

(51) International Patent Classification:  
*H04L 9/32* (2006.01) *H04L 9/14* (2006.01)**ER, Jesse** [US/US]; 10992 NW Appellate Way, Portland, Oregon 97229 (US).(21) International Application Number:  
PCT/US2011/044733(74) Agents: **VINCENT, Lester J.** et al.; Blakely Sokoloff Taylor & Zafman, 1279 Oakmead Parkway, Sunnyvale, California 940855 (US).(22) International Filing Date:  
20 July 2011 (20.07.2011)

(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, RO, RS, RU, 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.

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
61/367,726 26 July 2010 (26.07.2010) US  
12/913,708 27 October 2010 (27.10.2010) US(71) Applicant (for all designated States except US): **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, MS: RNB-4-150, Santa Clara, California 95052 (US).

(72) Inventors; and

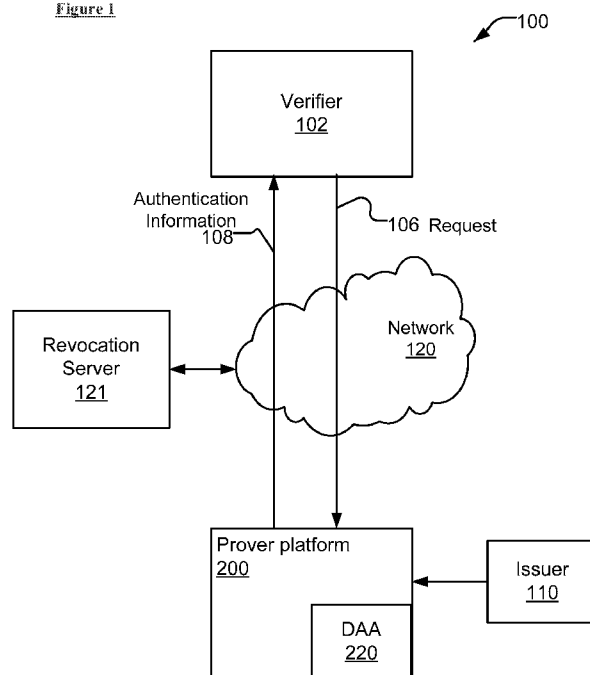
(75) Inventors/Applicants (for US only): **BRICKELL, Ernest F.** [US/US]; 2409 NE Jamie Drive, Hillsboro, Oregon 97124 (US). **LI, Jiangtao** [CN/US]; 12572 SW Sheldrake Way, Beaverton, Oregon 97007 (US). **WALK-**

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, 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,

[Continued on next page]

(54) Title: METHODS FOR ANONYMOUS AUTHENTICATION AND KEY AGREEMENT

Figure 1



(57) Abstract: Methods for anonymous authentication and key exchange are presented. In one embodiment, a method includes initiating a two-way mutual authentication between a device and a remote entity. The device remains anonymous to the remote entity after performing the authentication. The method also includes establishing a mutually shared session key for use in secure communication, wherein the initiating and the establishing are in conjunction with direct anonymous attestation (DAA).



---

SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG). **Published:**

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

## **METHODS FOR ANONYMOUS AUTHENTICATION AND KEY AGREEMENT**

### **FIELD OF THE INVENTION**

Embodiments of the invention relate to the field of cryptography, more  
5 particularly, relate to direct anonymous attestation.

### **BACKGROUND OF THE INVENTION**

The objective of direct anonymous attestation (DAA) is to enable a party to prove  
that the party is a member in good standing in a group without revealing information about  
10 its identity. In the DAA scheme, there are three types of entities: an issuer, a prover, and  
verifiers.

An issuer is an entity that issues a unique DAA private key to each member of the  
group. A verifier is an entity which is trying to establish whether the platform is a member  
of the group. A platform is an entity which is trying to prove membership in the group. If  
15 the platform is indeed a member in the group in good standing (i.e., the platform owns a  
valid DAA private key and the private key has not been revoked), the authentication  
process will be successful.

For each DAA group, there is a group public key and a group issuing private key  
(master key). The group issuing private key is used for generating a unique private key for  
20 each group member. The issuing private key is kept securely by the issuer. Each platform  
uses its DAA private key to digitally sign a message. The resulting signature is referred to  
as a DAA signature. The verifier uses the group public key to verify the correctness of a  
DAA signature, i.e., to verify that the signature was indeed created by a platform with a  
valid DAA private key. The DAA signature however does not reveal any information  
25 about which unique private key was used to create the DAA signature. The DAA scheme  
includes methods to handle revocation, such as, for example, a private-key based  
revocation and a signature based revocation. DAA scheme does not include generating  
mutual shared session keys.

The SIGMA (SIGN-and-MAC Approach) protocol is a Diffie-Hellman based key  
30 exchange protocol using digital signatures. The protocol is used by the Internet Key  
Exchange (IKE) standards and IPsec standards.

### **BRIEF DESCRIPTION OF THE DRAWINGS**

Embodiments of the present invention will be understood more fully from the detailed description given below and from the accompanying drawings of various embodiments of the invention, which, however, should not be taken to limit the invention to the specific embodiments, but are for explanation and understanding only.

5        **Figure 1** is a system featuring a platform implemented with a DAA module in accordance with one embodiment of the invention.

**Figure 2** shows an embodiment of the platform including the DAA module with respect to Figure 1.

10       **Figure 3** shows a flow diagram of one embodiment of a process to perform authentication and to establish a shared key.

**Figure 4** shows a flow diagram of one embodiment of a process for signature based revocation.

**Figure 5** shows a flow diagram of one embodiment of a process to perform bilateral anonymous authentication.

15       **Figure 6** illustrates a computer system for use with one embodiment of the present invention.

**Figure 7** illustrates a point-to-point computer system for use with one embodiment of the invention.

## 20       **DETAILED DESCRIPTION OF THE INVENTION**

      Methods for anonymous authentication and key exchange are presented. In one embodiment, a method includes initiating a two-way mutual authentication between a device and a remote entity. The device remains anonymous to the remote entity after performing the authentication. The method also includes establishing a mutually shared session key for use in secure communication, wherein the initiating and the establishing are in conjunction with direct anonymous attestation (DAA).

25       In the following description, numerous details are set forth to provide a more thorough explanation of embodiments of the present invention. It will be apparent, however, to one skilled in the art, that embodiments of the present invention may be practiced without these specific details. In other instances, well-known structures and devices are shown in block diagram form, rather than in detail, in order to avoid obscuring embodiments of the present invention.

      Some portions of the detailed descriptions which follow are presented in terms of

algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussion, it is appreciated that throughout the description, discussions utilizing terms such as "processing" or "computing" or "calculating" or "determining" or "displaying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

In the following description, certain terminology is used to describe certain features of one or more embodiments of the invention. For instance, "platform" is defined as any type of communication device that is adapted to transmit and receive information. Examples of various platforms include, but are not limited or restricted to computers, personal digital assistants, cellular telephones, set-top boxes, facsimile machines, printers, modems, routers, smart cards or other like form factor device including an integrated circuit, or other like device such as a bank card, credit card, identification card and the like including logic to perform enhanced revocation according to any one of the described embodiments. A "communication link" is broadly defined as one or more information-carrying mediums adapted to a platform. Examples of various types of communication links include, but are not limited or restricted to electrical wire(s), optical fiber(s), cable(s), bus trace(s), or wireless signaling technology.

Embodiments of present invention also relate to apparatuses for performing the

operations herein. Some apparatuses may be specially constructed for the required purposes, or it may comprise a general purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program may be stored in a computer readable storage medium, such as, but not limited to, any type of disk including floppy disks, optical disks, CD-ROMs, DVD-ROMs, and magnetic-optical disks, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, NVRAMs, magnetic or optical cards, or any type of media suitable for storing electronic instructions, and each coupled to a computer system bus.

The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various general purpose systems may be used with programs in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatus to perform the required method steps. The required structure for a variety of these systems will appear from the description below. In addition, embodiments of the present invention are not described with reference to any particular programming language. It will be appreciated that a variety of programming languages may be used to implement the teachings of the invention as described herein.

A machine-readable medium includes any mechanism for storing or transmitting information in a form readable by a machine (e.g., a computer). For example, a machine-readable medium includes read only memory ("ROM"); random access memory ("RAM"); magnetic disk storage media; optical storage media; flash memory devices; etc.

The method and apparatus described herein are for anonymous authentication and a key exchange. Specifically, the method and apparatus described herein are primarily discussed in reference to multi-core processor computer systems. However, the methods and apparatus for anonymous authentication and a key exchange are not so limited, as they may be implemented on or in association with any integrated circuit device or system, such as cell phones, personal digital assistants, embedded controllers, mobile platforms, desktop platforms, and server platforms, as well as in conjunction with other resources.

### Overview

Methods for anonymous authentication and key exchange are presented. In one embodiment, a method includes initiating a two-way mutual authentication between a device and a remote entity. The device remains anonymous to the remote entity after performing the authentication. The method also includes establishing a mutually shared

session key for use in secure communication, wherein the initiating and the establishing are in conjunction with direct anonymous attestation (DAA).

In one embodiment, a “verifier” is an entity (e.g., person, platform, system, and/or device) that requests some verification of authenticity or authority from another entity.

5 Normally, this is performed prior to disclosing or providing the requested information. A “prover” is an entity that is requested to provide some proof of its authority, validity, and/or identity. An “issuer” organizes or manages a trusted membership group and engages with hardware devices to join the trusted membership group. A “device manufacturer,” which may be used interchangeably with “certifying manufacturer,” is any  
10 entity that manufactures or configures a platform or a device (e.g., a Trusted Platform Module). An issuer may be a device/certifying manufacturer.

Figure 1 is a system featuring a platform implemented with a DAA module in accordance with one embodiment of the invention. Many related components such as buses and peripherals have not been shown to avoid obscuring the invention. Referring to  
15 Figure 1, the system includes verifier 102, prover platform 200, DAA 220, issuer 110, revocation server 121, and network 120. In one embodiment, verifier 102 receives request 106 from prover platform 200 and sends authentication information 108 to prover platform 200.

In one embodiment, a trusted platform module is a trusted hardware device. DAA  
20 220 is a part of the trusted platform module (TPM). In another embodiment, DAA 220 is a module independent from the TPM. Verifier 102 (e. g., a first platform) transmits authentication request 106 to prover platform 200 (e.g., a second platform) via network 120. In response to request 106, prover platform 200 provides authentication information 108. In one embodiment, network 120 forms part of a local or wide area network, a  
25 conventional network infrastructure, or any combinations thereof, such as a company’s Intranet, the Internet, or other like network.

In one embodiment, for heightened security, verifier 102 verifies whether that prover platform 200 is manufactured by a selected device manufacturer or a selected group of device manufacturers (hereinafter referred to as “device manufacturers”). In one  
30 embodiment, verifier 102 challenges prover platform 200 to show that prover platform 200 has cryptographic information (e.g., a private member key) generated by issuer 110. Prover platform 200 replies to the challenge by providing authentication information 108, in the form of a reply, to convince verifier platform 102 that prover platform 200 has

cryptographic information generated by issuer 110, without revealing the cryptographic information or any unique, device/platform identification information also referred to herein as “unique, device identification information” to enable a trusted member device to remain anonymous to the verifier.

5           In one embodiment, functionality of DAA 220, which is configured to prove to verifier 102 that information (e.g., cryptographic key, digital signature, digital certificate, etc.) from DAA 220 is uncompromised, is deployed as firmware. However, it is contemplated that such functionality may be deployed as dedicated hardware, software, or the combination thereof. Instructions or code forming the firmware or software are stored  
10   on a machine-readable medium. As described herein, DAA is a scheme that enables remote authentication of DAA 220, while preserving the privacy of the user of the platform that contains DAA 220.

          Figure 2 shows an embodiment of the platform including a DAA module with respect to Figure 1. Many related components such as buses and peripherals have not been  
15   shown to avoid obscuring the invention. Referring to Figure 2, the platform includes CPU 202, PCH (platform controller hub) 210, DAA 220, memory 212, Hard disk (HDD) 214, graphic engines 218, flash memory 280, I/O device 216-1, and one or more I/O devices 216-N. In one embodiment, flash memory 280 stores cryptographic information 230.

          In one embodiment, platform 200 includes DAA 220 to convince a verifier that  
20   platform 200 possesses uncompromised cryptographic information without disclosure of the cryptographic information or any unique device identification information. In one embodiment, DAA 220 includes a unique group membership certificate and a private member key to provide a private signature. In one embodiment, DAA 220 in combination with platform 200 generates authentication information using private unique signature key  
25   230 to prove to a verifier that platform 200 is a member of a trusted membership group defined by an issuer (e.g., device manufacturer), without disclosure of any unique device identification information including the private signature key. This enables trusted platform 200 to remain anonymous to a verifier. As described herein, cryptographic information 230 may be alternatively referred to as a private member key/private signature  
30   key. Representatively, computer system 200 comprises link 204 for communicating information between processor (CPU) 202 and PCH 210. As described herein, PCH 210 or chipset describe the various devices coupled to CPU 202 to perform desired system functionality.



In one embodiment, graphic engines 218, HDD 214, and main memory 212 are coupled to PCH 210. In one embodiment, PCH 210 is configured to include a memory controller, an input/output (I/O) controller, or both to communicate with I/O devices 216 (216-1, ..., 216-N). In one embodiment, PCH 210 is configured to incorporate graphics engines 218 and operates as a graphics memory controller hub (GMCH). In one embodiment, main memory 212 includes, but is not limited to, random access memory (RAM), dynamic RAM (DRAM), static RAM (SRAM), synchronous DRAM (SDRAM), double data rate (DDR) SDRAM (DDR-SDRAM), Rambus DRAM (RDRAM), or any device capable of supporting high-speed buffering of data.

#### DAA-SIGMA Protocol

Figure 3 shows a flow diagram of one embodiment of a process to perform authentication and to establish a shared key. The process is performed by processing logic that may comprise hardware (circuitry, dedicated logic, etc.), software (such as one that is run on a general purpose computer system or a dedicated machine), or a combination of both. In one embodiment, the process is performed in conjunction with a system (e.g., the system with respect to Figure 1). In one embodiment, the process is performed by platform 301 and server 303.

In one embodiment, the notations in Table 1 are used to describe Figures 3-5. In one embodiment, as described below, bsn and SIG-RL are optional inputs.

$(M)_k$ : This denotes an encryption of message M using key k (in conjunction with key k).

$[M]_k$ : This denotes a message M concatenated with a Message Authentication Code (MAC) of message M. The MAC is computed using key k (in conjunction with key k).

$\text{Sign}_A(M)$ : This denotes a digital signature of M computed in conjunction with the entity A's private key.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>DAA-Sign<sub>A</sub>(M, bsn, SIG-RL): This denotes a DAA signature of message M computed using the entity A's DAA private key, where bsn is the verifier's basename and SIG-RL is the signature based revocation list. Both bsn and SIG-RL are optional inputs.</p> <p>Cert<sub>s</sub>: This denotes a server's certificate.</p> <p>Cert<sub>p</sub>: This denotes a platform's DAA group certificate with which DAA group public key is derivable. A public key certification of P issued by a certificate authority (CA) to certify the group public key (gpk)</p> <p>a  b: denotes a string concatenation operation involving "a" and "b", or more generically a result by combining "a" and "b"</p> <p>PRF(g<sup>ab</sup>): denotes generating a value using a pseudo-random function in conjunction with g<sup>ab</sup>.</p> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Table 1 Notations

In one embodiment, a DAA-SIGMA protocol is performed between a platform (e.g., platform 301) and server (e.g., server 303). Platform 301 owns a unique DAA private key and an associated DAA group certificate. Server 303 has a public-private key pair and a certificate. This protocol is performed in conjunction with a Diffie-Hellman (DH) based protocol with signature and MAC for authentication. The objective of performing the process is for mutual authentication between platform 301 and server 303 and to establish a shared key between both parties. In one embodiment, platform 301 authenticates to server 303 anonymously.

10 In one embodiment, the process begins by platform 301 sending message 1 to server 303 (process block 311).

In one embodiment, platform 301 chooses a random value "a" as the ephemeral DH private key. The platform computes g<sup>a</sup> as the ephemeral DH public key. The platform sends g<sup>a</sup> to the server in message 1.

15 In one embodiment, server 303 prepares sending Message 2 to platform 301

(process block 312).

In one embodiment, server 303 chooses a random value “b” as its ephemeral DH private key. Server 303 computes  $g^b$  as its ephemeral DH public key. Server 303 computes  $g^{ab} = (g^a)^b$ . Server 303 securely erases b. Server 303 computes  $SK \parallel MK = \text{PRF}(g^{ab})$ , where  
 5 PRF is a pseudo-random function. SK is a session key and MK is a MAC key. Server 303 computes a MAC of (based on)  $bsn_s$  and  $Cert_s$  using MK as a key. In one embodiment,  $bsn_s$  is either the basename of server 303 or a special symbol “ $\perp$ ”. In one embodiment, server 303 signs  $(g^b, g^a)$  using its private key (a signing key) and generates  $\text{Sign}_s(g^b \parallel g^a)$ . Accordingly, server 303 sends Message 2 comprising:  $g^b$ ,  $[bsn_s, Cert_s]_{MK}$ , and  $\text{Sign}_s(g^b \parallel g^a)$   
 10 to platform 301.

In one embodiment, platform 301, in response to receiving Message 2, verifies Message 2.

In one embodiment, platform 301 computes  $g^{ab} = (g^b)^a$ . Platform 301 securely erases “a”. Platform 301 computes  $SK \parallel MK = \text{PRF}(g^{ab})$ . Platform 301 verifies server  
 15 303’s public key certificate  $Cert_s$ . Platform 301 verifies the MAC of  $bsn_s$  and  $Cert_s$  by using MK (i.e., the MAC key). Platform 301 verifies the signature of  $(g^b, g^a)$  by using server 303’s public key which is retrievable from  $Cert_s$ . In one embodiment, if any of the above MAC verification, certificate verification, or signature verification fails, platform 301 aborts the protocol.

20 In one embodiment, platform 301 prepares sending Message 3 to server 303 (process block 313).

In one embodiment, platform 301 computes a MAC of its DAA group certificate using MK and produces  $[g^a, Cert_p]_{MK}$ . Platform 301 uses its DAA private key and  $bsn_s$  (optional) to sign  $(g^a \parallel g^b)$  and produces  $\text{DAA-Sign}_p(g^a \parallel g^b, bsn_s)$ . Accordingly, platform  
 25 301 sends  $[g^a, Cert_p]_{MK}$  and  $\text{DAA-Sign}_p(g^a \parallel g^b, bsn_s)$  in Message 3 to server 303.

In one embodiment, server 303, in response to receiving the Message 3, verifies Message 3.

In one embodiment, server 303 verifies  $[g^a, Cert_p]_{MK}$  using MK (the MAC key). Server 303 verifies the DAA group certificate  $[g^a, Cert_p]$ . Server 303 verifies the DAA  
 30 signature of  $(g^a, g^b)$  using the DAA public key (derived from  $Cert_p$ ) and the basename  $bsn_s$ . In one embodiment, if  $bsn_s$  is used in the protocol, the authentication is anonymous but linkable authentication. If  $bsn_s$  is not used, the authentication is an anonymous authentication.

In one embodiment, two options are available for generating a DAA signature, such as, for example, a random based option and a name-based option. In random based option (i.e., the basename is a special symbol “ $\perp$ ”), the DAA signature is anonymous and non-linkable. In name based option, a verifier sends its basename to platform 301, and  
5 platform 301 creates a DAA signature based in part on the basename of the verifier.

In one embodiment, platform 301 and server 303 have established a shared session key SK. Both parties are able to use SK for secure and authenticated communication between them.

In one embodiment, platform 301 has been provisioned with a unique Direct  
10 Anonymous Attestation (DAA) key. In one embodiment, for example, DAA is implemented in conjunction with Intel <sup>®</sup> Enhanced Privacy ID (EPID).

In one embodiment, platform 301 is to mutually authenticate with a service provider and to establish a session key for future secure communication. The service provider authenticates to platform 301 using traditional PKI certificate, whereas platform  
15 301 authenticates (itself) to the service provider anonymously using DAA-SIGMA. In one embodiment, platform 301 anonymously authenticates to a verifier in a secure handshake protocol and derives a shared session key for future secure communication.

In one embodiment, the process begins by initiating a two-way mutual authentication between a device and a remote entity. The device remains anonymous to  
20 the remote entity after performing the authentication. The parties establish a mutually shared session key for use in secure communication. The initiating and the establishing are in conjunction with direct anonymous attestation (DAA).

#### Platform Role

25 In one embodiment, processing logic (e.g., platform 301) selects a random value (e.g., DH private key) and sends a first message comprising at least a key-exchange-protocol public key (e.g., DH public key) computed based on the random value. Processing logic computes, in response to receiving a second message, a shared value (e.g.,  $g^a$ ,  $g^b$ ) based on the random value and a key-exchange-protocol public key associated  
30 with the remote entity. Processing logic generates a session key and a message authentication code (MAC) key based at least on the shared value (e.g.,  $g^{ab}$ ). Processing logic verifies, using the MAC key (e.g., MK), a public key certificate associated with a remote entity. Processing logic authenticates a digital signature from the second message

based on combined public keys ( $g^a || g^b$ ) retrievable from the digital signature. The digital signature is associated with the remote entity and is retrievable using a public key from the public key certificate. Processing logic generates, using the MAC key, a MAC (e.g.,  $[Cert_P]_{MK}$ ) based on a DAA-based group certificate. Processing logic generates, using a  
 5 DAA-based private key, a DAA-based signature based on the combined public keys. Processing logic sends a third message comprising at least the DAA-based signature and the MAC.

In one embodiment, processing logic detects whether there is a failure during MAC verification, signature verification, or certificate verification. Processing logic aborts the  
 10 authentication if a failure is detected.

#### Verifier Role

In one embodiment, processing logic (e.g., server 303, a remote entity) receives a first message from a device with a request to perform mutual anonymous authentication.  
 15 In one embodiment, processing logic computes, based on a random value (e.g., “b”), a DH public key (e.g.,  $g^b$ ) associated with the remote entity. Processing logic computes a shared value (e.g.,  $g^{ab}$  or  $g^a, g^b$ ) based on the random number and a DH public key associated with the device (the DH public key is retrievable from the first message). Processing logic securely erases the random value. Processing logic generates a session  
 20 key and a message authentication code (MAC) key based at least on the shared value (e.g.,  $g^a, g^b$ ). Processing logic generates, using the MAC key, a MAC (e.g.,  $[bsn_s, Cert_s]_{MK}$ ) on a public key certificate associated with the remote entity. Processing logic generates, using a remote entity private key, a digital signature (e.g.,  $Sign_s(g^b || g^a)$  based at least on combined public keys. The combined public keys include, for example, the DH public key  
 25 associated with the remote entity and the DH public key associated with the device. Processing logic sends a second message comprising at least the digital signature and the MAC. Processing logic then receives a third message from the device. Processing logic verifies, using the MAC key, a DAA-based public key (e.g.,  $[Cert_P]$ ) retrievable from the third message. Processing logic verifies at least, using the DAA-based public key, a DAA-  
 30 based signature (e.g.,  $DAA-Sign_P(g^a || g^b, bsn_s)$ ) in the third message.

#### DAA-SIGMA Protocol with Signature Based Revocation

Figure 4 shows a flow diagram of one embodiment of a process for signature based

revocation. The process is performed by processing logic that may comprise hardware (circuitry, dedicated logic, etc.), software (such as one that is run on a general purpose computer system or a dedicated machine), or a combination of both. In one embodiment, the process is performed in conjunction with a system (e.g., the system with respect to  
 5 Figure 1). In one embodiment, the process is performed by platform 401 and server 403.

In one embodiment, in signature based revocation, an issuer revokes a platform based on the signature generated by the platform. This revocation method is used when a key becomes subject to revocation criteria but has not been exposed yet. In one embodiment, an issuer is able to revoke a platform by revoking the platform's signatures. The method is  
 10 also known as signature based revocation. In such revocation, platform 401 needs to refer to (e.g., read) a revocation list (referred to herein as SIG-RL). Platform 401 produces a "non-revoked proof" along with the DAA signature. Server 403 reviews and determines whether or not to accept the "non-revoked proof". In one embodiment, for signature based revocation, both the platform and the verifier perform some computations to enable the  
 15 verifier to perform its responsibility of checking whether the platform has been revoked according to SIG-RL.

In one embodiment, multiple DAA groups are present. Each DAA group is associated with a unique group ID and a group certificate.

In one embodiment, the process begins by platform 401 sending message 1 to  
 20 server 403 (process block 411).

In one embodiment, platform 401 performs a protocol substantially similar to process block 311 with respect to Figure 3. In addition to public key  $g^a$ , platform 401 includes DAA group ID "GID" in message 1 and sends message 1 to server 403. GID is used by a verifier to identify to which DAA group a platform belongs.

25 In one embodiment, server 403, in response to receiving the message 1, prepares to send message 2 (process block 412).

Server 403 obtains SIG-RL corresponding with GID. Server 403 computes a MAC (e.g.,  $[SIG-RL, bsns, Certs]_{MK}$ ) based on SIG-RL,  $bsns$ , and  $Certs$  using MK (the MAC key). In one embodiment, server 403 performs a protocol substantially similar to process  
 30 block 312 with respect to Figure 3. Accordingly, server 403 sends  $g^b$ ,  $[SIG-RL, bsns, Certs]_{MK}$ , and  $Signs(g^b || g^a)$  to platform 401.

In one embodiment, platform 401 prepares to send message 3 to server 403 (process block 413).

In one embodiment, platform 401 generates (based on current DAA private key, SIG-RL, and  $bsn_S$ ) a DAA signature (e.g.,  $DAA-Sign_P(g^a || g^b, bsn_S, SIG-RL)$ ). In one embodiment, non-revoked proof is embedded in the DAA signature. Accordingly, platform 401 sends  $[g^a, Cert_P]_{MK}$  and  $DAA-Sign_P(g^a || g^b, bsn_S, SIG-RL)$  to server 403.

5 In one embodiment, server 403, in response to receiving message 3, verifies message 3. In one embodiment, server 403 verifies the DAA signature including the revocation check using SIG-RL.

In one embodiment, there are two operations performed to prove a membership in a membership scheme: (1) Sign and (2) Verify.

10 With respect to (1) sign process: a platform generates a DAA signature on a message using its private key, the verifier's basename, and the SIG-RL (if provided). The SIG-RL is given as input if the platform needs to conduct "zero-knowledge" proofs to prove that the platform has not been revoked on the SIG-RL. The outputs of "non-revoked" proofs are part of the DAA signature.

15 With respect to the (2) verify process: a verifier verifies the correctness of a DAA signature using the group public key. The verifier also verifies that the creator of the DAA signature has not been revoked in PRIV-RL and SIG-RL.

In one embodiment, to control the size of the revocation lists (PRIV-RL or SIG-RL), an issuer creates multiple DAA groups. For example, suppose there are 10 million  
20 platforms. An issuer creates 100 DAA groups and each group has 100,000 group members. To issue a DAA private key for a platform, an issuer first chooses a DAA group for the platform, and then generates an DAA private key in that group. To conduct proof of membership, a platform needs to first reveal which DAA group the platform belongs to, and then proves that the platform is a valid member of that group.

25 In one embodiment, in private-key based revocation, an issuer revokes a platform based on the platform's private key. This revocation method is used when a platform's private key becomes exposed and subject to revocation criteria. PRIV-RL denotes the revocation list corresponding to the private-key based method. For private-key based revocation, a platform does not need to perform any action and it is the verifier's  
30 responsibility to check whether the platform has been revoked in PRIV-RL.

#### DAA-SIGMA Protocol with Bilateral Anonymous Authentication

Figure 5 shows a flow diagram of one embodiment of a process to perform

bilateral anonymous authentication. The process is performed by processing logic that may comprise hardware (circuitry, dedicated logic, etc.), software (such as one that is run on a general purpose computer system or a dedicated machine), or a combination of both. In one embodiment, the process is performed in conjunction with a system (e.g., the system with respect to Figure 1). In one embodiment, the process is performed in conjunction with platform A 501 and platform B 503. In one embodiment, the process is performed by a computer system with respect to Figure 7. In one embodiment, platform A 501 and platform B 503 are within a same platform, for example, as a processing core and a chipset.

In one embodiment, the process supports two-way anonymous authentication (bilaterally). Two platforms authenticate to each other anonymously and set up a secure channel by using a mutually shared session key generated during process. In one embodiment, platform B 503 is a remote entity or a second hardware platform.

In one embodiment, the process begins by platform 501 sending message 1 to platform B 503 (process block 511).

In one embodiment, platform A 501 chooses a random value “a” as its ephemeral DH private key. Platform A 501 computes an ephemeral DH public key (e.g.,  $g^a$ ). Platform A 501 sends  $bsn_A$  and  $g^a$  to platform B 503. In one embodiment,  $bsn_A$  is either the basename of the platform A 501 or a symbol “ $\perp$ ”.

In one embodiment, platform B 503 sends message 2 to platform 503 (process block 512).

In one embodiment, platform B 503 chooses a random value “b” as its ephemeral DH private key. Platform B 503 computes  $g^b$  as its ephemeral DH public key. Platform B 503 computes  $g^{ab} = (g^a)^b$  and securely erases b. Platform B 503 computes  $SK \parallel MK = PRF(g^{ab})$ . SK is the session key and MK is the MAC key. Platform B 503 computes a MAC based on  $g^b$ ,  $bsn_B$ , and  $Cert_B$  by using MK. In one embodiment,  $bsn_B$  is either the basename of platform B 503 or a symbol “ $\perp$ ”.  $Cert_B$  is platform B 503’s DAA group certificate. Platform B 503 signs  $(g^b, g^a)$  in conjunction with its DAA private key and  $bsn_A$  and produces  $DAA-Sign_B(g^b \parallel g^a, bsn_A)$ . Accordingly, platform B 503 sends  $g^b$ ,  $[g^b, bsn_B, Cert_B]_{MK}$ , and  $DAA-Sign_B(g^b \parallel g^a, bsn_A)$  to platform A 501.

In one embodiment, platform 501, in response to receiving the message 2, verifies message 2.

In one embodiment, platform A 501 computes  $g^{ab} = (g^b)^a$  and securely erases “a”.



Platform A 501 computes  $SK \parallel MK = \text{PRF}(g^{ab})$ . Platform A 501 verifies the platform B 503's group certificate  $\text{Cert}_B$ . Platform A 501 verifies the MAC (e.g.,  $[g^b, \text{bsn}_B, \text{Cert}_B]_{MK}$ ) of  $\text{bsn}_B$  and  $\text{Cert}_B$  by using the MAC key (i.e.,  $MK$ ). Platform A 501 verifies the DAA-Sign<sub>P</sub>( $g^a \parallel g^b, \text{bsn}_A$ ) using the group public key (retrievable in  $\text{Cert}_B$ ) and basename  $\text{bsn}_A$ .

5 In one embodiment, platform A 501 prepares to send message 3 to platform B 503 (process block 513).

In one embodiment, platform A 501 computes a MAC of its DAA group certificate using  $MK$ . Platform A 501 produces  $[g^a, \text{Cert}_A]_{MK}$ . Platform A 501 uses its DAA private key and  $\text{bsn}_B$  to sign ( $g^a, g^b$ ) and produces  $\text{DAA-Sign}_A(g^a \parallel g^b, \text{bsn}_B)$ . Accordingly, platform  
10 A 501 sends  $[g^a, \text{Cert}_A]_{MK}$ ,  $\text{DAA-Sign}_A(g^a \parallel g^b, \text{bsn}_B)$  to platform B 503.

In one embodiment, platform B 503, in response to receiving the message 3, verifies message 3.

In one embodiment, platform B 503 verifies  $[g^a, \text{Cert}_A]_{MK}$  using the MAC key,  $MK$ . Platform B 503 verifies the DAA group certificate  $\text{Cert}_A$ . Platform B 503 verifies the  
15 DAA signature of ( $g^a, g^b$ ) using the DAA public key in  $\text{Cert}_A$  and the basename  $\text{bsn}_B$ .

Embodiments of the invention may be implemented in a variety of electronic devices and logic circuits. Furthermore, devices or circuits that include embodiments of the invention may be included within a variety of computer systems. Embodiments of the invention may also be included in other computer system topologies and architectures.

20 Figure 6, for example, illustrates a computer system in conjunction with one embodiment of the invention. Processor 705 accesses data from level 1 (L1) cache memory 706, level 2 (L2) cache memory 710, and main memory 715. In other embodiments of the invention, cache memory 706 may be a multi-level cache memory comprise of an L1 cache together with other memory such as an L2 cache within a  
25 computer system memory hierarchy and cache memory 710 are the subsequent lower level cache memory such as an L3 cache or more multi-level cache. Furthermore, in other embodiments, the computer system may have cache memory 710 as a shared cache for more than one processor core.

Processor 705 may have any number of processing cores. Other embodiments of  
30 the invention, however, may be implemented within other devices within the system or distributed throughout the system in hardware, software, or some combination thereof.

Main memory 715 may be implemented in various memory sources, such as dynamic random-access memory (DRAM), hard disk drive (HDD) 720, solid state disk

725 based on NVRAM technology, or a memory source located remotely from the computer system via network interface 730 or via wireless interface 740 containing various storage devices and technologies. The cache memory may be located either within the processor or in close proximity to the processor, such as on the processor's local bus  
5 707. Furthermore, the cache memory may contain relatively fast memory cells, such as a six-transistor (6T) cell, or other memory cell of approximately equal or faster access speed.

Other embodiments of the invention, however, may exist in other circuits, logic units, or devices within the system of Figure 6. Furthermore, other embodiments of the  
10 invention may be distributed throughout several circuits, logic units, or devices illustrated in Figure 6.

Similarly, at least one embodiment may be implemented within a point-to-point computer system. Figure 7, for example, illustrates a computer system that is arranged in a point-to-point (PtP) configuration. In particular, Figure 7 shows a system where  
15 processors, memory, and input/output devices are interconnected by a number of point-to-point interfaces.

The system of Figure 7 may also include several processors, of which only two, processors 870, 880 are shown for clarity. Processors 870, 880 may each include a local memory controller hub (MCH) 811, 821 to connect with memory 850, 851. Processors  
20 870, 880 may exchange data via a point-to-point (PtP) interface 853 using PtP interface circuits 812, 822. Processors 870, 880 may each exchange data with a chipset 890 via individual PtP interfaces 830, 831 using point to point interface circuits 813, 823, 860, 861. Chipset 890 may also exchange data with a high-performance graphics circuit 852 via a high-performance graphics interface 862. Embodiments of the invention may be coupled  
25 to computer bus (834 or 835), or within chipset 890, or coupled to data storage 875, or coupled to memory 850 of Figure 7.

Other embodiments of the invention, however, may exist in other circuits, logic units, or devices within the system of Figure 7. Furthermore, other embodiments of the invention may be distributed throughout several circuits, logic units, or devices illustrated  
30 in Figure 7.

The invention is not limited to the embodiments described, but can be practiced with modification and alteration within the spirit and scope of the appended claims. For example, it should be appreciated that the present invention is applicable for use with all

types of semiconductor integrated circuit ("IC") chips. Examples of these IC chips include but are not limited to processors, controllers, chipset components, programmable logic arrays (PLA), memory chips, network chips, or the like. Moreover, it should be appreciated that exemplary sizes/models/values/ranges may have been given, although  
5   embodiments of the present invention are not limited to the same. As manufacturing techniques (e.g., photolithography) mature over time, it is expected that devices of smaller size could be manufactured.

Whereas many alterations and modifications of the embodiment of the present invention will no doubt become apparent to a person of ordinary skill in the art after  
10   having read the foregoing description, it is to be understood that any particular embodiment shown and described by way of illustration is in no way intended to be considered limiting. Therefore, references to details of various embodiments are not intended to limit the scope of the claims which in themselves recite only those features regarded as essential to the invention.

15

**CLAIMS**

What is claimed is:

- 5     1. A method comprising:  
initiating a two-way mutual authentication between a first device and a remote  
entity, wherein the first device remains anonymous to the remote entity  
after performing the authentication; and  
establishing a mutually shared session key for use in secure communication,  
10     wherein the initiating and the establishing are in conjunction with direct  
anonymous attestation (DAA).
2. The method of claim 1, further comprising:  
selecting a first random value; and  
15     sending a first message comprising at least a key-exchange-protocol public key  
computed based on the first random value.
3. The method of claim 2, further comprising:  
computing, in response to receiving a second message, a shared value based on the  
20     first random value and a second key-exchange-protocol public key  
associated with the remote entity;  
generating a session key and a message authentication code (MAC) key based at  
least on the shared value;  
verifying, by using the MAC key, a first public key certificate associated with the  
25     remote entity; and  
authenticating a first digital signature from the second message based on combined  
public keys retrievable from the first digital signature, wherein the first  
digital signature is associated with the remote entity and is retrievable by  
using a public key from the first public key certificate.  
30
4. The method of claim 3, further comprising:  
generating, by using the MAC key, a MAC based at least on a DAA-based group  
certificate;

generating, by using a DAA-based private key, a DAA-based signature based on  
the combined public keys; and  
sending a third message comprising at least the DAA-based signature and the  
MAC.

5

5. The method of claim 4, wherein the second message further includes a basename associated with the remote entity and the DAA-based signature is generated further based on the basename, wherein the basename is a random based signature such that the remote entity remains anonymous and non-linkable.

10

6. The method of claim 4, further comprising:  
detecting whether there is a failure during MAC verification, signature verification,  
or certificate verification; and  
aborting the authentication if a failure is detected.

15

7. The method of claim 4, wherein the remote entity is a server acting as a verifier, wherein the first message further includes a group ID (GID), wherein the DAA-based signature in the third message is generated further based on a signature-based revocation list and includes non-revoked proof.

20

8. The method of claim 4, wherein the remote entity is a second device, wherein the first message further includes a basename associated with the first device, wherein the first digital signature is a DAA-based signature generated by using a DAA-based private key associated with the second device.

25

9. The method of claim 4, wherein the first random value is an ephemeral Diffie-Hellman (DH) private key associated with the first device, wherein the key-exchange-protocol public key is a DH public key, wherein the session key and the MAC key are generated using a pseudo-random function.

30

10. A method comprising:  
receiving, by a remote entity, a first message from a first device with a request to  
perform bilateral mutual anonymous authentication; and

establishing a shared key for use in secure communication, wherein the receiving and the establishing are performed in conjunction with direct anonymous attestation (DAA).

5 11. The method of claim 10, further comprising:

computing, based on a random value, a DH public key associated with the remote entity;

computing a shared value based on the random number and a DH public key associated with the first device retrievable from the first message;

10 secure erasing, the random value;

generating a session key and a message authentication code (MAC) key based at least on the shared value;

generating, by using the MAC key, a MAC based on a public key certificate associated with the remote entity;

15 generating, by using a remote entity private key, a first digital signature based at least on combined public keys, wherein the combined public keys include the DH public key associated with the remote entity and the DH public key associated with the first device; and

20 sending a second message comprising at least the first digital signature and the MAC.

12. The method of claim 11, further comprising:

receiving a third message from the first device;

25 verifying, by using the MAC key, a DAA-based public key retrievable from the third message; and

verifying at least, by using the DAA-based public key, a DAA-based signature from the third message.

13. The method of claim 12, wherein the remote entity is a server acting as a verifier, wherein the first message further includes a group ID (GID), wherein the MAC in the second message is generated further based on a signature-based revocation list, wherein the DAA-based signature in the third message further includes non-revoked proof, further comprising determining whether or not the first device is revoked from a trusted

30

membership based at least on the revocation list and the non-revoked proof.

14. The method of claim 12, wherein the remote entity is a second device, wherein the first message further includes a basename associated with the first device, wherein the first  
5 digital signature is a DAA-based signature generated by using a DAA-based private key associated with the second device, wherein the first and the second devices authenticate to each other anonymously.

15. The method of claim 12, wherein the first random value is an ephemeral DH private  
10 key associated with the remote entity.

16. An apparatus comprising:

a memory to store cryptographic information from an issuer;  
a digital signature logic to generate digital signatures; and  
15 a direct anonymous attestation module (DAA) to convince a verifier that the DAA possess cryptographic information from an issuer of a trusted membership group without disclosure of any unique identification information associated with the apparatus, wherein the DAA is operable to initiate two-way mutual authentication with a remote entity and remain  
20 anonymous to the remote entity after performing the authentication;  
and  
establish a mutually shared session key for use in secure communication.

17. The apparatus of claim 16, wherein the DAA is operable to  
25 send a first message comprising at least a key-exchange-protocol public key computed based on a first random value;  
compute, in response to receiving a second message, a shared value based on the first random value and a second key-exchange-protocol public key associated with the remote entity;  
30 generate a session key and a message authentication code (MAC) key based at least on the shared value;  
authenticate a first digital signature from the second message based on combined public keys retrievable from the first digital signature, wherein the first

digital signature is associated with the remote entity and is retrievable by  
using a public key from the first public key certificate;  
generate, by using a DAA-based private key, a DAA-based signature based on the  
combined public keys; and  
5 send a third message comprising at least the DAA-based signature.

18. The apparatus of claim 17, wherein the remote entity is a server acting as a verifier,  
wherein the first message further includes a group ID (GID), wherein the DAA-based  
signature in the third message is generated further based on a signature-based revocation  
10 list and includes non-revoked proof.

19. The apparatus of claim 17, wherein the remote entity is a second device, wherein the  
first message further includes a basename associated with the first device, wherein the first  
digital signature is a DAA-based signature generated in conjunction with a DAA-based  
15 private key associated with the second device.

20. An article of manufacture comprising a computer readable storage medium including  
data storing instructions thereon that, when accessed by a machine, cause the machine to  
perform a method comprising:  
20 initiating mutual authentication between a first device and a remote entity, wherein  
the first device remains anonymous to the remote entity after performing  
the authentication; and  
establishing a mutually shared session key for use in secure communication,  
wherein the initiating and the establishing are in conjunction with direct  
25 anonymous attestation (DAA).

21. The article of claim 20, wherein the method further comprising:  
sending a first message comprising at least a key-exchange-protocol public key  
computed based on a first random value;  
30 computing, in response to receiving a second message, a shared value based on the  
first random value and a second key-exchange-protocol public key  
associated with the remote entity;  
generating a session key and a message authentication code (MAC) key based at



- least on the shared value;  
authenticating a first digital signature from the second message based on combined  
public keys retrievable from the first digital signature, wherein the first  
digital signature is associated with the remote entity and is retrievable by  
5 using a public key from the first public key certificate;  
generating, by using a DAA-based private key, a DAA-based signature based on  
the combined public keys; and  
sending a third message comprising at least the DAA-based signature.
- 10 22. The article of claim 21, wherein the remote entity is a verifier, wherein the first  
message further includes a group ID (GID), wherein the DAA-based signature in the third  
message is generated further based on a signature-based revocation list and includes non-  
revoked proof.
- 15 23. The article of claim 21, wherein the remote entity is a second peer device, wherein the  
first message further includes a basename associated with the first device, wherein the first  
digital signature is a DAA-based signature generated by using a DAA-based private key  
associated with the second device.

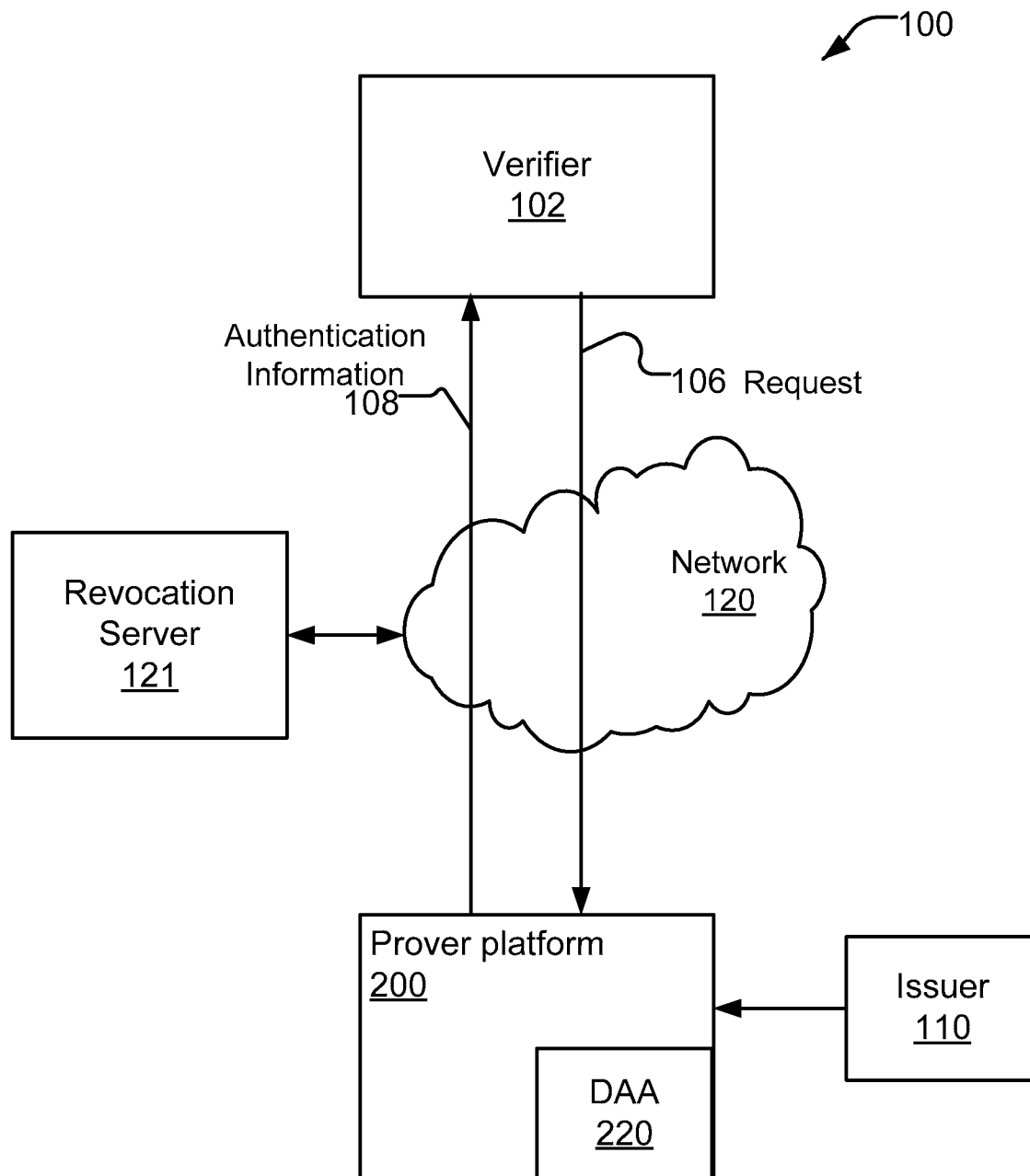
Figure 1

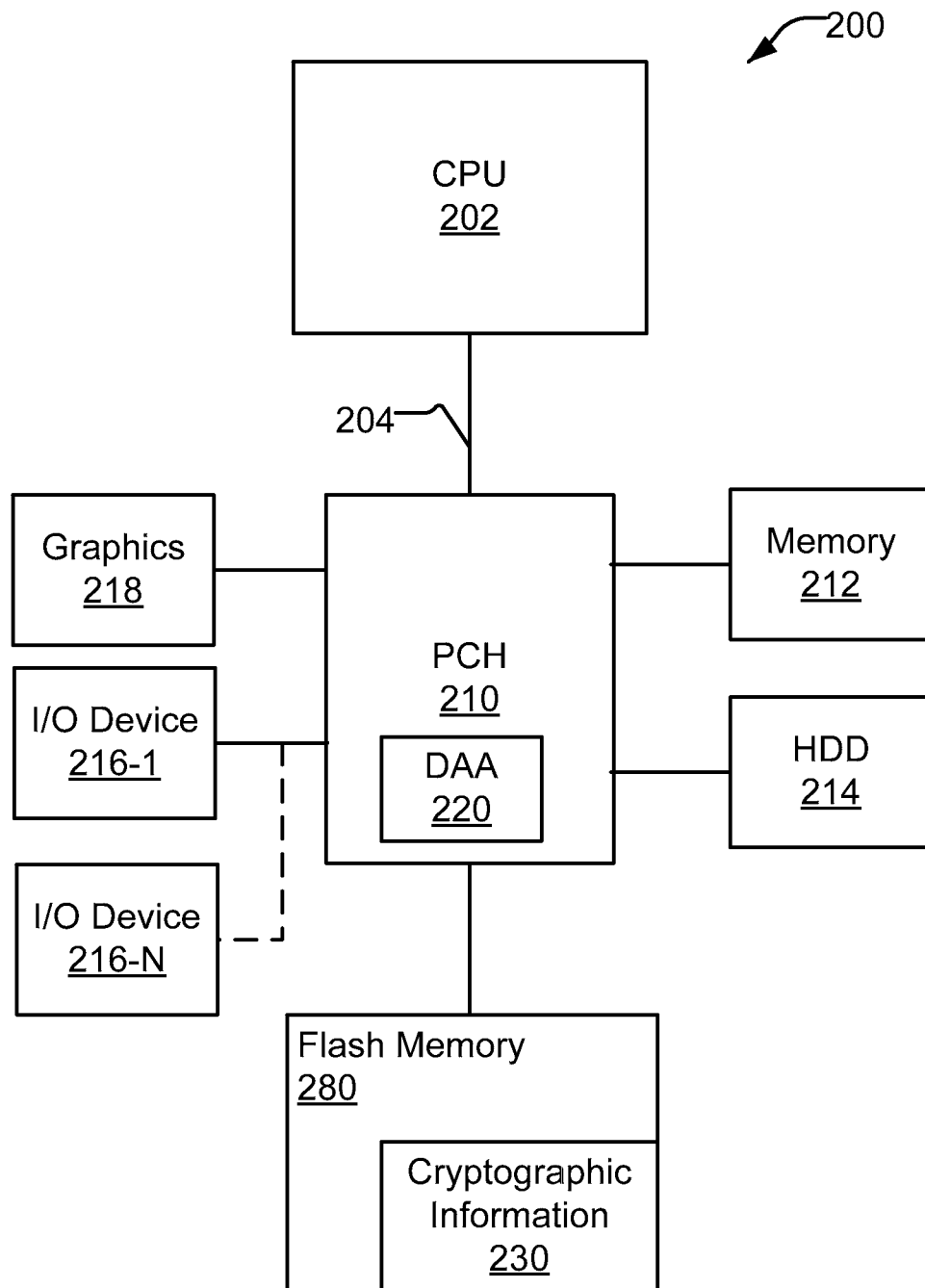
Figure 2

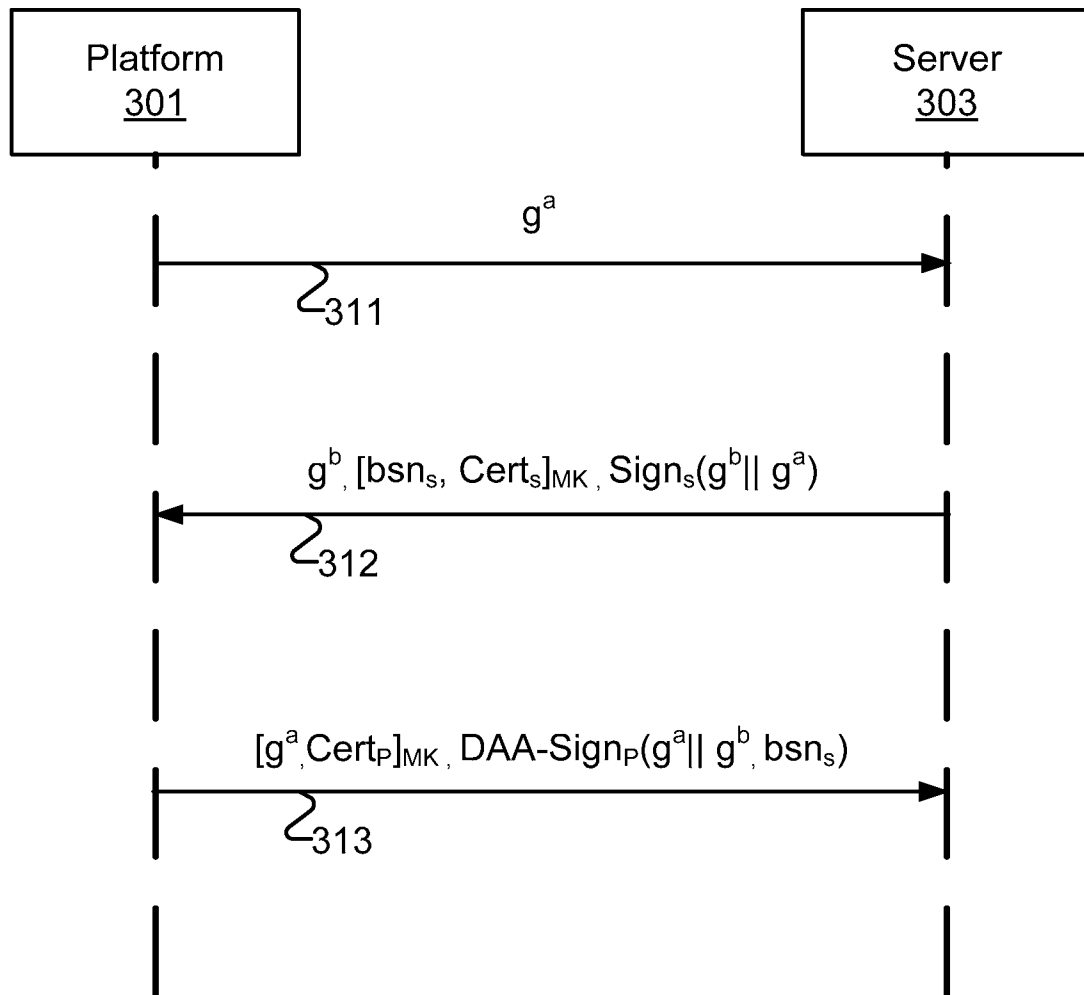
Figure 3

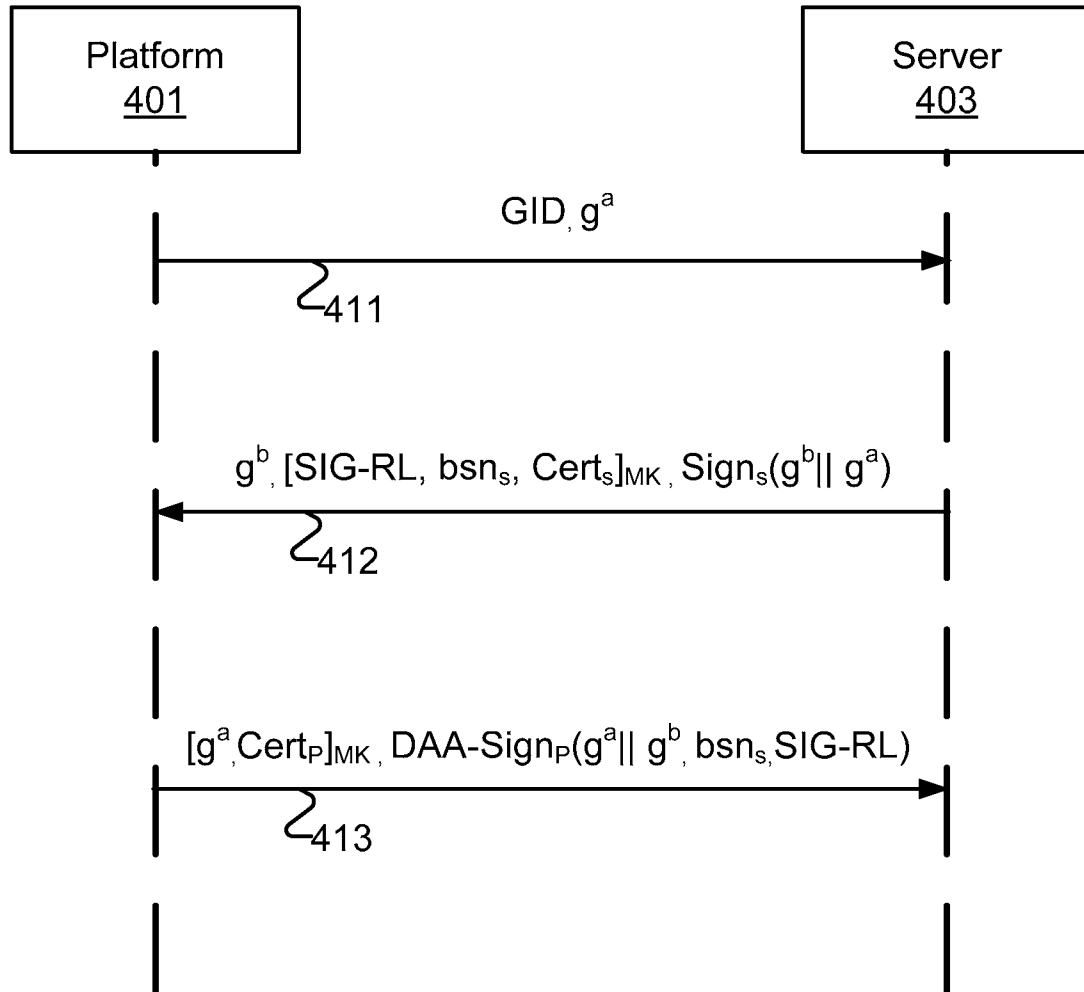
Figure 4

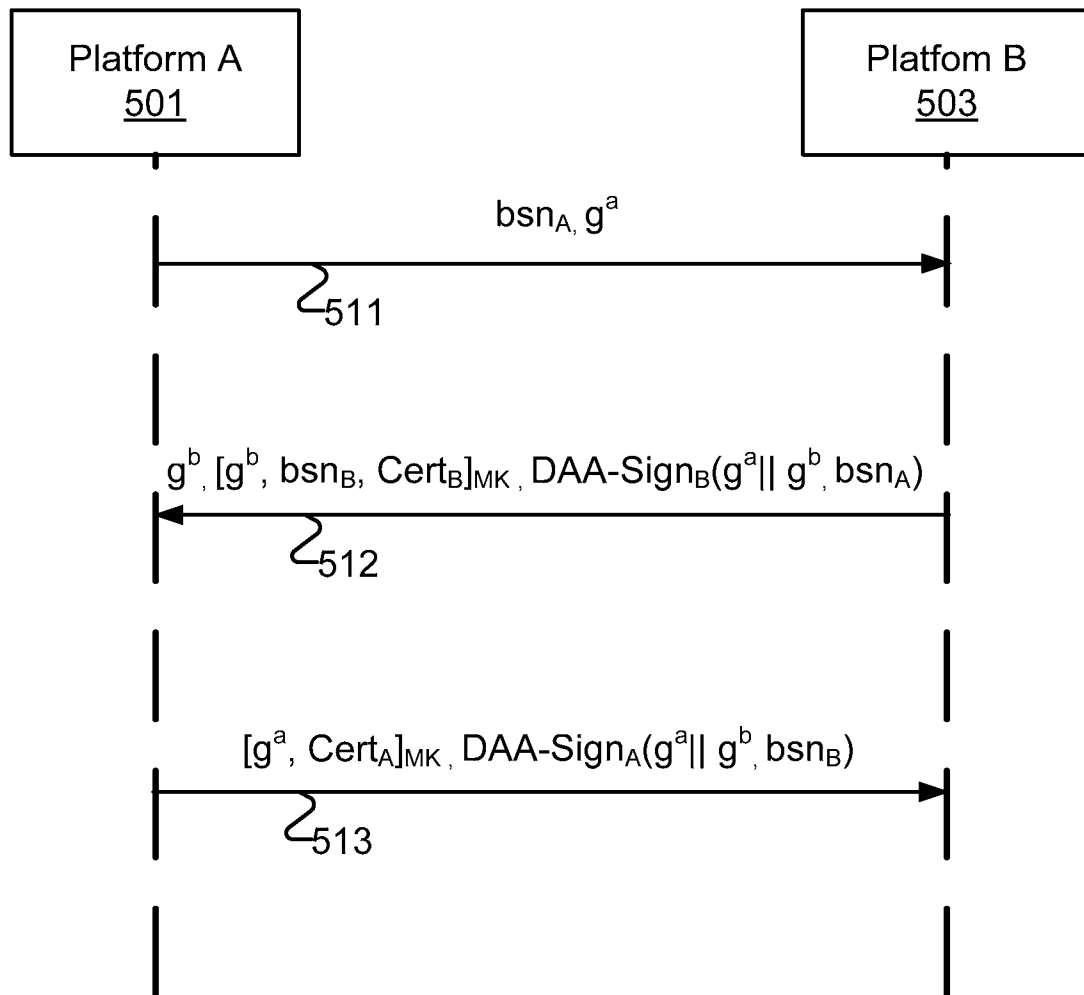
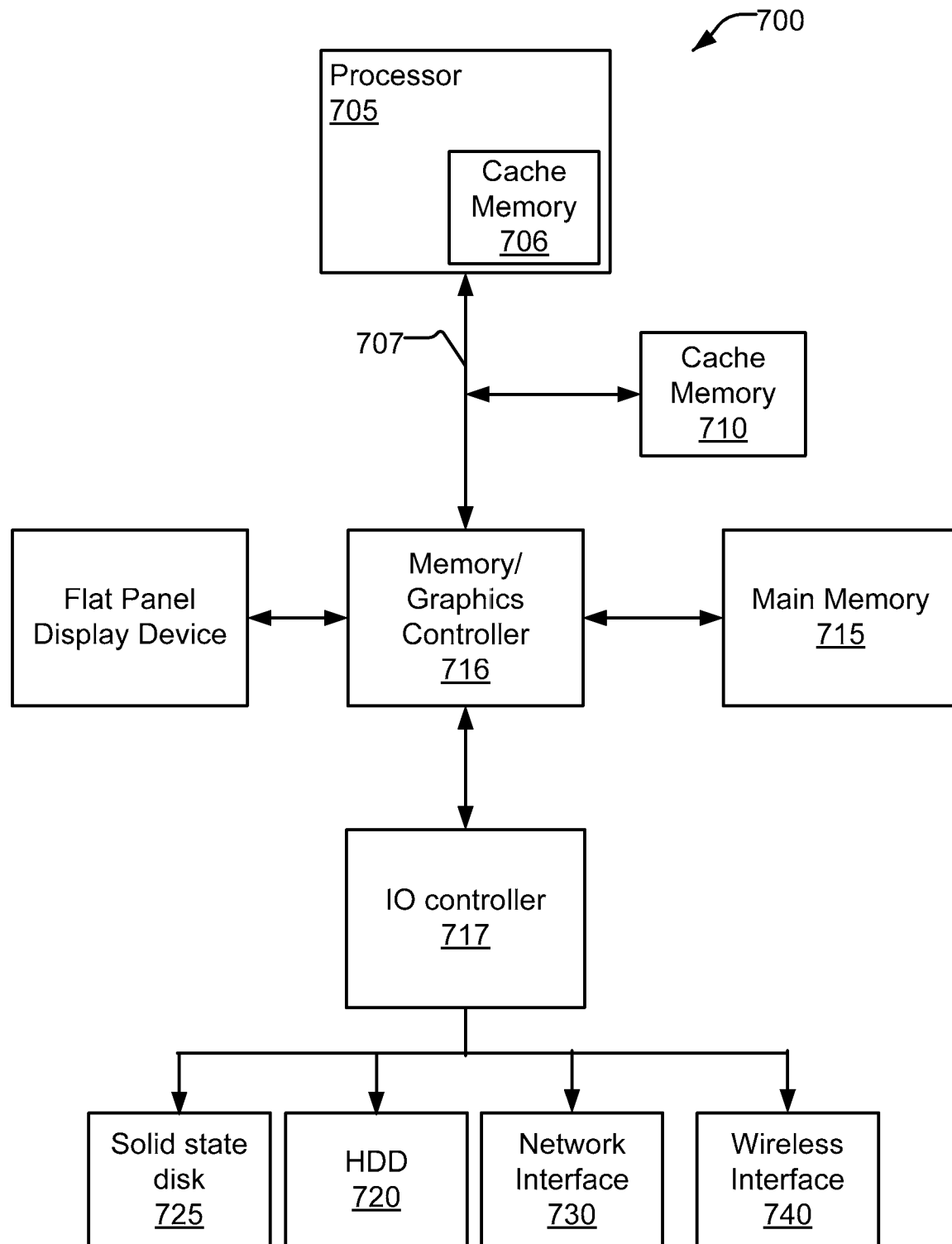
Figure 5

Figure 6

**Figure 7**