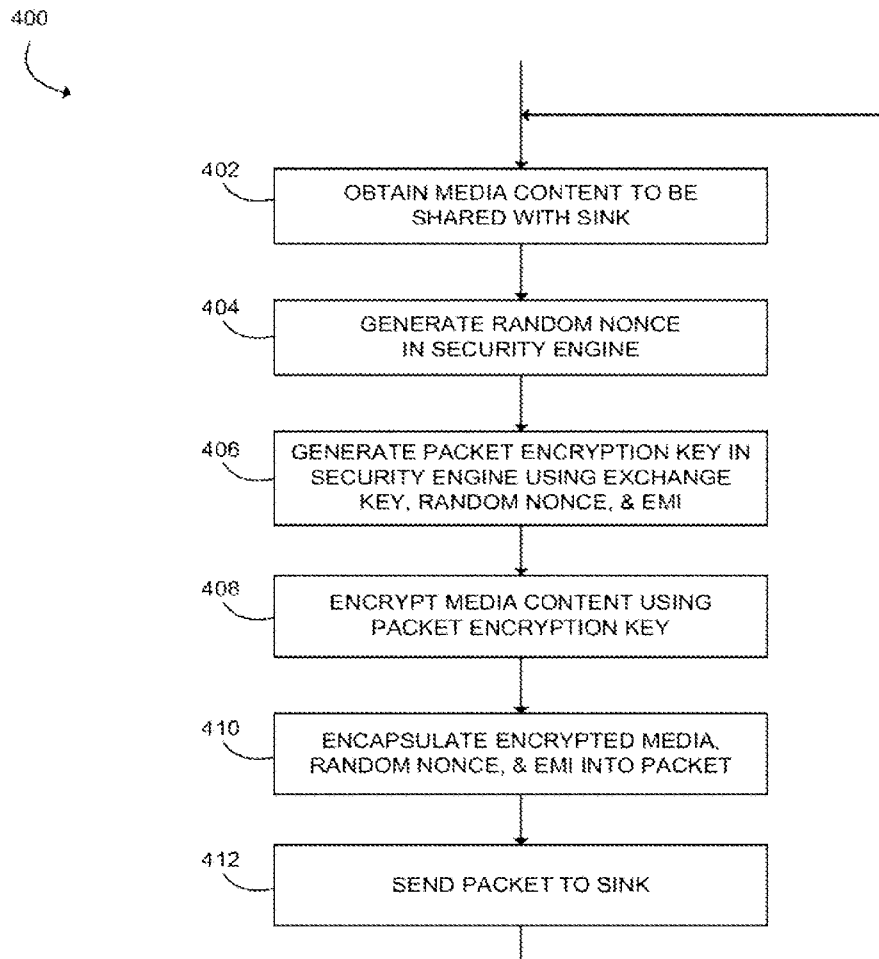


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/065094**A. CLASSIFICATION OF SUBJECT MATTER****G06F 21/24(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/24; G06F 17/00; G06F 12/14; H04L 9/00; H04R 3/02; G06F 1/24

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: "authentication, key, exchange, security, cryptographic, authorization, engine"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2011-0154061 A1 (CHILUKURI BABU et al.) 23 June 2011 See the abstract, paragraphs 27-48, figs. 2 and 3.	1-39
A	US 2008-0229104 A1 (JU HAK-SOO et al.) 18 September 2008 See the abstract, paragraphs 31-56.	1-39
A	US 7813822 B1 (HOFFBERG STEVEN M.) 12 October 2010 See the abstract, column 4, line 4-25.	1-39
A	US 6324288 B1 (HOFFMAN; JEFFREY D.) 27 November 2001 See the abstract, column 1, line 10-column 2, line 14.	1-39

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

27 AUGUST 2012 (27.08.2012)

Date of mailing of the international search report

27 AUGUST 2012 (27.08.2012)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan
City, 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Soak, Sang Moon

Telephone No. 82-42-481-8470



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2011/065094

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011-0154061 A1	23.06.2011	None	
US 2008-0229104 A1	18.09.2008	EP 1971074 A2 KR 10-2008-0084480 A KR20080084480A	17.09.2008 19.09.2008 19.09.2008
US 7813822 B1	12.10.2010	US 2007-0053513 A1 US 6850252 B1 US 7974714 B2	08.03.2007 01.02.2005 05.07.2011
US 6324288 B1	27.11.2001	AU 2000-46929 A1 CN 1160901 C0 CN 1361958 A0 DE 60021560 D1 DE 60021560 T2 EP 1179242 A1 EP 1179242 B1 TW 490968 A TW 490968 B WO 00-70817 A1	05.12.2000 04.08.2004 31.07.2002 01.09.2005 24.05.2006 13.02.2002 27.07.2005 11.06.2002 11.06.2002 23.11.2000

(51) International Patent Classification:
G06F 21/20 (2006.01) G06F 21/22 (2006.01)(21) International Application Number:
PCT/US2011/065072(22) International Filing Date:
15 December 2011 (15.12.2011)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): **INTEL CORPORATION** [US/US]; 2200 Mission College Blvd, Santa Clara, California 95052 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **KHOSRAVI, Hormuzd M.** [IN/US]; 4816 NW 166th Ave, Portland, Oregon 97229 (US). **MOGILAPPAGARI, Sudheer** [IN/US]; 131 NE Greenridge Ter, Hillsboro, Oregon 97124 (US). **KUSHWAHA, Priyalee** [IN/US]; 107 NE 64 Terr, Hillsboro, Oregon 97124 (US). **CHERUVU, Sunil** [US/US]; 5000 W Chandler Blvd, MS CH6-455, Chandler, Arizona 85226 (US). **SCHOLLMAYER, David** [US/US]; 4771 W Harrison St, Chandler, Arizona 85226 (US).(74) Agent: **KELLETT, Glen M.**; Barnes & Thornburg, LLP, C/O CPA Global, PO Box 52050, Minneapolis, Minnesota 55402 (US).

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

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

Published:

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

(54) Title: METHOD, DEVICE, AND SYSTEM FOR PROTECTING AND SECURELY DELIVERING MEDIA CONTENT

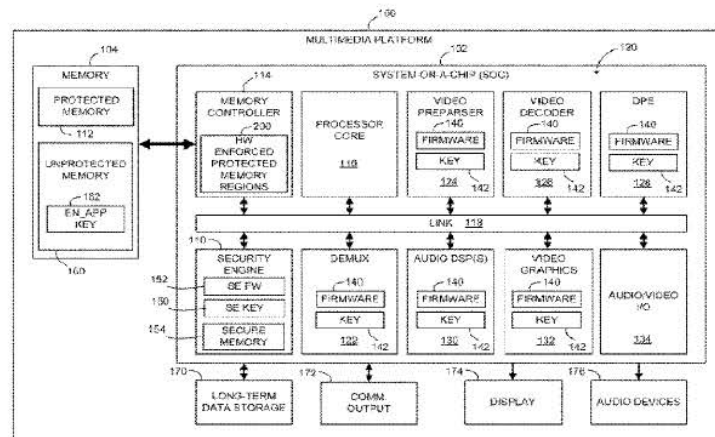


FIG. 1

(57) Abstract: A method, device, and system for protecting and securely delivering media content includes configuring a memory controller of a system-on-a-chip (SOC) to establish a protected memory region, authenticating a firmware of a hardware peripheral using a security engine of the SOC, and storing the authenticated firmware in the protected memory region. The security engine may authenticate the firmware by authenticating a peripheral cryptographic key used to encrypt the firmware. Only authenticated hardware peripherals may access the protected memory region.

METHOD, DEVICE, AND SYSTEM FOR PROTECTING AND SECURELY DELIVERING MEDIA CONTENT

BACKGROUND

The way in which content users access media content is changing from the traditional
5 opportunistic access to on-demand access. On-demand media content, as well as some standard
media content, is often delivered by streaming the content to a multimedia platform, such as a
set-top box, a smart phone, a computer tables, a laptop, or the like. If the multimedia content is
premium content, the multimedia content is often protected in some manner during transmission
to the multimedia platform. For example, various Digital Rights Management (DRM) and
10 Conditional Access (CA) technologies may be used to provide protection for the media content
from the media source to the multimedia platform. Such technologies generally involve
encryption of the content media.

System-on-a-chip (SOC) devices are integrated circuits that incorporate various
components, in addition to the processing core, of electronic systems on a single die. For
15 example, an SOC may include a processor core, memory controller, video components, audio
components, and/or communication components on a single chip. Due to their relatively small
size, SOC's are used in many multimedia platforms.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention described herein is illustrated by way of example and not by way of
20 limitation in the accompanying figures. For simplicity and clarity of illustration, elements
illustrated in the figures are not necessarily drawn to scale. For example, the dimensions of
some elements may be exaggerated relative to other elements for clarity. Further, where
considered appropriate, reference labels have been repeated among the figures to indicate
corresponding or analogous elements.

25 FIG. 1 is a simplified block diagram of at least one embodiment of a multimedia platform
including a system-on-a-chip (SOC);

FIG. 2 is a simplified block diagram of at least one embodiment of a memory controller
and memory of the multimedia platform of FIG. 1;

30 FIG. 3 is a simplified block diagram of at least one embodiment of a protected media
content flow of the SOC of FIG. 1;

FIG. 4 is a simplified flow diagram of at least one embodiment of a method for
establishing a protected memory region in the SOC of FIG. 1;

FIG. 5 is a simplified flow diagram of at least one embodiment of a method for authenticating a hardware peripheral of the SOC of FIG. 1; and

FIG. 6 is a simplified flow diagram of at least one embodiment of a method for delivering content media from the SOC of FIG. 1;

5 DETAILED DESCRIPTION OF THE DRAWINGS

While the concepts of the present disclosure are susceptible to various modifications and alternative forms, specific exemplary embodiments thereof have been shown by way of example in the drawings and will herein be described in detail. It should be understood, however, that there is no intent to limit the concepts of the present disclosure to the particular forms disclosed, but on the contrary, the intention is to cover all modifications, equivalents, and alternatives
10 consistent with the present disclosure and the appended claims.

In the following description, numerous specific details such as logic implementations, opcodes, means to specify operands, resource partitioning/sharing/duplication implementations, types and interrelationships of system components, and logic partitioning/integration choices are set forth in order to provide a more thorough understanding of the present disclosure. It will be appreciated, however, by one skilled in the art that embodiments of the disclosure may be practiced without such specific details. In other instances, control structures, gate level circuits and full software instruction sequences have not been shown in detail in order not to obscure the invention. Those of ordinary skill in the art, with the included descriptions, will be able to
15 implement appropriate functionality without undue experimentation.

References in the specification to “one embodiment,” “an embodiment,” “an example embodiment,” etc., indicate that the embodiment described may include a particular feature, structure, or characteristic, but every embodiment may not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is within the knowledge of one skilled in the art to effect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described.
25

Embodiments of the invention may be implemented in hardware, firmware, software, or any combination thereof. Embodiments of the invention implemented in a computer system may include one or more bus-based interconnects or links between components and/or one or more point-to-point interconnects between components. Embodiments of the invention may also be implemented as instructions carried by or stored on a transitory or non-transitory machine-
30

readable medium, which may be read and executed by one or more processors. A machine-readable medium may be embodied as any device, mechanism, or physical structure for storing or transmitting information in a form readable by a machine (e.g., a computing device). For example, a machine-readable medium may be embodied as read only memory (ROM); random
5 access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices; mini- or micro-SD cards, memory sticks, electrical signals, and others.

In the drawings, specific arrangements or orderings of schematic elements, such as those representing devices, modules, instruction blocks and data elements, may be shown for ease of description. However, it should be understood by those skilled in the art that the specific
10 ordering or arrangement of the schematic elements in the drawings is not meant to imply that a particular order or sequence of processing, or separation of processes, is required. Further, the inclusion of a schematic element in a drawing is not meant to imply that such element is required in all embodiments or that the features represented by such element may not be included in or combined with other elements in some embodiments.

15 In general, schematic elements used to represent instruction blocks may be implemented using any suitable form of machine-readable instruction, such as software or firmware applications, programs, functions, modules, routines, processes, procedures, plug-ins, applets, widgets, code fragments and/or others, and that each such instruction may be implemented using any suitable programming language, library, application programming interface (API), and/or
20 other software development tools. For example, some embodiments may be implemented using Java, C++, and/or other programming languages. Similarly, schematic elements used to represent data or information may be implemented using any suitable electronic arrangement or structure, such as a register, data store, table, record, array, index, hash, map, tree, list, graph, file (of any file type), folder, directory, database, and/or others.

25 Further, in the drawings, where connecting elements, such as solid or dashed lines or arrows, are used to illustrate a connection, relationship or association between or among two or more other schematic elements, the absence of any such connecting elements is not meant to imply that no connection, relationship or association can exist. In other words, some connections, relationships or associations between elements may not be shown in the drawings
30 so as not to obscure the disclosure. In addition, for ease of illustration, a single connecting element may be used to represent multiple connections, relationships or associations between elements. For example, where a connecting element represents a communication of signals, data or instructions, it should be understood by those skilled in the art that such element may

represent one or multiple signal paths (e.g., a bus), as may be needed, to effect the communication.

Referring now to FIG. 1, in one embodiment, a multimedia platform 100 is configured to deliver media content to a user of the platform 100. The multimedia platform 100 may be embodied as any type of device configured to deliver media content. For example, the multimedia platform may be embodied as a set-top box, a smartphone, a tablet computer, a laptop computer, a mobile internet device (MID), a desktop computer, or other device capable of delivery of media content. The multimedia platform 100 may be configured to deliver any type of media content to the user including, for example, movies, pictures, images, songs, audio and/or video recordings, and/or any other type of audio, video, and/or audio and video content.

The multimedia platform 100 includes a system-on-a-chip (SOC) 102 and a platform memory 104. As discussed in more detail below, the SOC 102 is configured to protect and securely deliver the media content while within the SOC 102 and memory 104. To do so, a security engine 110 of the SOC 102 establishes a protected memory 112 in the memory 104, which is hardware enforced by a memory controller 114 of the SOC 102. The memory controller 114 ensures that only authorized hardware peripherals of the SOC 102 may access the protected memory 112. The security engine 110 of the SOC 102 authorizes each hardware peripheral by authenticating the firmware of each peripheral prior to loading the firmware in the protected memory 112. Decrypted media content is also stored in the protected memory 112 and is accessible only by authorized hardware peripherals. In this way, a trusted data path is established in the SOC 102 wherein decrypted media content is accessible only by authenticated components of the SOC 102.

The SOC 102 may be embodied as any type of system-on-a-chip, which may include various components and structures. In the illustrative embodiment of FIG. 1, the SOC 102 includes the security engine 110 and memory controller 114 as discussed above, a processor core 116, and a plurality of hardware peripherals 120, which are communicatively coupled to each other via a link 118. The link 118 may be embodied as any type of interconnect such as a bus, point-to-point, or other interconnect capable of facilitating communication between the various components of the SOC 102. The hardware peripherals 120 may include any type of hardware peripheral component depending upon the intended functionality of the SOC 102. For example, in the illustrative embodiment, the hardware peripherals 120 include a demux 122, a video preparser 124, a video decoder 126, a Display Processing Engine (DPE) 128, an audio digital signal processor (DSP) 130, a video graphics 132, and an audio/video I/O 134. Each of the hardware peripherals 120 includes an associated firmware 140 and a cryptographic key 142. As

discussed in more detail below, the cryptographic key 142 of each hardware peripheral 120 is previously signed by the security engine 110 using a security key 150 of the security engine 110.

The security engine 110 may be embodied as a security co-processor or processing circuitry separate from the processor core 116. The security engine 110 includes a security engine firmware 152 and a secure memory 154, which is accessible only by the security engine 110. In the illustrative embodiment, the secure memory 154 forms a physical portion of the security engine 110, but may form a portion of the memory 104 in other embodiments (i.e., a portion of the protected memory 112). The security engine 110 stores the security key 150, and other cryptographic keys as discussed below, in the secure memory 154. The security key 150 may be provisioned during the manufacturing of the SOC 102 or may be generated by the SOC 102 during operation. For example, in some embodiments, the security key 150 is based on blown fuses within the security engine 110. Additionally or alternatively, the security engine 110 may include a key-generating module, such as a trusted platform module (TPM), to generate the security key 150. During use, the security engine 110 may use any number of security keys 150, which may be identical or different from each other.

As discussed above, the memory 104 includes the protected memory 112 and an unprotected memory 160. Various data may be stored in the unprotected memory 160 in a decrypted or encrypted form during operation of the multimedia platform 100. For example, as discussed in more detail below, an encrypted application key 162 may be stored in the unprotected memory 160 of the memory 104, along with any encrypted media content for delivery to a user.

In some embodiments, the multimedia platform 100 may include additional components and structures other than the SOC 102 and memory 104. For example, in the illustrative embodiment, the multimedia platform 100 includes a long-term data storage 170 such as a hard drive or solid-state drive, a communications output 172, a display 174, and audio devices 176 such as speakers, each of which may be communicate or otherwise interact with the SOC 102.

Referring now to FIG. 2, as discussed above, the protected memory 112 of the memory 104 is enforced by the memory controller 114. To do so, the memory controller 114 is configured to establish a hardware enforced protected memory region 200, which correlates and defines the protected memory 112 of the memory 102. The hardware enforced protected memory region may include any number of protected memory regions or sub-regions. For example, in the illustrative embodiment of FIG. 2, the hardware enforced protected memory region includes a firmware protected memory region 202 in which authenticated firmware is stored, a frame buffer protected memory region 204 in which decrypted video is stored, an audio

protected memory region 206 in which decrypted audio is stored, a compressed video protected memory region 208, a security engine-to-Transport Stream Demultiplexor (TSD) protected memory region 210, and/or one or more other protected memory regions 212. Of course, in other embodiments, the hardware enforced protected memory region 200 may include fewer or greater number protected memory regions depending on, for example, the intended functionality of the SOC 102.

Each of the protected memory regions 202, 204, 206, 208, 210, 212 may include similar or different security attributes depending on the respective use. The memory controller 114 secures such attributes into corresponding registers such that the attributes cannot be subsequently altered. Additionally, the memory controller 114 may ensure that the protected memory regions 202, 204, 206, 208, 210, 212 are configured appropriately (e.g., that the corresponding memory addresses do not overlap) and, in some embodiments, may perform other security and error checks on the protected memory 112.

During use, the memory controller 114 provides hardware enforced protection for the protected memory 112. For example, a hardware peripheral 120 may communicate with a memory interface 220 of the memory controller 114 to retrieve data from the memory 102. The memory controller 114 determines whether the hardware peripheral 120 is requesting data from the protected memory 112 (e.g., from one of the protected memory regions 200). If so, the memory controller 114 allows access (arrow 230) to the corresponding hardware enforced protected memory region 200 of the protected memory 112 only if the requesting hardware peripheral 120 has been previously authenticated by the security engine 110 as discussed below. If not, the memory controller 114 denies the requested access. Alternatively, the hardware peripheral 120 may request access (arrow 232) to the unprotected memory 160, which is allowed by the memory controller 114.

As discussed above, the establishment of the hardware enforced protected memory regions 200 and authentication of hardware peripherals 120 configures a trusted data path within the SOC 102 in which media content is protected throughout its delivery. For example, on illustrative embodied of a trusted data path 300 is shown in FIG. 3. In the diagram of FIG. 3, the trusted data path 300 is shown as filled arrows while unfilled arrows indicate an unprotected data path. Additionally, each authenticated hardware component of the SOC 102 is shown with double brackets to indicate that the component has been previously authenticated by the security engine 110.

As shown in FIG. 3, a host software 302 may be executed on the multimedia platform 100. The host software 302 may request delivery (e.g., playback) of encrypted media content 304.

The encrypted media content 304 may be stored, for example, in the unprotected memory 104. In response to the delivery request, the security engine 110 retrieves the encrypted media content 304 from memory 160. The security engine 110 decrypts the media content into an A/V stream 306 using the encrypted application key 162. In so doing, as discussed in more detail below, the security engine 110 ensures that the application key 162 is never unprotected when in the decrypted state (e.g., the security engine 110 stores the decrypted application key in the secure memory 154). Similarly, the security engine 110 ensures the protection of the decrypted media content by storing the decrypted media stream in the protected memory region 200, which is accessible only by authenticated hardware peripherals 120.

The A/V stream 306 is accessed by the demux 122, which separates the audio and video from the A/V stream 306. Additionally, the demux 122 may provide section data 320 of the media content to the host software. The transfer of the section data 320 is unprotected as indicated by the unfilled arrow in FIG. 3. The audio 308 of the A/V stream 306 is accessed by the audio DSP 130, which generates a processed audio 310 to the A/V outputs 134. Additionally, the compressed video 312 of the A/V stream 306 is accessed by the video preparser 124. The video preparser 124 may generate metadata 322, which is provided to the host software 302 in an unprotected transfer. The preparsed compressed video 314 is accessed by the video decoder 136, which generates video pixels 316. The video pixels 316 are accessed by the DPE 128 to generate video pixels 318, which are subsequently accessed by the video graphics 132 to generate the uncompressed video stream at the A/V outputs 134. In this way, the decryption and decompression of media content is performed in the SOC 102 through the trusted data path 300 such that access to the media content is protected throughout the delivery of the media content.

Referring now to FIG. 4, in use, the SOC 102 may execute a method 400 to establish the protected memory region 200. The method 400 begins with block 402 in which an operating system of the multimedia platform 100 may be loaded. During the boot process, the driver of the security engine 110 is loaded in block 404. In block 406, the SOC 102 determines whether the SOC 102 is configured for delivery of media content using the trusted data path. If not, the method 400 exits and the multimedia platform 100 boots as normal. However, if the SOC 102 is configured for trusted data path delivery, the method 400 advances to block 408 in which the security engine driver obtains information pertaining to the hardware enforced protected memory region 200. Such information may include, for example, the address range of each protected memory region 200, the region type of each protected memory region 200, and any additional attributes associated with each protected memory region 200. Such information may be obtained

from a secured data table or the like. In block 410, the security engine driver sends the protected memory region information to the security engine firmware 152 for validation. The security engine firmware 152 validates the protected memory region information in block 414. The security engine firmware 152 may perform any type of validation on the protected memory regions including, for example, ensuring that the address ranges of the individual protected memory ranges of the protected memory region 200 do not overlap with each other, that the type and attributes correspond correctly, and so forth.

In block 416, the SOC 102 determines whether the configuration of the protected memory region 200 was determined to be valid by the security engine 110. If the configuration of the protected memory region 200 is not valid, the method 400 advances to block 418 in which a security engine driver error is generated. In response thereto, the SOC 102 may perform one or more security actions including, for example, rebooting, reconfiguring the memory controller 114, and/or other corrective action. However, if the configuration of the protected memory region 200 is determined to be valid, the method 400 advances to block 420 in which the security engine firmware 152 holds all hardware peripherals 120, which have not yet been authenticated, in a reset mode.

After the memory controller 114 has been configured for the protected memory region 200, the security engine 110 of the SOC 102 may authenticate hardware peripherals 120 of the SOC 102. To do so, the SOC 102 may execute a method 500 for authenticating a hardware peripheral 120. The method 500 begins with block 502 in which the security engine 110 determines whether a request to load the firmware 140 of the hardware peripheral 120 has been received. If so, the security engine driver retrieves the cryptographic key 142 of the requesting hardware peripheral 120 and the associated encrypted firmware 140 in block 504. The security engine driver generates a firmware loading package including the peripheral cryptographic key 142, the encrypted peripheral firmware 140, and the memory address of the associated firmware protected memory region 202.

The security engine driver sends the firmware loading package to the security engine firmware 152 in block 508. In response, the security engine firmware 152 authenticates the peripheral cryptographic key 142 in block 510. To do so, the security engine firmware 152 may use the security key 150 of the security engine 110 to verify that the peripheral cryptographic key 142 was previously signed by the security engine 110.

In block 512, the SOC 102 determines whether the security engine 110 successfully authenticated the peripheral cryptographic key 142. If not, the method 500 advances to block 514 in which a peripheral driver loading error is generated, and the hardware peripheral is held in

reset mode. Additionally, the SOC 102 may take additional security responses to such loading error.

If the peripheral cryptographic key 142 is authenticated by the security engine 110, the method 500 advances to block 516 in which the security engine firmware 152 authenticates the peripheral firmware 140 using the now-authenticated peripheral cryptographic key 142. For example, in embodiments wherein the firmware 140 is encrypted, the security engine 110 may decrypt the firmware 140. Additionally or alternatively, the security engine 110 may ensure that the firmware 140 has been previously signed using the peripheral cryptographic key 142 based on, for example, a hash function of the firmware 140 or the like.

In block 518, the SOC 102 determines whether the security engine 110 successfully authenticated the peripheral firmware 140. If not, the method 500 advances to block 514 in which a peripheral driver loading error is generated, and the hardware peripheral is held in reset mode. However, if the peripheral firmware 140 is authenticated, the method 500 advances to block 520 in which the security engine firmware 152 loads the authenticated (and decrypted) hardware peripheral firmware 140 into the associated firmware protected memory region 202 and releases the hardware peripheral 120 from reset mode. In this way, only authenticated firmware of the hardware peripherals is loaded and executed by the SOC 102. Additionally, only the authenticated hardware peripherals have access to the protected memory region 200 and the decrypted media content contained therein.

Referring now to FIG. 6, after the hardware peripherals 120 have been authenticated, the SOC 102 may deliver content to a user of the multimedia platform 100. To do so, the SOC 102 may execute a method 600 for delivering content media in a trusted data path. The method 600 begins with block 602 in which any digital rights management (DRM) firmware is loaded by the SOC. The DRM firmware may support the decryption operation of media content to be delivered on the multimedia platform 602. During the loading of the DRM firmware, an application cryptographic key 162 for decrypting the media content is stored in the memory 104. In the illustrative embodiment, the application cryptographic key 162 is stored in encrypted form in the unprotected memory 160 of the memory 104. Additionally, the encrypted media content to be delivered to the user may be stored in the unprotected memory 160.

In block 606, the SOC 102 determines whether a user has requested delivery of the media content. If so, the method 600 advances to block 608 in which the security engine 110 retrieves the encrypted application key 162 from the unprotected memory 160 of the memory 104. In block 610, the security engine 110 decrypts the application key 162 and stores the decrypted application key in the secure memory 154 of the security engine 110 in block 612.

Subsequently, in block 614, the security engine 110 decrypts the encrypted media content, which may be stored in the unprotected memory 160, using the decrypted application key 162. The decrypted media content is stored in the streaming frame buffer protected memory region 204.

5 In block 618, authenticated hardware peripherals 120 access the decrypted media content in the protected memory region 200, and the media content is processed by the various authenticated hardware peripherals 120 and delivered to the A/V outputs 134 of the SOC 102 for playback to the user of the multimedia platform 100. In so doing, it should be appreciated that the decrypted application key 162 and the decrypted media content are never left in an unprotected state.

10 It should be appreciated that the above-described system delivers media content in a secure and protected manner. For example, the decrypted media content and the decrypted application key 162 are stored in protected and secured memory locations whenever in the decrypted state. Additionally, only authenticated hardware peripherals 120 have access to the protected memory region 200 in which the decrypted media content is stored during processing of the content for
15 delivery. In this way, media content is secured within the SOC 102 itself during the delivery process.

While the disclosure has been illustrated and described in detail in the drawings and foregoing description, such an illustration and description is to be considered as exemplary and not restrictive in character, it being understood that only illustrative embodiments have been
20 shown and described and that all changes and modifications consistent with the disclosure and recited claims are desired to be protected.

CLAIMS:

1. A system-on-a-chip apparatus comprising:
a memory having at least one protected region to store at least decrypted media content therein; and
5 a system-on-a-chip comprising:
a memory controller coupled to the memory to enforce protection of the protected memory region such that access to the protected memory region is permitted only to authenticated peripheral devices of the system-on-a-chip; and
a security engine coupled to the memory controller to authenticate a
10 firmware of a hardware peripheral of the system-on-a-chip to allow the hardware peripheral access to the protected memory region of the memory.
2. The system-on-a-chip apparatus of claim 1, wherein the security engine to store the firmware of the hardware peripheral in the protected memory region in response to the
15 firmware being authenticated by the security engine and allow execution of the firmware from the protected memory region to activate the hardware peripheral.
3. The system-on-a-chip apparatus of claim 1, wherein the firmware comprises an encrypted firmware of the hardware peripheral,
20 the security engine to obtain a peripheral cryptographic key of the hardware peripheral and authenticate the peripheral cryptographic key using a security cryptographic key of the security engine.
4. The system-on-a-chip apparatus of claim 3, wherein the security engine to
25 authenticate the encrypted firmware using the peripheral cryptographic key in response to the peripheral cryptographic key being authenticated using the security cryptographic key.
5. The system-on-a-chip apparatus of claim 4, wherein the security engine to decrypt the encrypted firmware using the peripheral cryptographic key.
30
6. The system-on-a-chip apparatus of claim 5, wherein the security engine to store the decrypted firmware in the protected memory region.

7. The system-on-a-chip apparatus of claim 1, wherein the firmware comprises an encrypted firmware,

the security engine to decrypt the encrypted firmware of the hardware peripheral using a peripheral cryptographic key of the hardware peripheral that has been authenticated by a security cryptographic key of the security engine.

8. The system-on-a-chip apparatus of claim 1, wherein the security engine to retrieve an encrypted application key from memory in response to receiving a request to deliver media content.

9. The system-on-a-chip apparatus of claim 8, wherein the security engine to decrypt the encrypted application key with a security cryptographic key of the security engine and store the decrypted application key in the protected memory region.

10. The system-on-a-chip apparatus of claim 9, wherein the security engine to access encrypted media content and decrypt the media content using the decrypted application key.

11. The system-on-a-chip apparatus of claim 10, wherein the security engine to store the decrypted media content in the protected memory region.

12. The system-on-a-chip apparatus of claim 11, wherein the authenticated hardware peripheral to access the protected memory region to retrieve the decrypted media content.

13. The system-on-a-chip apparatus of claim 11, further comprising a plurality of authenticated hardware peripherals to deliver the decrypted media to an output of the system-on-a-chip such that no unauthenticated hardware peripheral access the decrypted media content.

14. A method comprising:
configuring a memory controller of a system-on-a-chip to establish a protected memory region, the protected memory region accessible only by authenticated hardware peripherals;

authenticating a firmware of a hardware peripheral of the system-on-a-chip using a security engine of the system-on-a-chip;

storing the firmware in the protected memory region in response to the firmware being authenticated by the security engine; and

5 executing the firmware from the protected memory region to activate the hardware peripheral.

15 15. The method of claim 14, wherein configuring the memory controller comprises obtaining protected memory region information and configuring the memory controller using the identified information.

16. The method of claim 15, wherein obtaining protected memory region information comprises obtaining an address range of the protected memory region.

15 17. The method of claim 15, wherein obtaining protected memory region information comprises obtaining an address range of the protected memory region, a type of the protected memory region, and at least one attribute of the protected memory region.

20 18. The method of claim 15, further comprising validating the protected memory region information using the security engine of the system-on-a-chip.

19. The method of claim 14, wherein authenticating the firmware of the hardware peripheral comprises:

25 obtaining a peripheral cryptographic key of the hardware peripheral and an encrypted firmware of the hardware peripheral, and

 authenticating the peripheral cryptographic key using a security cryptographic key of the security engine.

30 20. The method of claim 19, wherein authenticating the firmware comprises authenticating the encrypted firmware using the peripheral cryptographic key in response to the peripheral cryptographic key being authenticated using the security cryptographic key.

21. The method of claim 20, wherein authenticating the encrypted firmware comprises decrypting the encrypted firmware using the peripheral cryptographic key.

22. The method of claim 21, wherein storing the firmware comprises storing the decrypted firmware in the protected memory region.

23. The method of claim 14, wherein authenticating the firmware of the hardware peripheral comprises decrypting an encrypted firmware of the hardware peripheral using a peripheral cryptographic key of the hardware peripheral that has been authenticated by a security cryptographic key of the security engine.

24. The method of claim 14, further comprising retrieving an encrypted application key from memory using the security engine in response to receiving a request to deliver media content.

25. The method of claim 24, further comprising decrypting the encrypted application key with a security cryptographic key of the security engine and storing the decrypted application key in the protected memory region.

26. The method of claim 25, further comprising accessing encrypted media content and decrypting the media content using the decrypted application key.

27. The method of claim 26, further comprising storing the decrypted media content in the protected memory region.

28. The method of claim 27, further comprising accessing the protected memory region with an authenticated hardware peripheral to retrieve the decrypted media content.

29. The method of claim 27, further comprising delivering the decrypted media to an output of the system-on-a-chip such that no unauthenticated hardware peripheral accesses the decrypted media content.

30. A multimedia platform comprising:
a system-on-a-chip including a plurality of instructions that when executed results in the system-on-a-chip performing the method of any of claims 14-29.

31. One or more machine readable media comprising a plurality of instructions stored thereon, that in response to being executed result in a system-on-a-chip performing the method of any of claims 14-29.

5 32. A method comprising:
 configuring a memory controller of a system-on-a-chip to establish a protected memory region;
 receiving, with a security engine of the system-on-a-chip, a peripheral cryptographic key of a hardware peripheral and an encrypted firmware of the hardware
10 peripheral;
 authenticating the peripheral cryptographic key using a security cryptographic key of the security engine;
 authenticating the encrypted firmware using the peripheral cryptographic key in response to the peripheral cryptographic key being authenticated;
15 storing the decrypted firmware in the protected memory region; and
 executing the decrypted firmware from the protected memory region to release the hardware peripheral from a reset state.

20 33. The method of claim 32, further comprising retrieving an encrypted application key from memory using the security engine in response to receiving a request to deliver media content.

25 34. The method of claim 33, further comprising decrypting the encrypted application key with the security cryptographic key of the security engine and storing the decrypted application key in the protected memory region.

 35. The method of claim 34, further comprising accessing encrypted media content and decrypting the media content using the decrypted application key.

30 36. The method of claim 35, further comprising storing the decrypted media content in the protected memory region.

37. The method of claim 36, further comprising accessing the protected memory region with an authenticated hardware peripheral to retrieve the decrypted media content.

5 38. The method of claim 36, further comprising delivering the decrypted media to an output of the system-on-a-chip such that no unauthenticated hardware peripheral accesses the decrypted media content.

 39. A multimedia platform comprising:
10 a system-on-a-chip including a plurality of instructions that when executed results in the system-on-a-chip performing the method of any of claims 32-37.

 40. One or more machine readable media comprising a plurality of instructions stored thereon, that in response to being executed result in a system-on-a-chip
15 performing the method of any of claims 32-37.

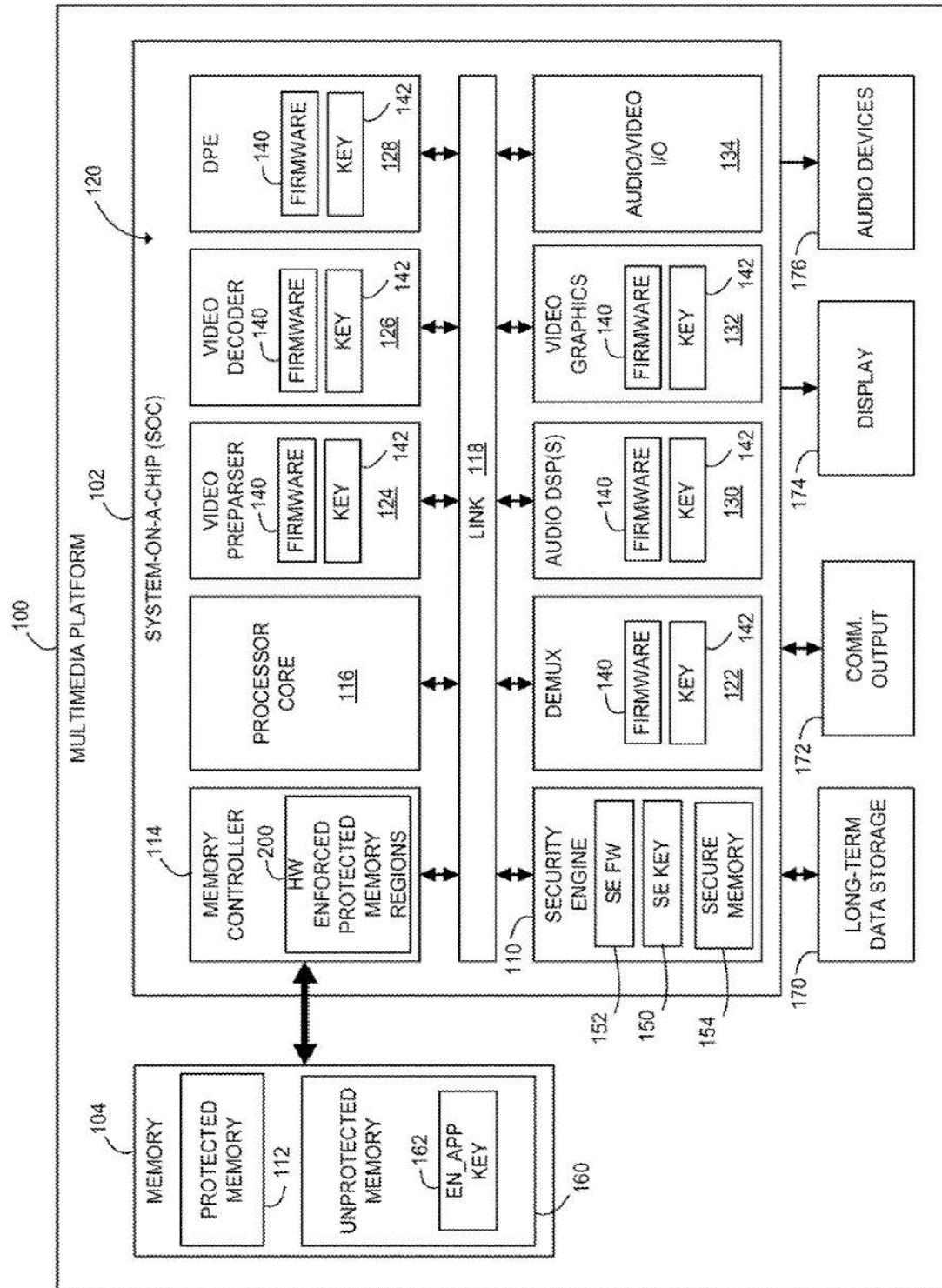


FIG. 1

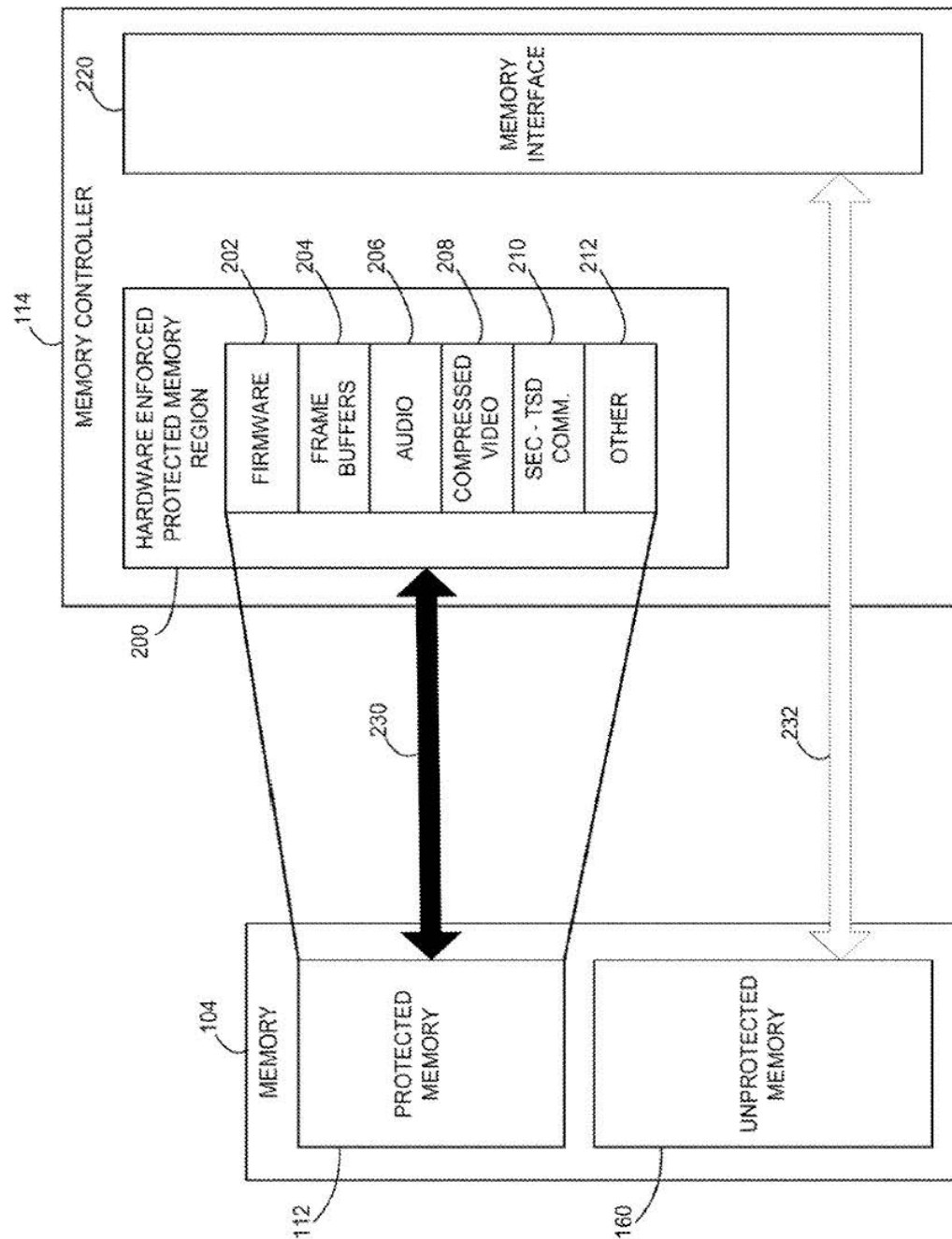


FIG. 2

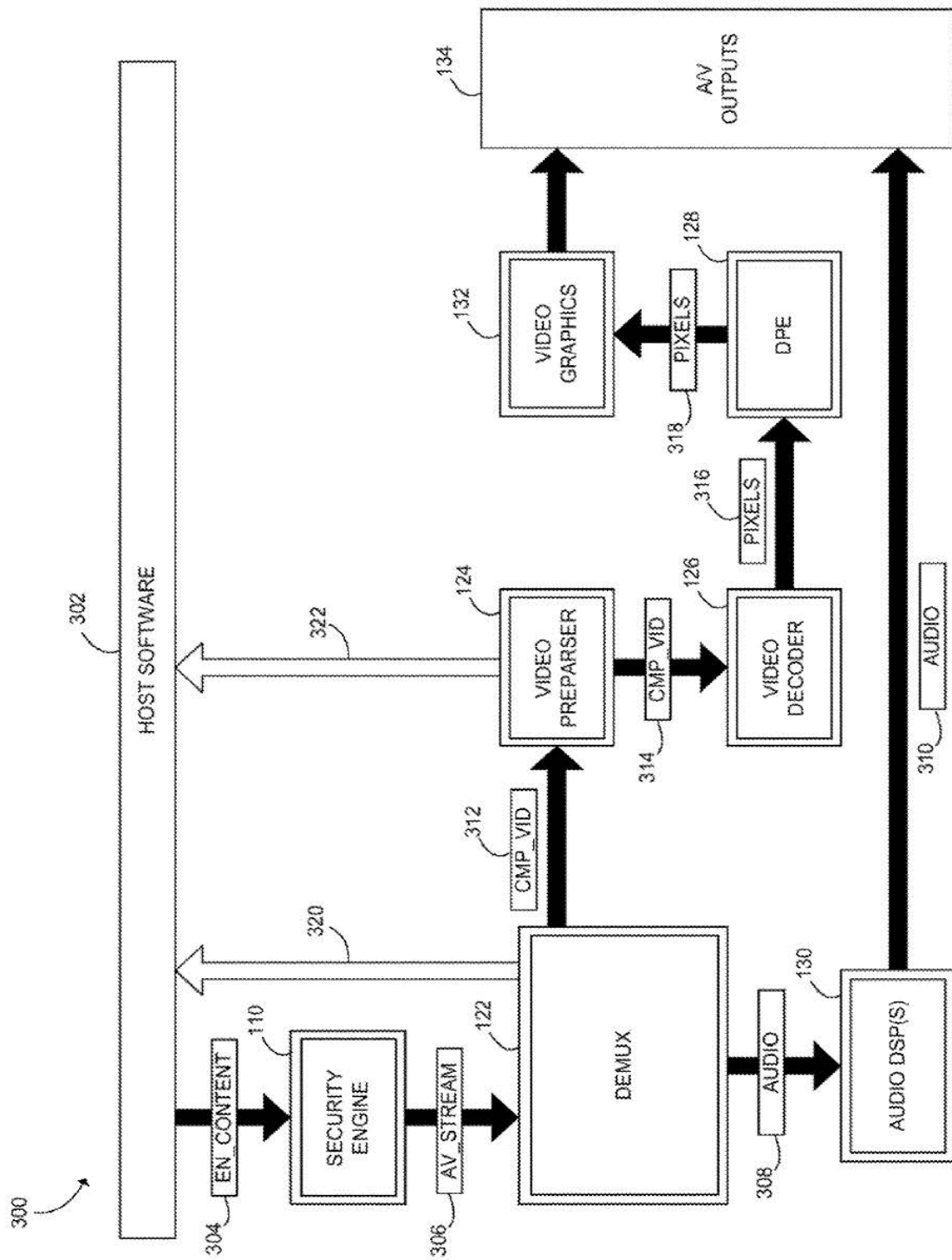


FIG. 3

4/6

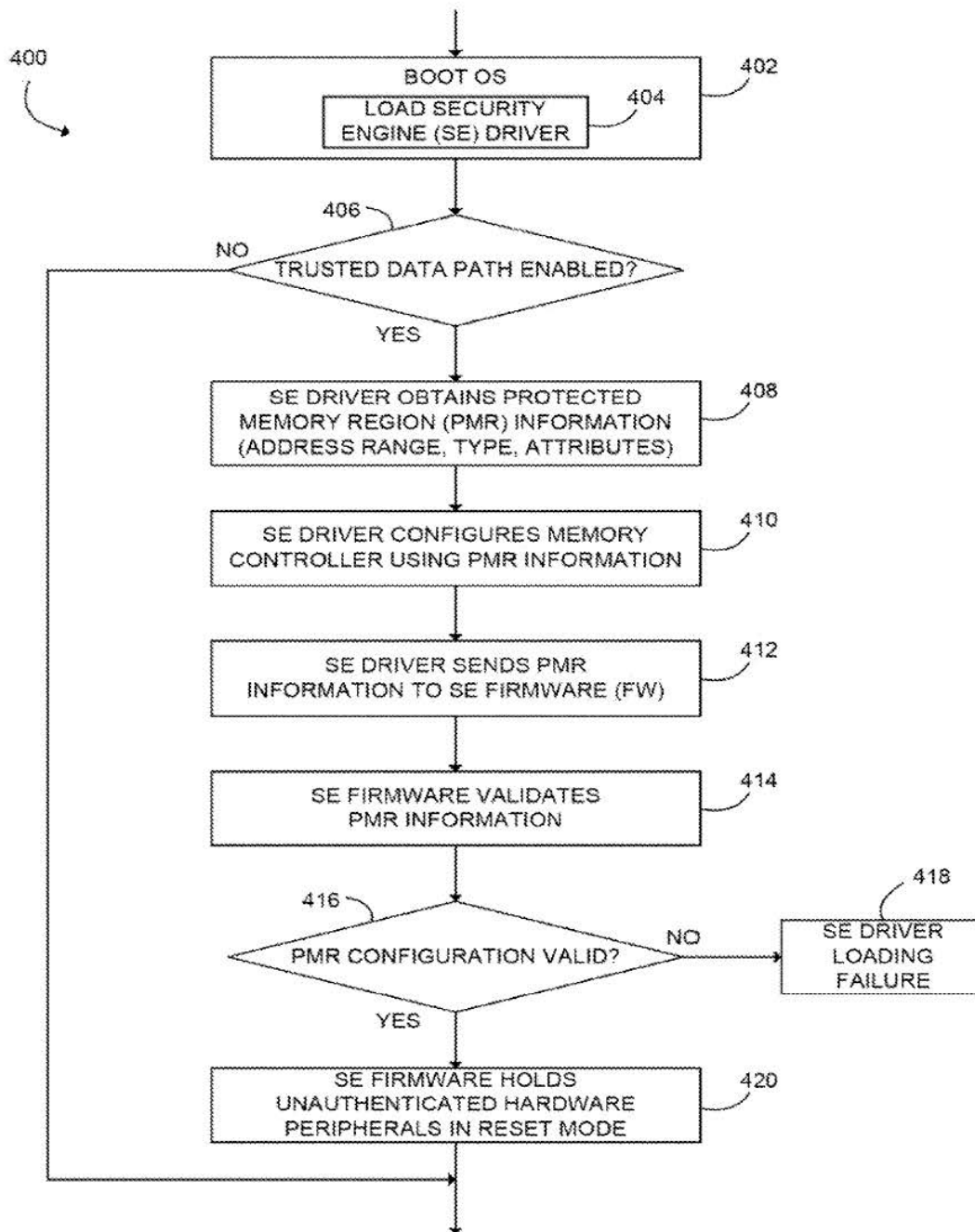


FIG. 4

5/6

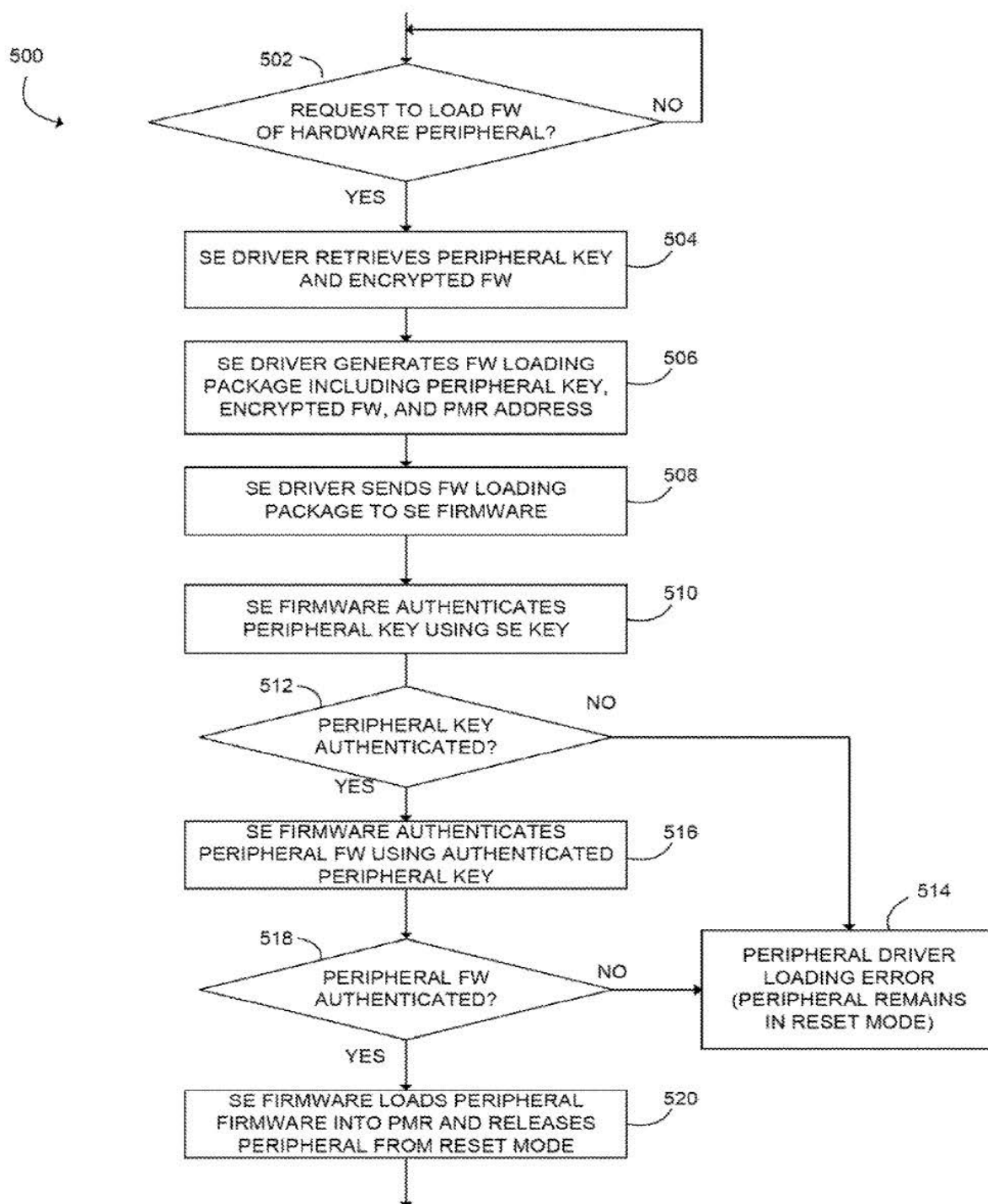


FIG. 5

6/6

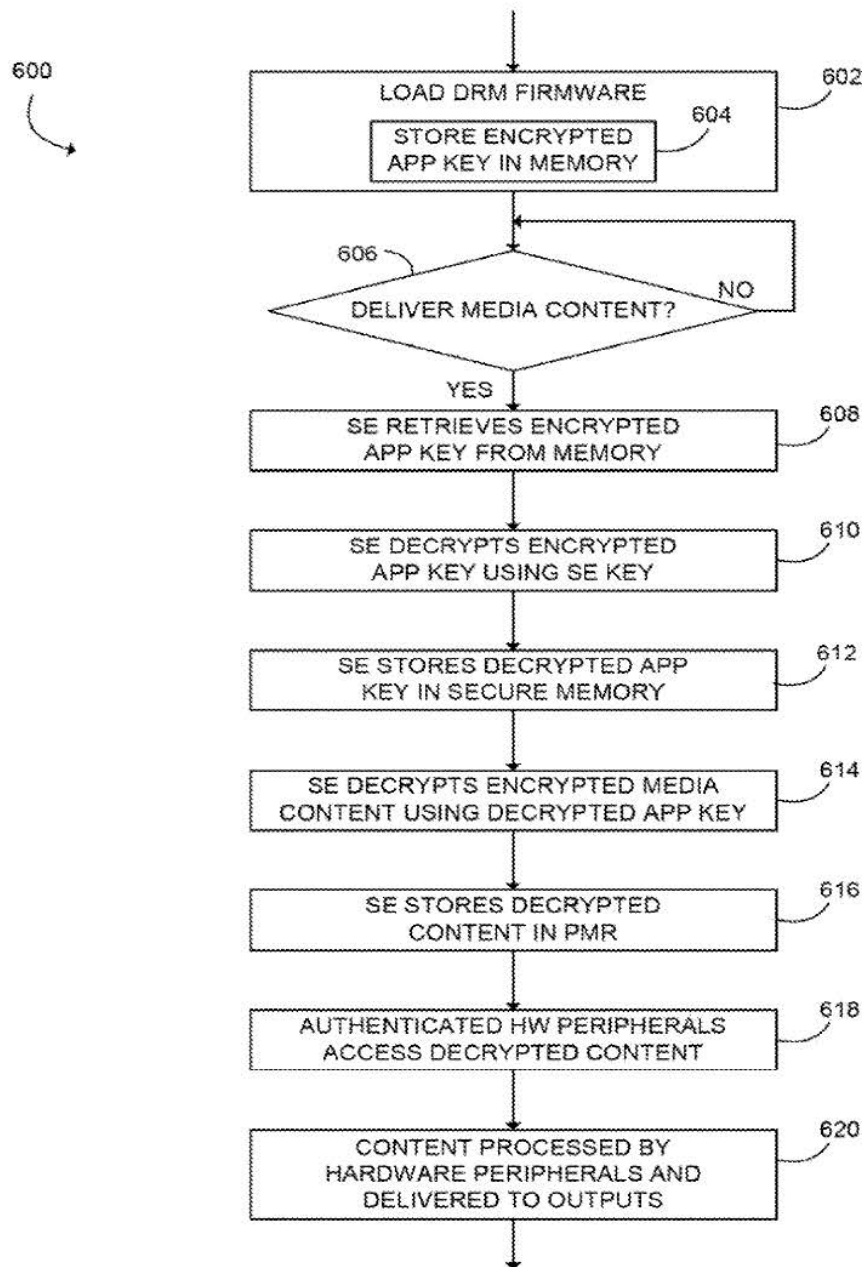


FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/065072**A. CLASSIFICATION OF SUBJECT MATTER****G06F 21/20(2006.01)i, G06F 21/22(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/20; G06F 12/14; H04L 9/32; H04L 9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords:

(SOC*,systemonchip*,systemonachip*,embed*,embedded*)+(peripheral*,demux*,video*,preparser*,DPE*,DSP*,audio*)+(firmwar*,soft
twar* applicat* PROGRAM* SW* DRIVER*)+(authentificat* access* VALIDATION* CERTIFIC*)+(proteect* secur* hidden* lock* shield**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	US 2004-0243823 A1 (MOYER WILLIAM C. et al.) 02 December 2004 See abstract, paragraphs [0011],[0014],[0017],[0022] and figures 1-3	1,2,14,30,31 3-13,15-29,32-40
Y A	US 2005-0114687 A1 (VINCENT ZIMMER et al.) 26 May 2005 See abstract, paragraphs [0048],[0062]-[0067] and figure 4,7	1,2,14,30,31 3-13,15-29,32-40
A	US 2007-0156987 A1 (IUE-SHUENN CHEN et al.) 05 July 2007 See abstract, paragraphs [0038]-[0039] and figure 5	1-40
A	US 2008-0022395 A1 (MICHAEL HOLTZMAN et al.) 24 January 2008 See abstract, paragraphs [0064],[0066] and figure 2	1-40

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

31 MAY 2012 (31.05.2012)

Date of mailing of the international search report

18 JULY 2012 (18.07.2012)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan
City, 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

UHM, In Kwon

Telephone No. 82-42-481-5712



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2011/065072

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004-0243823 A1	02.12.2004	CN 1799030 A	05.07.2006
		CN 1799030 C0	27.02.2008
		JP 2007-501477 A	25.01.2007
		JP 2007-501477 T	25.01.2007
		KR 10-1010801 B1	25.01.2011
		KR20060032954A	18.04.2006
		US 7444668 B2	28.10.2008
		WO 2004-107176 A1	09.12.2004
US 2005-0114687 A1	26.05.2005	None	
US 2007-0156987 A1	05.07.2007	None	
US 2008-0022395 A1	24.01.2008	CN 101484903 A	15.07.2009
		CN 101484904 A	15.07.2009
		CN 101490687 A	22.07.2009
		CN 101490688 A	22.07.2009
		CN 101490689 A	22.07.2009
		EP 2038799 A2	25.03.2009
		EP 2038800 A2	25.03.2009
		EP 2038802 A2	25.03.2009
		EP 2038803 A2	25.03.2009
		EP 2038804 A2	25.03.2009
		JP 2009-543207 A	03.12.2009
		JP 2009-543208 A	03.12.2009
		JP 2009-543210 A	03.12.2009
		JP 2009-543211 A	03.12.2009
		JP 2009-543212 A	03.12.2009
		KR 10-2009-0026357 A	12.03.2009
		KR 10-2009-0028806 A	19.03.2009
		KR 10-2009-0033191 A	01.04.2009
		KR 10-2009-0034332 A	07.04.2009
		KR 10-2009-0052321 A	25.05.2009
		TW 200821837 A	16.05.2008
		TW 200822669 A	16.05.2008
		TW 200822670 A	16.05.2008
		TW 200823715 A	01.06.2008
		US 2008-0010449 A1	10.01.2008
		US 2008-0010450 A1	10.01.2008
		US 2008-0010451 A1	10.01.2008
		US 2008-0010452 A1	10.01.2008
		US 2008-0010455 A1	10.01.2008
		US 2008-0010458 A1	10.01.2008
		US 2008-0010685 A1	10.01.2008
		US 2008-0022413 A1	24.01.2008
		US 2008-0034440 A1	07.02.2008
		US 2010-0138652 A1	03.06.2010
		US 8140843 B2	20.03.2012
		WO 2008-008243 A2	17.01.2008

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2011/065072

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		WO 2008-008243 A3	17.01.2008
		WO 2008-008244 A2	17.01.2008
		WO 2008-008244 A3	17.01.2008
		WO 2008-008245 A2	17.01.2008
		WO 2008-008245 A3	17.01.2008
		WO 2008-013655 A2	31.01.2008
		WO 2008-013655 A3	31.01.2008
		WO 2008-013656 A2	31.01.2008
		WO 2008-013656 A3	31.01.2008
		WO 2011-075281 A1	23.06.2011

Electronic Acknowledgement Receipt	
EFS ID:	16909180
Application Number:	13997412
International Application Number:	
Confirmation Number:	1045
Title of Invention:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor/Applicant Name:	Hormuzd M. Khosravi
Customer Number:	73486
Filer:	Christopher A. Singh/Brittany McCloud
Filer Authorized By:	Christopher A. Singh
Attorney Docket Number:	P41624US/45631-225521
Receipt Date:	20-SEP-2013
Filing Date:	
Time Stamp:	11:20:54
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Green Tech Petition under 37 CFR 1.102	P41624US_SupplDS.pdf	612830 5a8566ef4adc91a816249f359479533302c7824	no	1

Warnings:

Information:

2	Foreign Reference	FR1.pdf	1228206	no	26
			c5da4735459f3bc5744e3eb8d84f7aa02551fc1		
Warnings:					
Information:					
3	Foreign Reference	FR2.pdf	1249494	no	26
			77fcd878995bb12ae253529bdf57d40110685e0f		
Warnings:					
Information:					
4	Non Patent Literature	NPL1.pdf	976167	no	20
			4ce667bd5d0d998c2ce7b292fd3e9c5a9ecc8af72		
Warnings:					
Information:					
5	Non Patent Literature	NPL2.pdf	2347767	no	4
			8863815220bab4391cd0d500083aa49b92880637		
Warnings:					
Information:					
6	Non Patent Literature	NPL3.pdf	1487605	no	9
			059e827cc5d699e551c8c9a610c025afb1d3e785		
Warnings:					
Information:					
7	Non Patent Literature	NPL4.pdf	1221958	no	8
			496868b1fe5dcac1810daaf50ee89ad776f553030		
Warnings:					
Information:					
8	Non Patent Literature	NPL5.pdf	687585	no	4
			3e0eb18e2f1d3b019b77dc1990f8230515efc2c		
Warnings:					
Information:					
9	Non Patent Literature	NPL6.pdf	3129728	no	50
			d1dccb8dc9a44b0d323352b641ec73ba826858bd2		
Warnings:					
Information:					
Total Files Size (in bytes):			12941340		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)

Approved for use through 07/31/2012. OMB 0651-0031

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13997412
	Filing Date		2013-06-24
	First Named Inventor	Hormuzd M. Khosravi	
	Art Unit	UNK	
	Examiner Name	UNK	
	Attorney Docket Number	P41624US/45631-225521	

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8205238	B2	2012-06-19	Blumenthal et al.	
	2	7813822	B1	2010-10-12	Hoffberg	
	3	6324288	B1	2001-11-27	Hoffman	
If you wish to add additional U.S. Patent citation information please click the Add button.						
U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1.	20130080764	A1	2013-03-28	Khosravi et al.	
	2	20120137137	A1	2012-05-31	Brickell et al.	
	3	20110154061	A1	2011-06-23	Chilukuri et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13997412	
	Filing Date		2013-06-24	
	First Named Inventor	Hormuzd M. Khosravi		
	Art Unit	UNK		
	Examiner Name	UNK		
	Attorney Docket Number	P41624US/45631-225521		

	4	20080229104	A1	2008-09-18	Ju et al.	
	5	20080148061	A1	2008-06-19	Jin et al.	
	6	20080022395	A1	2008-01-24	Holtzman et al.	
	7	20070156987	A1	2007-07-05	Chen	
	8	20050114687	A1	2005-05-26	Zimmer et al.	
	9	20040243823	A1	2004-12-02	Moyer et al.	

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

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2013089728	WO	A1	2013-06-20	Intel Corporation		☐
	2	2013089726	WO	A1	2013-06-20	Intel Corporation		☐

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

NON-PATENT LITERATURE DOCUMENTS

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13997412
	Filing Date		2013-06-24
	First Named Inventor	Hormuzd M. Khosravi	
	Art Unit	UNK	
	Examiner Name	UNK	
	Attorney Docket Number	P41624US/45631-225521	

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	BAJIKAR, "Trusted Platform Module (TPM) based Security on Notebook PCs," White Paper, June 20, 2002, 20 pages.	☐
	2	INTEL CORP., "Product Brief: Intel® Atom™ Processor CE4100," 2009, 4 pages.	☐
	3	"Diffie-Hellman key exchange," Wikipedia, The Free Encyclopedia, available: <http://en.wikipedia.org/w/index.php?title=Diffie%E2%80%93Hellman_key_exchange&oldid=464229141>, accessed December 8, 2011, 9 pages.	☐
	4	"Elliptic curve cryptography," Wikipedia, The Free Encyclopedia, available: <http://en.wikipedia.org/w/index.php?title=Elliptic_curve_cryptography&oldid=464634149>, accessed December 8, 2011, 8 pages.	☐
	5	"Scrambler," Wikipedia, The Free Encyclopedia, available: <http://en.wikipedia.org/w/index.php?title=Scrambler&oldid=460036487>, accessed December 8, 2011, 4 pages.	☐
	6	U.S. Patent Application Serial No. 13/694,221, filed November 8, 2012, 50 pages.	☐

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

EXAMINER SIGNATURE

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

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

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

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

Application Number	13997412
Filing Date	2013-06-24
First Named Inventor	Hormuzd M. Khosravi
Art Unit	UNK
Examiner Name	UNK
Attorney Docket Number	P41624US/45631-225521

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/CHRISTOPHER A. SINGH/	Date (YYYY-MM-DD)	2013-09-20
Name/Print	CHRISTOPHER A. SINGH	Registration Number	61236

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

Privacy Act Statement

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

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

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

BARNES & THORNBURG LLP

11 South Meridian Street
Indianapolis, Indiana 46204

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Int'l Application No.: PCT/US2011/068279

Int'l Application Filing Date: December 15, 2011

U.S. Application No.: 13/997,412

Confirmation No.: 1045

Art Unit: Unknown

Examiner: Unknown

Application Title: METHOD AND DEVICE FOR
SECURE COMMUNICATIONS
OVER A NETWORK USING A
HARDWARE SECURITY ENGINE

First Named Inventor: Hormuzd M. Khosravi

Filed: June 24, 2013

Attorney Docket: P41624US/45631-225521

**ELECTRONICALLY
SUBMITTED ON:**

APRIL 3, 2014

**RESPONSE TO NOTIFICATION OF MISSING REQUIREMENTS UNDER 35 U.S.C. 371
IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US)**

MAIL STOP PCT
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

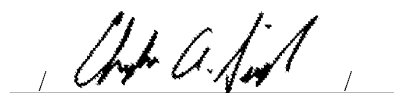
In response to the Notification of Missing Requirements under 35 U.S.C. 371 dated July 23, 2013, Applicants respectfully submit herewith:

1. An executed Declaration signed by inventor Farhana Kabir identifying the present application by the International application number and international filing date; and

2. An executed Supplemental Declaration signed by inventor Hormuzd M. Khosravi and an executed Supplemental Declaration signed by inventor Edward C. Epp, each identifying the present application by the International application number and international filing date, and each being in compliance with 37 CFR 1.497(a) and (b).

Applicants believe this submission completes the requirements for acceptance under 35 U.S.C. 371. No fee is believed to be due with regard to this submission. However, the Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment, to Deposit Account No. 50-4238 with reference to Docket No. P41624US.

Respectfully submitted,



Christopher A. Singh
Registration No. 61,236
Barnes & Thornburg LLP
11 South Meridian Street
Indianapolis, Indiana 46204-3535
Telephone: (317) 231-6458
Fax: (317) 231-7433

Docket No.: P41624US
PATENT

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, mailing address, and citizenship are as stated below, next to my name.

I believe I am the original and first inventor (if only one name is listed below) or an original and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE

the specification of which (check one):

is attached hereto.
X was filed on June 24, 2013 as
 United States Application Number 13/997,412
 or PCT International Application Number _____
 and was amended on _____.
 (If applicable)

I hereby authorize and request my attorney, associated with Customer Number 73486, to insert on the designated lines above, the filing date, application number, PCT International Application Number and amendment date, as applicable, of the patent application should this Declaration be filed after filing the specification.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment specifically referred to above.

I hereby claim the benefit under 35 U.S.C. § 120 or 365(c) of any United States and PCT international application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose material information as defined in 37 C.F.R. § 1.56(a) which became available between the filing date of the prior application and the national or PCT international filing date of this application:

PCT International Application No. PCT/US2011/065069 filed December 15, 2011.

I acknowledge the duty to disclose all information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim the benefit under 35 U.S.C § 119(e) of any United States provisional application(s) listed below:

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)	Priority Claimed?	Certified Copy Attached?

Docket No.: P41624US
PATENT

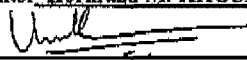
(Number)	(Country)	(Foreign Filing Date - MM/DD/YYYY)	Yes	No	Yes	No
(Number)	(Country)	(Foreign Filing Date - MM/DD/YYYY)	Yes	No	Yes	No
(Number)	(Country)	(Foreign Filing Date - MM/DD/YYYY)	Yes	No	Yes	No

I hereby appoint practitioners associated with the Customer Number: **73486**
as my/our attorney(s) or agents(s), with full power of substitution and revocation, to prosecute this application and to
transact all business in the United States Patent and Trademark Office connected therewith.

Please direct all correspondence to the address associated with the Customer Number: **73486**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made
on information and belief are believed to be true; and further that these statements were made with the
knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both,
under Section 1001 of Title 18 of the United States Code and that such willful false statements may
jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor: **Hormuzd M. KHOSRAVI**

Inventor's Signature  Date 3/14/2014
Residence Portland, OR Citizenship ~~India~~ U.S.A
(City, State) (Country) 

Post Office Address 4737 NW Rainier Ter
Portland, OR 97229

Full Name of Second/Joint Inventor: **Edward C. EPP**

Inventor's Signature _____ Date _____
Residence Portland, OR Citizenship United States of America
(City, State) (Country)

Post Office Address 3035 NE 23rd Av
Portland, OR 97212

Docket No.: P41624US
PATENT

Full Name of Third/Joint Inventor Farhana KABIR

Inventor's Signature _____ Date _____

Residence Camas, WA _____ Citizenship United States of America
(City, State) (Country)

Post Office Address 20021 SE 3rd Circle
Camas, WA 98607

Docket No.: P41624US
PATENT

Title 37, Code of Federal Regulations, Section 1.56
Duty to Disclose Information Material to Patentability

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclose information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

- (1) Prior art cited in search reports of a foreign patent office in a counterpart application, and
- (2) The closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.
- (b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and
 - (1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or
 - (2) It refutes, or is inconsistent with, a position the applicant takes in:
 - (i) Opposing an argument of unpatentability relied on by the Office, or
 - (ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

- (c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:
 - (1) Each inventor named in the application;
 - (2) Each attorney or agent who prepares or prosecutes the application; and
 - (3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.
- (d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.
- (e) In any continuation-in-part application, the duty under this section includes the duty to disclose to the Office all information known to the person to be material to patentability, as defined in paragraph (b) of this section, which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.
- (d)

Docket No.: P41624US
PATENT**DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION**

As a below named inventor, I hereby declare that:

My residence, mailing address, and citizenship are as stated below, next to my name.

I believe I am the original and first inventor (if only one name is listed below) or an original and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

**METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A
HARDWARE SECURITY ENGINE**

the specification of which (check one):

 X is attached hereto.
 X was filed on June 24, 2013 as
 United States Application Number 13/997,412
 or PCT International Application Number _____
 and was amended on _____
 (if applicable)

I hereby authorize and request my attorney, associated with Customer Number 73486, to insert on the designated lines above, the filing date, application number, PCT International Application Number and amendment date, as applicable, of the patent application should this Declaration be filed after filing the specification.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment specifically referred to above.

I hereby claim the benefit under 35 U.S.C. § 120 or 365(c) of any United States and PCT international application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose material information as defined in 37 C.F.R. § 1.56(a) which became available between the filing date of the prior application and the national or PCT international filing date of this application:

PCT International Application No. PCT/US2011/065069 filed December 15, 2011.

I acknowledge the duty to disclose all information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim the benefit under 35 U.S.C § 119(e) of any United States provisional application(s) listed below:

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed:

<u>Prior Foreign Application(s)</u>	<u>Priority Claimed?</u>	<u>Certified Copy Attached?</u>
_____	_____	_____

Docket No.: P41624US
PATENT

(Number)	(Country)	(Foreign Filing Date - MM/DD/YYYY)	Yes	No	Yes	No
____	____	____	____	____	____	____
____	____	____	____	____	____	____
____	____	____	____	____	____	____

I hereby appoint practitioners associated with the Customer Number: **73486**
as my/our attorney(s) or agents(s), with full power of substitution and revocation, to prosecute this application and to transact all business in the United States Patent and Trademark Office connected therewith.

Please direct all correspondence to the address associated with the Customer Number: **73486**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

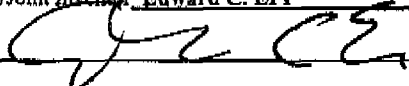
Full Name of Sole/First Inventor Hormuzd M. KHOSRAVI

Inventor's Signature _____ Date _____

Residence Portland, OR Citizenship India
(City, State) (Country)

Post Office Address 4737 NW Rainier Ter
Portland, OR 97229

Full Name of Second/Joint Inventor Edward C. EPP

Inventor's Signature  Date 3-14-19

Residence Portland, OR Citizenship United States of America
(City, State) (Country)

Post Office Address 3035 NE 23rd Av
Portland, OR 97212

Docket No.: P41624US
PATENT

Full Name of Third/Joint Inventor Farhana KABIR

Inventor's Signature _____ Date _____

Residence Camas, WA _____ Citizenship United States of America
(City, State) (Country)

Post Office Address 20021 SE 3rd Circle
Camas, WA 98607

Docket No.: P41624US
PATENT

Title 37, Code of Federal Regulations, Section 1.56
Duty to Disclose Information Material to Patentability

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclose information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine;

(1) Prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) The closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application;

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.

(e) In any continuation-in-part application, the duty under this section includes the duty to disclose to the Office all information known to the person to be material to patentability, as defined in paragraph (b) of this section, which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

(d)

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, mailing address, and citizenship are as stated below, next to my name.

I believe I am the original and first inventor (if only one name is listed below) or an original and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

**METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A
HARDWARE SECURITY ENGINE**

the specification of which (check one):

_____ is attached hereto.
X_____ was filed on June 24, 2013 as
United States Application Number 13/997,412
or PCT International Application Number _____
and was amended on _____
(if applicable)

I hereby authorize and request my attorney, associated with Customer Number 73486, to insert on the designated lines above, the filing date, application number, PCT International Application Number and amendment date, as applicable, of the patent application should this Declaration be filed after filing the specification.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment specifically referred to above.

I hereby claim the benefit under 35 U.S.C. § 120 or 365(c) of any United States and PCT international application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose material information as defined in 37 C.F.R. § 1.56(a) which became available between the filing date of the prior application and the national or PCT international filing date of this application:

PCT International Application No. PCT/US2011/065069 filed December 15, 2011.

I acknowledge the duty to disclose all information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim the benefit under 35 U.S.C § 119(c) of any United States provisional application(s) listed below:

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed:

<u>Prior Foreign Application(s)</u>	<u>Priority Claimed?</u>	<u>Certified Copy Attached?</u>
_____	_____	_____

(Number)	(Country)	(Foreign Filing Date - MM/DD/YYYY)	Yes	No	Yes	No
____	____	____	____	____	____	____
(Number)	(Country)	(Foreign Filing Date - MM/DD/YYYY)	Yes	No	Yes	No
____	____	____	____	____	____	____
(Number)	(Country)	(Foreign Filing Date - MM/DD/YYYY)	Yes	No	Yes	No
____	____	____	____	____	____	____

I hereby appoint practitioners associated with the Customer Number: 73486
as my/our attorney(s) or agents(s), with full power of substitution and revocation, to prosecute this application and to
transact all business in the United States Patent and Trademark Office connected therewith.

Please direct all correspondence to the address associated with the Customer Number: 73486

I hereby declare that all statements made herein of my own knowledge are true and that all statements made
on information and belief are believed to be true; and further that these statements were made with the
knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both,
under Section 1001 of Title 18 of the United States Code and that such willful false statements may
jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor Hormuzd M. KHOSRAVI

Inventor's Signature _____ Date _____

Residence Portland, OR Citizenship India
(City, State) (Country)

Post Office Address 4737 NW Rainier Ter
Portland, OR 97229

Full Name of Second/Joint Inventor Edward C. EPP

Inventor's Signature _____ Date _____

Residence Portland, OR Citizenship United States of America
(City, State) (Country)

Post Office Address 3035 NE 23rd Av
Portland, OR 97212

Docket No.: P41624US
PATENT

Full Name of Third/Joint Inventor Farhana KABIR
Inventor's Signature Farhana M. Kabir Date 03/24/2014
Residence Camas, WA Citizenship United States of America
(City, State) (Country)
Post Office Address 20021 SE 3rd Circle
Camas, WA 98607

Title 37, Code of Federal Regulations, Section 1.56
Duty to Disclose Information Material to Patentability

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclose information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

- (1) Prior art cited in search reports of a foreign patent office in a counterpart application, and
- (2) The closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and

- (1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or
- (2) It refutes, or is inconsistent with, a position the applicant takes in:
 - (i) Opposing an argument of unpatentability relied on by the Office, or
 - (ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

- (1) Each inventor named in the application;
 - (2) Each attorney or agent who prepares or prosecutes the application; and
 - (3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.
- (d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.
 - (e) In any continuation-in-part application, the duty under this section includes the duty to disclose to the Office all information known to the person to be material to patentability, as defined in paragraph (b) of this section, which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.
 - (d)

Electronic Acknowledgement Receipt	
EFS ID:	18662321
Application Number:	13997412
International Application Number:	
Confirmation Number:	1045
Title of Invention:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor/Applicant Name:	Hormuzd M. Khosravi
Customer Number:	73486
Filer:	Christopher A. Singh/Ernest Carlson
Filer Authorized By:	Christopher A. Singh
Attorney Docket Number:	P41624US/45631-225521
Receipt Date:	03-APR-2014
Filing Date:	
Time Stamp:	13:13:21
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	225521TransmittalLetter.pdf	134279 72745e44c03823e08f2316d04d2a795bc19594f5	no	3

Warnings:

Information:

2	Supplemental Response or Supplemental Amendment	P41624US_RespNotificationMissingReqs.pdf	113885 6baaac009c4528e48dd6ff1ceafae9e530fdacla	no	2
Warnings:					
Information:					
3	Oath or Declaration filed	P41624US_Declarations.pdf	368819 a550d522852ece44ba01d13c071081d87a711aa	no	12
Warnings:					
Information:					
Total Files Size (in bytes):			616983		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A SUBMISSION UNDER 35 U.S.C. 371		Attorney Docket No. P41624US/45631-225521
International Application No. PCT/US2011/065069		U.S. Application No. (if known, see 37 CFR 1.5) 13/997,412
International Filing Date 15 December 2011 (15.12.11)	Priority Date Claimed 15 December 2011 (15.12.11)	
Title of Invention METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE		
First Named Inventor KHOSRAVI, Hormuzd M., et al.		
Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information. 1. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). NOTE: The express request under 35 U.S.C. 371(f) will not be effective unless the requirements under 35 U.S.C. 371(c)(1), (2), and (4) for payment of the basic national fee, copy of the International Application and English translation thereof (if required), and the oath or declaration of the inventor(s) have been received. 2. ☐ A copy of the International Application (35 U.S.C. 371(c)(2)) is attached hereto (not required if the International Application was previously communicated by the International Bureau or was filed in the United States Receiving Office (RO/US)). 3. An English language translation of the International Application (35 U.S.C. 371(c)(2)) a. ☐ is attached hereto. b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4). 4. An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)) a. ☒ is attached. b. ☐ was previously filed in the international phase under PCT Rule 4.17(iv). Items 5 to 8 below concern amendments made in the international phase. <u>PCT Article 19 and 34 amendments</u> 5. ☐ Amendments to the claims under PCT Article 19 are attached (not required if communicated by the International Bureau) (35 U.S.C. 371(c)(3)). 6. ☐ English translation of the PCT Article 19 amendment is attached (35 U.S.C. 371(c)(3)). 7. ☐ English translation of annexes (Article 19 and/or 34 amendments only) of the International Preliminary Examination Report is attached (35 U.S.C. 371(c)(5)). <u>Cancellation of amendments made in the international phase</u> 8a. ☐ Do not enter the amendment made in the international phase under PCT Article 19. 8b. ☐ Do not enter the amendment made in the international phase under PCT Article 34. NOTE: A proper amendment made in English under Article 19 or 34 will be entered in the U.S. national phase application absent a clear instruction from applicant not to enter the amendment(s). The following items 9 to 17 concern a document(s) or information included. 9. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98. 10. ☐ A preliminary amendment. 11. ☐ An Application Data Sheet under 37 CFR 1.76. 12. ☐ A substitute specification. NOTE: A substitute specification cannot include claims. See 37 CFR 1.125(b). 13. ☐ A power of attorney and/or change of address letter. 14. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.3 and 37 CFR 1.821-1.825. 15. ☐ Assignment papers (<i>cover sheet and document(s)</i>). Name of Assignee: _____ 16. ☐ 37 CFR 3.73(c) Statement (<i>when there is an Assignee</i>). _____		

This collection of information is required by 37 CFR 1.414 and 1.491-1.492. The information is required to obtain or retain a benefit by the public, which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 15 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

U.S. APPLN. No. (if known – see 37 CFR 1.5) 13/997,412	INTERNATIONAL APPLICATION No. PCT/US2011/065069	ATTORNEY DOCKET No. P41624US/45631-225521
17. ☒ Other items or information: RESPONSE TO NOTIFICATION OF MISSING REQUIREMENTS UNDER 35 U.S.C. 371 IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US)		
The following fees have been submitted.		CALCULATIONS PTO USE ONLY
18. ☐ Basic national fee (37 CFR 1.492(a)) \$280		\$
19. ☐ Examination fee (37 CFR 1.492(c)) If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4) \$0 All other situations \$720		\$
20. ☐ Search fee (37 CFR 1.492(b)) If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4) \$0 Search fee (37 CFR 1.445(a)(2)) has been paid on the international application to the USPTO as an International Searching Authority \$120 International Search Report prepared by an ISA other than the US and provided to the Office or previously communicated to the US by the IB \$480 All other situations \$600		\$
TOTAL OF 18, 19, and 20 =		\$ 0.00
☐ Additional fee for specification and drawings filed in paper over 100 sheets (excluding sequence listing in compliance with 37 CFR 1.821(c) or (e) in an electronic medium or computer program listing in an electronic medium) (37 CFR 1.492(j)). Fee for each additional 50 sheets of paper or fraction thereof \$400		
Total Sheets	Extra Sheets	Number of each addition 50 or fraction thereof (round up to a whole number)
- 100 =	/ 50 =	x \$400
		\$
Surcharge of \$140.00 for furnishing any of the search fee, examination fee, or the oath or declaration after the date of commencement of the national stage (37 CFR 1.492(h)).		\$
CLAIMS	NUMBER FILED	NUMBER EXTRA
Total claims	- 20 =	x \$80
Independent claims	- 3 =	x \$420
MULTIPLE DEPENDENT CLAIM(S) (if applicable)		+ \$780
Processing fee of \$140.00 for furnishing the English translation later than 30 months from the earliest claimed priority date (37 CFR 1.492(i)).		\$
TOTAL OF ABOVE CALCULATIONS =		\$ 0.00
☒ Applicant asserts small entity status. See 37 CFR 1.27. Fees above are reduced by ½.		
☐ Applicant certifies micro entity status. See 37 CFR 1.29. Fees above are reduced by ¾. Applicant must attach form PTO/SB/15A or B or equivalent.		
TOTAL NATIONAL FEE =		\$ 0.00
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). \$40.00 per property.		\$
TOTAL FEES ENCLOSED =		\$ 0.00
		Amount to be refunded:
		\$
		Amount to be charged:
		\$

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.

a. ☐ A check in the amount of \$_____ to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of \$_____ to cover the above fees.

c. ☒ The Director is hereby authorized to charge additional fees which may be required, or credit any overpayment, to Deposit Account No. 50-4238 as follows:

i. ☐ any required fee.

ii. ☐ any required fee except for excess claims fees required under 37 CFR 1.492(d) and (e) and multiple dependent claim fee required under 37 CFR 1.492(f).

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038. The PTO-2038 should only be mailed or faxed to the USPTO. However, when paying the basic national fee, the PTO-2038 may NOT be faxed to the USPTO.

ADVISORY: If filing by EFS-Web, do **NOT** attach the PTO-2038 form as a PDF along with your EFS-Web submission. Please be advised that this is **not** recommended and by doing so your **credit card information may be displayed via PAIR**. To protect your information, it is recommended to pay fees online by using the electronic payment method.

NOTE: Where an appropriate time limit under 37 CFR 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the International Application to pending status.

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

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013, and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.

NOTE: A U.S. national stage application may not claim priority to the international application of which it is the national phase. The filing date of a U.S. national stage application is the international filing date. See 35 U.S.C. 363.

Correspondence Address

☒ The address associated with Customer Number: 73456 OR ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country				Telephone	
Email					

Signature	/Christopher A. SINGH/	Date	2014-04-03
Name (Print/Type)	Christopher A. SINGH	Registration No. (Attorney/Agent)	61236

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)

Approved for use through 07/31/2012. OMB 0651-0031

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13997412	
	Filing Date		2013-06-24	
	First Named Inventor	Hormuzd M. Khosravi		
	Art Unit	UNK		
	Examiner Name	UNK		
	Attorney Docket Number	P41621US/45631-225520		

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8295484	B2	2012-10-23	Buer et al.	
If you wish to add additional U.S. Patent citation information please click the Add button.						Add
U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20140129827	A1	2014-05-08	Khosravi et al.	
	2	20130297936	A1	2013-11-07	Khosravi et al.	
	3	20130275769	A1	2013-10-17	Khosravi et al.	US equivalent of TW 201340692 below.
	4	20120079287	A1	2012-03-29	Leclercq	
	5	20070209072	A1	2007-09-06	Chen	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13997412	
	Filing Date		2013-06-24	
	First Named Inventor	Hormuzd M. Khosravi		
	Art Unit	UNK		
	Examiner Name	UNK		
	Attorney Docket Number	P41621US/45631-225520		

	6	20020163522	A1	2002-11-07	Porter et al.	
--	---	-------------	----	------------	---------------	--

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

FOREIGN PATENT DOCUMENTS

Remove

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	201340692	TW	A	2013-10-01	Intel Corporation	Taiwanese equivalent of US 20130275769 above.	☒

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

NON-PATENT LITERATURE DOCUMENTS

Remove

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

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

EXAMINER SIGNATURE

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

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	13997412
	Filing Date	2013-06-24
	First Named Inventor	Hormuzd M. Khosravi
	Art Unit	UNK
	Examiner Name	UNK
	Attorney Docket Number	P41621US/45631-225520

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/CHRISTOPHER A. SINGH/	Date (YYYY-MM-DD)	2014-05-27
Name/Print	CHRISTOPHER A. SINGH	Registration Number	61236

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

Privacy Act Statement

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

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

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



(19)中華民國智慧財產局

(12)發明說明書公開本

(11)公開編號：TW 201340692 A

(43)公開日：中華民國 102 (2013) 年 10 月 01 日

(21)申請案號：101147203

(22)申請日：中華民國 101 (2012) 年 12 月 13 日

(51)Int. Cl.:

H04N21/4367(2011.01)

G06F21/10 (2013.01)

(30)優先權：2011/12/15

世界智慧財產權組織

PCT/US11/65072

(71)申請人：英特爾股份有限公司(美國) INTEL CORPORATION (US)

美國

(72)發明人：柯斯拉維 荷姆茲 KHOSRAVI, HORMUZD M. (IN)；摩吉拉帕葛利 蘇德希爾 MOGILAPPAGARI, SUDHEER (IN)；庫斯華哈 普李亞利 KUSHWAHA, PRIYALEE (IN)；雪魯夫 蘇尼爾 CHERUVU, SUNIL K. (US)；休梅爾 大衛 SCHOLLMAYER, DAVID A. (US)

(74)代理人：林志剛

申請實體審查：有 申請專利範圍項數：40 項 圖式數：6 共 37 頁

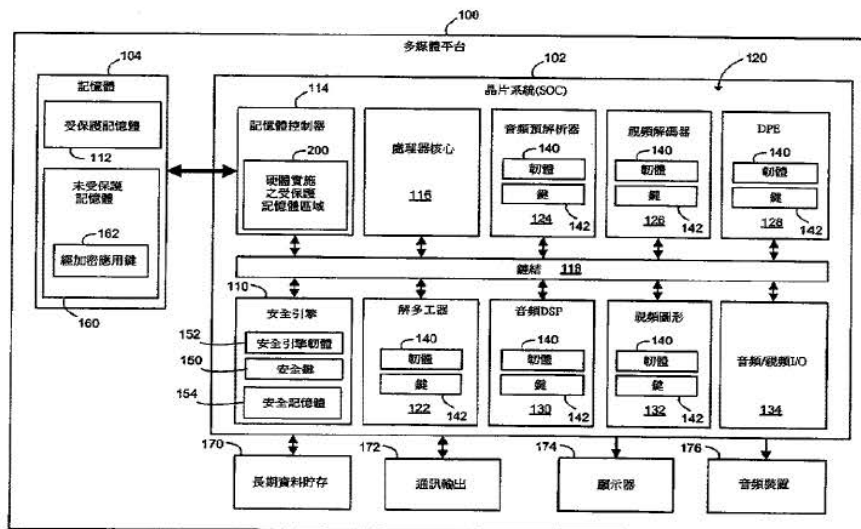
(54)名稱

用以保護並安全地傳遞媒體內容之方法，裝置，及系統

METHOD, DEVICE, AND SYSTEM FOR PROTECTING AND SECURELY DELIVERING MEDIA CONTENT

(57)摘要

用以保護並安全地傳遞媒體內容之方法、裝置、及系統包括組態晶片系統(SOC)之記憶體控制器以建立受保護記憶體區域，使用該 SOC 之安全引擎來鑑別硬體週邊的韌體，並儲存該經鑑別韌體於該受保護記憶體區域中。該安全引擎可藉由鑑別用來加密該韌體之週邊密碼鍵來鑑別該韌體。僅經鑑別硬體週邊可存取該受保護記憶體區域。



- 100：多媒體平台
- 102：晶片系統(SOC)
- 104：記憶體
- 110：安全引擎
- 112：受保護記憶體
- 114：記憶體控制器
- 116：處理器核心
- 118：鏈結
- 122：解多工器
- 124：音頻預解析器
- 126：視頻解碼器
- 130：音頻 DSP
- 132：視頻圖形
- 134：音頻/視頻 I/O
- 140：韌體

TW 201340692 A

142：鍵
150：安全鍵
152：安全引擎韌體
154：安全記憶體
160：未受保護記憶體
162：經加密應用鍵
170：長期資料貯存
172：通訊輸出
174：顯示器
176：音頻裝置
200：硬體實施之受保護記憶體區域



(19)中華民國智慧財產局

(12)發明說明書公開本

(11)公開編號：TW 201340692 A

(43)公開日：中華民國 102 (2013) 年 10 月 01 日

(21)申請案號：101147203

(22)申請日：中華民國 101 (2012) 年 12 月 13 日

(51)Int. Cl.:

H04N21/4367(2011.01)

G06F21/10 (2013.01)

(30)優先權：2011/12/15

世界智慧財產權組織

PCT/US11/65072

(71)申請人：英特爾股份有限公司(美國) INTEL CORPORATION (US)

美國

(72)發明人：柯斯拉維 荷姆茲 KHOSRAVI, HORMUZD M. (IN)；摩吉拉帕葛利 蘇德希爾 MOGILAPPAGARI, SUDHEER (IN)；庫斯華哈 普李亞利 KUSHWAHA, PRIYALEE (IN)；雪魯夫 蘇尼爾 CHERUVU, SUNIL K. (US)；休梅爾 大衛 SCHOLLMAYER, DAVID A. (US)

(74)代理人：林志剛

申請實體審查：有 申請專利範圍項數：40 項 圖式數：6 共 37 頁

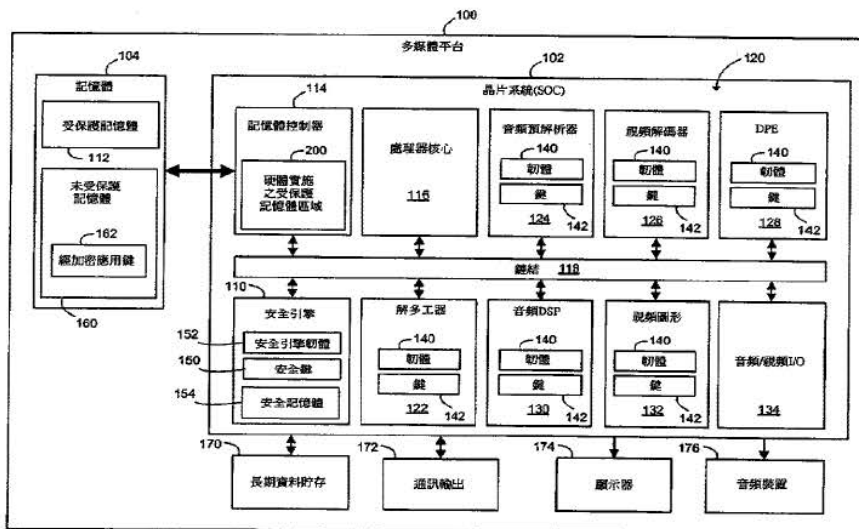
(54)名稱

用以保護並安全地傳遞媒體內容之方法，裝置，及系統

METHOD, DEVICE, AND SYSTEM FOR PROTECTING AND SECURELY DELIVERING MEDIA CONTENT

(57)摘要

用以保護並安全地傳遞媒體內容之方法、裝置、及系統包括組態晶片系統(SOC)之記憶體控制器以建立受保護記憶體區域，使用該 SOC 之安全引擎來鑑別硬體週邊的韌體，並儲存該經鑑別韌體於該受保護記憶體區域中。該安全引擎可藉由鑑別用來加密該韌體之週邊密碼鍵來鑑別該韌體。僅經鑑別硬體週邊可存取該受保護記憶體區域。



- 100：多媒體平台
- 102：晶片系統(SOC)
- 104：記憶體
- 110：安全引擎
- 112：受保護記憶體
- 114：記憶體控制器
- 116：處理器核心
- 118：鏈結
- 122：解多工器
- 124：音頻預解析器
- 126：視頻解碼器
- 130：音頻 DSP
- 132：視頻圖形
- 134：音頻/視頻 I/O
- 140：韌體

六、發明說明：

【發明所屬之技術領域】

本發明係有關用以保護並安全地傳遞媒體內容之方法，裝置，及系統。

【先前技術】

內容使用者存取媒體內容的方式正從傳統的伺機存取改變成按需（on-demand）存取。按需媒體內容，還有一些標準的媒體內容，時常藉由串流內容至多媒體平台而遞送，多媒體平台例如機上盒、智慧型手機、電腦桌、膝上型電腦、或類似者。如果多媒體內容為付費內容，在傳送到多媒體平台期間常以某種方式保護多媒體內容。例如，各種數位版權管理（DRM）及條件式存取（CA）技術可用來提供自媒體來源至多媒體平台的多媒體內容之保護。這樣的技術一般涉及內容媒體之加密。

晶片系統（SOC）為除了處理核心外另合併電子系統的各種構件於單一晶粒上之積體電路。例如，SOC可包括在單一晶片上之處理器核心、記憶體控制器、視頻構件、音頻構件、及/或通訊構件。由於其相對小的尺寸，SOC用於許多多媒體平台中。

【發明內容及實施方式】

雖然本公開之概念可輕易有各種修改及替代形式，其特定示範實施例已在圖中舉例顯示並將詳細在此說明。然

而，應了解到未意欲限制本公開的概念於所揭露之特定形式，但相反地，意在涵蓋與本公開及所附之申請專利範圍一致之所有修改、等效者、及替代。

在下列說明中，提出比如邏輯實作、運算碼、指定運算元之機構、來源分割/共享/複製實作、系統構件之類型及相互關係、及邏輯分割/整合選擇之各種特定細節，以提供本公開之更詳盡的理解。然而，熟悉此技藝人士可認知到公開之實施例可在無這種特定細節下加以實行。在其他例子中，並未詳細顯示控制結構、閘級電路、及完整軟體指令序列以不混淆本發明。此技藝中具有通常知識者，有鑑於所含之說明，將得以實施適當的功能而無需過度實驗。

說明書中對於「一實施例（one embodiment 或 an embodiment）」、「一範例實施例」等等之參照指示所述的實施例可包括特定特徵、結構、或特性，但每一個實施例並非一定都包括該特徵、結構、或特性。此外，這樣的詞語並非皆參照相同的實施例。另外，當連同一實施例敘述特定特徵、結構、或特性時，連同其他實施例（無論明確說明與否）實現這種特徵、結構、或特性應在熟悉此技藝人士的知識內。

可在硬體、韌體、軟體、或上述之任何組合中實現本發明之實施例。在電腦系統中實現的本發明之實施例可包括在構件間之一或更多個匯流排為基之互連或鏈結及/或構件間之一或更多個點對點互連。也可將本發明之實施例

實現為由暫態或非暫態機器可讀取媒體進行或儲存之指令，該機器可讀取媒體可由一或更多個處理器讀取並執行。機器可讀取媒體可體現為任何裝置、機制、或實體結構，以儲存或傳送具有機器（如計算裝置）可讀取形式之資訊。例如，機器可讀取媒體可體現為唯讀記憶體（ROM）、隨機存取記憶體（RAM）、磁碟儲存媒體、光學儲存媒體、快閃記憶體裝置、迷你或微型SD卡、記憶棒、電性信號、及其他者。

在圖中，為了方便說明可能顯示比如代表裝置、模組、指令區塊及資料元件的那些之示意元件的特定配置或排列。然而，熟悉此技藝人士應可了解到圖中的示意元件之特定排序或配置並非意圖暗示需要處理之特定順序或序列，或程序之分離。此外，圖中之示意元件的包括並非意圖暗示在所有實施例中都需要這種元件或由這種元件代表的特徵可能不包括在一些實施例中或在一些實施例中與其他元件結合。

一般而言，可使用任何適當形式的機器可讀取指令，比如軟體或韌體應用、程式、函數、模組、常式、程序（process）、步驟（procedure）、插件、小程序（applet）、小工具（widget）、碼段及/或其他者，來實現用來代表指令區塊之示意元件，並可使用任何適當的編程語言、程式庫、應用編程介面（API）、及/或其他軟體開發工具，來實現每一個這樣的指令。例如，可使用Java、C++、及/或其他程式語言來實現一些實施例。類似地，可使用

任何適當的電子配置或結構，比如暫存器、資料貯存、表、記錄、陣列、索引、散列、映圖、樹、列表、圖、檔案（任何檔案類型）、檔案夾、目錄、資料庫、及/或其他者，來實現用來代表資料或資訊之示意元件。

此外，在圖中，在比如實或虛線或箭頭之連接元件用來繪示兩或更多個其他的示意元件之間的連結、關係、或關聯之處，任何這種連接元件之缺少並非意圖暗示無連結、關係、或關聯可存在。換言之，元件之間的一些連結、關係、或關聯可能未顯示在圖中以不混淆本公開。另外，爲了方便繪示，單一連接元件可用來代表元件間之多個連結、關係、或關聯。例如，在一連接元件代表信號、資料、或指令的通訊之處，熟悉此技藝人士應可了解到，有需要時，這種元件可代表一或更多個信號路徑（如匯流排）來實現該通訊。

茲參照第 1 圖，在一實施例中，多媒體平台 100 組態成傳遞媒體內容至平台 100 之使用者。多媒體平台 100 可體現成組態成傳遞媒體內容的任何類型之裝置。例如，多媒體平台 100 可體現爲機上盒、智慧型手機、平板電腦、膝上型電腦、行動上網裝置（MID）、桌上型電腦、或能夠傳遞媒體內容之其他裝置。多媒體平台 100 可組態成傳遞任何類型的媒體內容至使用者，包括，例如，電影、圖案、影像、歌曲、音頻、及/或視頻記錄、及/或任何其他類型之音頻、視頻、及/或音頻和視頻內容。

多媒體平台 100 包括晶片系統（SOC）102 及平台記

憶體 104。將於後更詳細討論，SOC 102 組態成當媒體內容在 SOC 102 及記憶體 104 內的同時保護並安全地傳遞媒體內容。要這樣做，SOC 102 的安全引擎 110 在記憶體 104 中建立受保護記憶體 112，由記憶體 104 之記憶體控制器 114 硬體實施該記憶體。記憶體控制器 114 確保僅 SOC 102 之經授權的硬體週邊可存取受保護記憶體 112。SOC 102 之安全引擎 110 藉由在載入韌體到受保護記憶體 112 中之前鑑別每一個週邊的韌體來授權每一個硬體週邊。經解密的媒體內容也儲存於受保護記憶體 112 中並僅可由經授權的硬體週邊存取。依此方式，在 SOC 102 中建立受信賴的資料路徑，其中僅可由 SOC 102 之經鑑別構件存取經解密的媒體內容。

SOC 102 可體現成任何類型的晶片系統，其可包括各種構件及結構。在第 1 圖之例示實施例中，SOC 102 包括如上所述之安全引擎 110 及記憶體控制器 114、處理器核心 116、及複數個硬體週邊 120，其經由鏈結 118 互相通訊式耦合。鏈結 118 可體現成任何類型的互連，比如匯流排、點對點、或能夠促進 SOC 102 之各種構件間的通訊之其他互連。硬體週邊 120 可包括取決於 SOC 102 的預定功能之任何類型的硬體週邊構件。例如，在例示實施例中，硬體週邊 120 包括解多工器 122、視頻預解析器 124、視頻解碼器 126、顯示處理引擎（DPE）128、音頻數位信號處理器（DSP）130、視頻圖形 132、及音頻/視頻 I/O 134。硬體週邊 120 之每一者包括一關聯的韌體

140 及一密碼鍵 142。將於後更詳細討論，由安全引擎 110 使用安全引擎 110 的安全鍵 150 事先簽署每一個硬體週邊 120 的密碼鍵 142。

安全引擎 110 可體現為與處理器核心 116 分離之安全共處理器或處理電路。安全引擎 110 包括安全引擎韌體 152 及安全記憶體 154，其僅可由安全引擎 110 存取。在例示實施例中，安全記憶體 154 形成安全引擎 110 之實體部分，但在其他實施例中可形成記憶體 104 之一部分（亦即，受保護記憶體 112 之一部分）。安全引擎 110 儲存安全鍵 150，及如下所討論之其他密碼鍵，於安全記憶體 154 中。安全鍵 150 可在 SOC 102 的製造期間提供或可由 SOC 102 在操作期間產生。例如，在一些實施例中，安全鍵 150 係基於安全引擎 110 內的已熔斷的保險絲（blown fuses）。額外或替代地，安全引擎 110 可包括鍵產生模組，比如受信賴平台模組（TPM），來產生安全鍵 150。於使用期間，安全引擎 110 可使用任何數量的安全鍵 150，其可為彼此相同或不同。

如上所討論，記憶體 104 包括受保護記憶體 112 及未受保護記憶體 160。各種資料可於多媒體平台 100 的操作期間以經解密或加密的形式儲存於未受保護記憶體 160 中。例如，如下更詳細討論，經加密應用鍵 162 可連同用於傳遞給使用者之任何經加密的媒體內容儲存於記憶體 104 的未受保護記憶體 160 中。

在一些實施例中，多媒體平台 100 可包括除了 SOC

102 和記憶體 104 外的額外構件及結構。例如，在例示實施例中，多媒體平台 100 包括比如硬碟或固態驅動機之長期資料貯存 170、通訊輸出 172、顯示器 174、及比如揚聲器之音頻裝置 176，各與 SOC 102 通訊或否則互動。

茲參照第 2 圖，如上所討論，記憶體 104 的受保護記憶體 112 係由記憶體控制器 114 實施。要這樣做，記憶體控制器 114 組態成建立硬體實施之受保護記憶體區域 200，其相關並界定 SOC 102 之受保護記憶體 112。硬體實施之受保護記憶體區域可包括任何數量的受保護記憶體區域或子區域。例如，在第 2 圖之例示實施例中，硬體實施之受保護記憶體區域包括其中儲存經鑑別之韌體的韌體受保護記憶體區域 202、其中儲存經解密的視頻之訊框緩衝器受保護記憶體區域 204、其中儲存經解密音頻的音頻受保護記憶體區域 206、壓縮視頻受保護記憶體區域 208、安全引擎至輸送流解多工（TSD）受保護記憶體區域 210、及/或一或更多個受保護記憶體區域 212。當然，在其他實施例中，取決於，例如，SOC 102 之預定的功能，硬體實施之受保護記憶體區域 200 可包括更少或更多數量的受保護記憶體區域。

受保護記憶體區域 202、204、206、208、210、212 的每一者取決於個別用途可包括類似或不同的安全屬性。記憶體控制器 114 將這種屬性確保到相應的暫存器中，使得屬性後續無法被變更。另外，記憶體控制器 114 可確保受保護記憶體區域 202、204、206、208、210、212 為適

當組態（如相應的記憶體位址沒有重疊）且，在一些實施例中，可對受保護記憶體 112 履行其他安全及錯誤檢查。

於使用期間，記憶體控制器 114 為受保護記憶體 112 提供硬體實施的保護。例如，硬體週邊 120 可與記憶體控制器 114 的記憶體介面 220 通訊來從記憶體 102 擷取資料。記憶體控制器 114 判定硬體週邊 120 是否正從受保護記憶體 112（如從受保護記憶體區域 200 之一）請求資料。若是，僅若請求的硬體週邊 120 已由安全引擎 110 事先鑑別過（此將於下討論），記憶體控制器 114 才允許對受保護記憶體 112 之相應的硬體實施之受保護記憶體區域 200 之存取（箭頭 230）。若否，記憶體控制器 114 拒絕請求的存取。或者，硬體週邊 120 可請求對未受保護記憶體 160 之存取（箭頭 232），其被記憶體控制器 114 所允許。

如上討論過，硬體實施之受保護記憶體區域 200 之建立及硬體週邊 120 之鑑別組態 SOC 102 內之受信賴資料路徑，其中媒體內容在其整個傳遞過程中受到保護。例如，於第 3 圖中顯示受信賴資料路徑 300 之一例示實施例。在第 3 圖的圖中，顯示受信賴資料路徑 300 為填滿箭頭，而未填滿箭頭指示未受保護資料路徑。另外，以雙括號顯示 SOC 102 之每一個經鑑別的硬體構件以指示該構件已由安全引擎 110 先鑑別過。

如第 3 圖中所示，主機軟體 302 可在多媒體平台 100 上執行。主機軟體 302 可請求經加密媒體內容 304 之傳遞

(如播放)。經加密媒體內容 304 可例如儲存在未受保護的記憶體 104 中。回應於傳遞請求，安全引擎 110 從記憶體 160 擷取經加密媒體內容 304。安全引擎 110 使用經加密應用鍵 162 將媒體內容解密成 A/V 流 306。如此，如後更詳細討論，安全引擎 110 確保應用鍵 162 在解密狀態中時（例如，安全引擎 110 將經解密應用鍵儲存於安全記憶體 154 中）永遠不會未受到保護。類似地，安全引擎 110 藉由將經解密的媒體流儲存在受保護記憶體區域 200 中來確保經解密的媒體內容之保護，該受保護記憶體區域僅可由經鑑別的硬體週邊 120 存取。

由解多工器 122 存取 A/V 流 306，該解多工器從 A/V 流 306 分離出音頻及視頻。另外，解多工器 122 可提供媒體內容之區段資料 320 至主機軟體。區段資料 320 之傳送如第 3 圖之未填滿箭頭所示係未受保護。由音頻 DSP 130 存取 A/V 流 306 之音頻 308，該音頻 DSP 產生經處理之音頻 310 給 A/V 輸出 134。另外，由音頻預解析器 124 存取 A/V 流 306 之壓縮視頻 312。音頻預解析器 124 可產生元資料 322，其以未受保護傳送中提供至主機軟體 302。由視頻解碼器 136 存取經預解析之壓縮視頻 314，該視頻解碼器產生視頻畫素 316。由 DPE 128 存取視頻畫素 316 以產生視頻畫素 318，其後續由視頻圖形 132 存取來在 A/V 輸出 134 產生無壓縮的視頻流。依此方式，於 SOC 102 中在整個受信賴資料路徑 300 中履行媒體內容之解密及解壓縮，使得在整個媒體內容的傳遞過程中保護對媒體

內容之存取。

茲參照第 4 圖，在使用時，SOC 102 可執行方法 400 來建立受保護記憶體區域 200。方法 400 以區塊 402 開始，其中可載入多媒體平台 100 之操作系統。於啟動程序期間，於區塊 404 中載入安全引擎 110 的驅動器。在區塊 406 中，SOC 102 判定 SOC 102 是否組態成使用受信賴資料路徑來傳遞媒體內容。若否，則方法 400 離開並且多媒體平台 100 如正常般啟動。然而，如果 SOC 102 組態成受信賴資料路徑傳遞，方法 400 進至區塊 408，其中安全引擎驅動器獲得有關於硬體實施之受保護記憶體區域 200 的資訊。這種資訊可包括，例如，每一個受保護記憶體區域 200 的位址範圍、每一個受保護記憶體區域 200 之區域類型、及與每一個受保護記憶體區域 200 關聯之任何額外的屬性。可從安全的資料表或之類獲得這類資訊。在區塊 410 中，安全引擎驅動器發送受保護記憶體區域資訊至安全引擎韌體 152 以進行驗證。安全引擎韌體 152 在區塊 414 中驗證受保護記憶體區域資訊。安全引擎韌體 152 可對受保護記憶體區域履行任何類型的驗證，包括例如確保受保護記憶體區域 200 之個別受保護記憶體範圍的位址範圍未彼此重疊；類型及屬性正確相應；及諸如此類。

在區塊 416 中，SOC 102 判定受保護記憶體區域 200 之組態是否被安全引擎 110 判定為有效。如果受保護記憶體區域 200 之組態並非有效，則方法 400 進至區塊 418，其中產生安全引擎驅動器錯誤。作為對此之回應，SOC

102 可履行一或更多個安全動作，包括例如重新啓動、重新組態記憶體控制器 114、及/或其他校正動作。然而，如果受保護記憶體區域 200 之組態被判定爲有效，則方法 400 進至區塊 420，其中安全引擎韌體 152 將尚未經過鑑別的所有硬體週邊 120 保持於重設模式中。

在記憶體控制器 114 已針對受保護記憶體區域 200 組態後，SOC 102 之安全引擎 110 可鑑別 SOC 102 的硬體週邊 120。要這樣做，SOC 102 可執行用於鑑別硬體週邊 120 之方法 500。方法 500 以區塊 502 開始，其中安全引擎 110 判定是否已接收到載入硬體週邊 120 的韌體 140 之請求。若是，安全引擎驅動器在區塊 504 中擷取請求硬體週邊 120 之密碼鍵 142 及關聯的經加密韌體 140。安全引擎驅動器產生包括週邊密碼鍵 142、經加密的週邊韌體 140、及關聯之韌體受保護記憶體區域 202 的記憶體位址之韌體載入包。

安全引擎驅動器在區塊 508 中發送韌體載入包到安全引擎韌體 152。回應此，安全引擎韌體 152 在區塊 510 中鑑別週邊密碼鍵 142。要這樣做，安全引擎韌體 152 可使用安全引擎 110 之安全鍵 150 來驗證之前已由安全引擎 110 簽署過週邊密碼鍵 142。

在區塊 512 中，SOC 102 判定安全引擎 110 是否成功鑑別週邊密碼鍵 142。若否，則方法 500 進至區塊 514，其中產生週邊驅動器載入錯誤，並將硬體週邊保持在重設模式中。另外，SOC 102 可採取對這種載入錯誤之額外的