(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) **World Intellectual Property Organization**
International Bureau

(43) **International Publication Date**
20 June 2013 (20.06.2013)

W I P O | P C T

(10) **International Publication Number**
WO 2013/090881 Al

(51) **International Patent Classification:**
H04L 9/32 (2006.0 1) *H04L 9/20* (2006.0 1)

(21) **International Application Number:**
PCT/US20 12/0700 14

(22) **International Filing Date:**
17 December 2012 (17. 12.2012)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
13/326,837 15 December 201 1 (15. 12.201 1) US

(63) **Related by continuation (CON) or continuation-in-part (CIP) to earlier application:**
US 13/326,837 (CON)
Filed on 15 December 201 1 (15.12.201 1)

(71) **Applicant: TEXAS INSTRUMENTS INCORPORATED** [US/US]; P.O. Box 655474, Mail Station 3999, Dallas, TX 75265-5474 (US).

(71) **Applicant** *(for JP only):* **TEXAS INTRUMENTS JAPAN LIMITED** [JP/JP]; 24-1, Nishi-shinjuku 6- Chome, Shinjuku-ku Tokyo, 160-8366 (JP).

(72) **Inventor: PEETERS, Eric Thierry;** 9820 Crown Ridge Drive, Frisco, TX 75035 (US).

(74) **Agents: KEMPLER, William, B.** et al; Texas Instruments Incorporated, Deputy General Patent Counsel, P.O. Box 655474, Mail Station 3999, Dallas, TX 75265-5474 (US).

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

(84) **Designated States** *(unless otherwise indicated, for every kind cf 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, 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).

[Continued on nextpage]

(54) **Title:** COMBINED DIGITAL CERTIFICATE

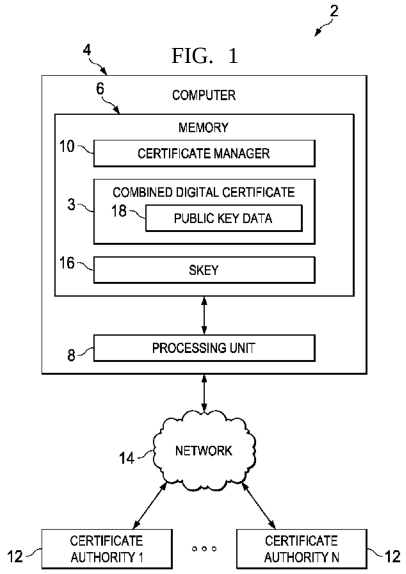


FIG. 1

(57) Abstract: A system (2) can comprise a memory (6) to store computer readable instructions and a processing unit (8) to access the memory (6) and to execute the computer readable instructions. The computer readable instructions can comprise a certificate manager (10) configured to request generation of N number of random values, where N is an integer greater than or equal to one. The certificate manager (10) can also be configured to request a digital certificate from at least one certificate authority (12) of at least two different certificate authorities (12). The request can include a given one of the N number of random values. The certificate manager (10) can also be configured to generate a private key (16) of a public-private key pair, wherein the private key (16) is generated based on a private key of each of the least two certificate authorities (12).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.1 7(H))*

— *as to the applicant's entitlement to claim the priority cf the earlier application (Rule 4.1 7(Hi))*

Published:

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

— *before the expiration cf the time limit for amending the claims and to be republished in the event cf receipt cf amendments (Rule 48.2(h))*

COMBINED DIGITAL CERTIFICATE

[0001] This relates to digital certificates in general and, more particularly, to apparatus and methods for generating combined digital certificates.

BACKGROUND

[0002] Public-key cryptography refers to a cryptographic system requiring two separate keys, one to lock or encrypt plaintext, and one to unlock or decrypt cyphertext. One of these keys is published or public (a public key) and the other is kept private (a private key). If the lock/encryption key is the one published then the system enables private communication from the public to the unlocking key's owner. If the unlock/decryption key is the one published then the system serves as a signature verifier of documents locked by the owner of the private key.

[0003] Several different public-key primitives can be used to provide a digital signature. Some are based on a discrete logarithm problem and are referred to as discrete logarithm-based public-key cryptosystem. A public-key cryptosystem can be employed in various schemes for providing confidentiality, integrity, authentication or non-repudiation function. Non-repudiation or authentication can be achieved through a digital certificate such as a public key digital certificate. A public key digital certificate can include two parts: the data and a signature of the data. The data can include the public-key and a unique identifier of a subscriber to a trusted third party: the certificate authority (CA). A signature of the CA on the subscriber's public-key conveys an authentic binding between the subscriber public key and the subscriber's identity (ID).

SUMMARY

[0004] One example relates to a system that can comprise a memory to store computer readable instructions and a processing unit to access the memory and to execute the computer readable instructions. The computer readable instructions can comprise a certificate manager configured to request generation of N number of random values, where N is an integer greater than or equal to one. The certificate manager can also be configured to request a digital certificate from at least one certificate authority of at least two certificate authorities. The request can include a given one of the N number of random values. The certificate manager can also be configured to generate a private key of a public-private key pair, wherein the private key is generated based on a private key of each of the at least two certificate authorities.

[0005] Another example relates to a method for generating a combined digital certificate. The method can comprise generating, at a computer, N number of values at a computer, wherein N is an integer greater than or equal to two. The method can also comprise, providing, from the computer, a request that includes a given one of the N number of random values to a corresponding certificate authority of N number of certificate authorities. The method can further comprise receiving, at the computer, a digital certificate from each of the N number of certificate authorities. The method can still further comprise generating, at the computer, a private key for the computer based on a combination of data received from each of the N number of certificate authorities. The method can yet further comprise generating, at the computer, a combined digital certificate based on a combination of each digital certificate received from each of the N number of certificate authorities.

[0006] Yet another example relates to a method for generating a combined digital certificate. The method can comprise generating, at a computer, a random value. The method can also comprise providing, from the computer, the random value to a first of two certificate authorities. The method can further comprise receiving, at the computer, a digital certificate from a second of the two certificate authorities. The digital certificate can be based on a digital certificate generated at the first certificate authority. The method can still further comprise generating, at the computer, a private key for the computer based on a number from each of the two certificate authorities. The method can yet further comprise generating, at the computer, a combined digital certificate based on data included in the digital certificate received at the computer.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] FIG. 1 illustrates an example of a system for generating a combined digital certificate.

[0008] FIGS. 2A and 2B illustrate a flowchart of an example method for generating a combined digital certificate.

[0009] FIGS. 3A and 3B illustrate another flowchart of an example method for generating a combined digital certificate.

[0010] FIG. 4 illustrates another example of a system for generating a combined digital certificate.

DETAILED DESCRIPTION OF EXAMPLE EMBODIMENTS

[0011] In one example, a computer, such as a crypto processor can be employed to generate and manage a combined digital certificate. The combined digital certificate can include data for generating a public key that is generated based on data received from multiple certificate authorities. Moreover, the computer can also generate a corresponding private key, which shall be stored separately (and securely) from the combined digital certificate. The private key can also be based on data provided from multiple certificate authorities. In this manner, even if an unauthorized user (e.g., a hacker) compromises one of the multiple certificate authorities, such an unauthorized user would be unable to determine the private key.

[0012] FIG. 1 illustrates an example of a system 2 for generating and managing a combined digital certificate 3. The combined digital certificate 3 can be generated by employing any discrete logarithm public key system, such as, but not limited to El-Gamal Signature, Schnorr Signature, Digital Secure Algorithm (DSA) or a variation thereof. Any of those schemes can use Elliptic curve cryptography (ECC) which provides inherently low memory and computation requirements. The system 2 can include, for example, a computer 4 that includes a memory 6 for storing machine readable instructions. The computer 4 could be implemented, for example, as a crypto processor, an application specific integrated circuit chip (ASIC), a smart card, a smart phone, a desktop computer, a notebook computer or the like. The memory 6 could be implemented, for example, as a non-transitory computer readable medium, such as random access memory (RAM), flash memory, a hard drive, etc. Some portions of the memory 6 can be accessed by external systems upon request. However, in some examples, some portions of the memory 6 can be secure and only accessible by internal components of the computer 4. The computer 4 can also include a processing unit 8 for accessing the memory 6 and executing the machine readable instructions. The processing unit 8 could be implemented, for example, as a processor core. The memory 6 can include a certificate manager 10 that can generate, modify and/or manage the combined digital certificate 3, which combined digital certificate 3, can also be stored in the memory 6. It is to be understood that in other examples, the certificate manager 10 could be stored on another system, such as an external system, such as a server or a host system, such a smart phone or other device that houses the computer 4.

[0013] The certificate manager 10 can initiate a generation of the combined digital certificate 3 in response to a condition being met. For instance, if the computer 4 is implemented as a crypto processor, the certificate manager 10 could initiate the generation of the digital certificate in response to an activation request from another system. In other examples, the certificate manager 10 could initiate the generation of the combined digital certificate 3 in response to user input.

[0014] The computer 4 can communicate with N number of certificate authorities 12 over a network 14, where N is an integer greater than or equal to two. The network 14 could be implemented, for example, as a public network (e.g., the Internet), a private network, or the like. Each certificate authority 12 of the N number of certificate authorities 12 can be implemented as a system that issues digital certificates. The digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (third parties) to rely upon signatures or assertions made by a private key that corresponds to the public key that is certified. In such a model of trust relationships, each of the 1-N certificate authorities 12 is a trusted third party that is trusted by both the subject (owner) of the certificate and the third party relying upon the certificate.

[0015] In one example, in response to initiation of the generation of the combined digital certificate 3, the certificate manager 10 can request that N number of random numbers be generated by the processing unit 8, which random numbers can be referred to as "rl ...rN." It is noted that in some examples, the certificate manager 10, can provide separate requests over a relatively large period of time for generation of the random numbers. For instance, the certificate manager 10 can be configured to request generation of r1 at a time of manufacture. Additionally, the certificate manager 10 can be configured to request generation of r2-rN after delivery of the computer 4 to a customer site. As one example, the computer 4 can be embedded with r1 and can be configured to request generation of r2-rN upon activation at the customer site.

[0016] The certificate manager 10 can send r1 (or a multiple thereof) to certificate authority 1. In response, the certificate authority 1 can return a digital certificate 1 which can include data for generating a public key for the computer 4, wherein the public key is associated with the certificate authority 1. The certificate authority 1 can also include data, such as an integer for generating a private key that corresponds to the public key associated with the certificate authority 1. It is noted that in some examples, the digital certificate 1 and the data for generating the private key and public key associated with the certificate authority 1 can be embedded into the computer 4 at a time of manufacture of the computer 4. Additionally, the certificate manager 10 can send r2. ..rN to a corresponding certificate authority 12 of each of the 2-N certificate authorities 12. In response, each of the 2-N certificate authorities 12 can provide the computer 4 with a corresponding digital certificate, and data for generating a public key and corresponding private key for the computer 4, which can be associated with a corresponding 2-N certificate authority 12, which data can be referred to as certificate data. The certificate manager 10 and/or the processing unit 8 can employ the certificate data provided by each of the 1-N certificate authorities 12 to generate a private key for the computer 4, which private key can be referred to as SKey 16. Moreover, in some examples, the certificate manager 10 can also provide public key data 18 that is based on the digital certificates 1-N for generating a public key for the computer 4 that corresponds to Skey 16, which can be referred to as PKey. In some examples, the public key data 18 can be provided to a third party. In other examples, the public key data 18 can be known by the third party through other methods (e.g., a registration service). In some examples, the certificate manager 10 can also generate the combination certificate 3 that can include the public key data 18. In some examples, the combination certificate 3 can also include data for identifying each of the 1-N certificate authorities 12. By employing this technique, the certificate manager 10 can generate the combined digital certificate 3 that is based on digital certificates provided by each of the 1-N certificate authorities 12. Moreover, by employing this technique, none of the 1-N certificate authorities 12 need to communicate with each other.

[0017] In another example, upon initiation of the generation of the digital certificate, the certificate manager 10 can request that one random number be generated by the processing unit 8, which random number can be referred to as r1. The certificate manager 10 can send r1 to certificate authority 1. In response, the certificate authority 1 can generate a digital certificate 1 and data (e.g., an integer) for generating a public key and corresponding private key for the computer 4. The certificate authority 1 can forward the data for generating the private key to the computer 4 and forward the digital certificate 1 to a certificate authority 2, wherein the private key is associated with certificate authority 1. Moreover, the certificate authority 2 can authenticate the certificate authority 1 to ensure that the digital certificate 1 originated from certificate authority 1 and not from an unauthorized source (e.g., a hacker). Certificate authority 2 can generate a digital certificate 2 based on the digital certificate 1 and forward the digital certificate 2 to the certificate manager 10, which digital certificate can include public key data 18 for generating a PKey associated with both certificate authority 1 and certificate authority 2. The certificate authority 2 can also provide data (e.g., an integer) for generating a private key associated with the certificate authority 2. The certificate manager 10 and/or the processing unit 8 can generate an SKey 16 based on data provided from the certificate authority 1 and the certificate authority 2, wherein the SKey 16 corresponds to the PKey . The certificate manager 10 and/or the processing unit 8 can also generate the combined digital certificate 3 based on the digital certificate 2. In some examples, the combined certificate 3 can include the public key data 18 which can be employed to generate the PKey. By employing this technique, the size of the combined certificate can be reduced, which can save memory.

[0018] In both techniques, the combined digital certificate 3 can be based on data provided by 1-N certificate authorities 12. In the first technique, even if an unauthorized user (e.g., a hacker) gains access to any one of the 1-N certificate authorities 12, the combined digital certificate 3 would not be compromised. In fact, to compromise the security of the combined digital certificate 3, such an unauthorized user would need to compromise to all of the 1-N certificate authorities 12. In the second technique, since the certificate authority 1 is authenticated by certificate authority 2, data provided by the certificate authority 1 can be trusted by the certificate authority 2. Thus, the combined digital certificate 3 provides significant resistance to security breaches. Moreover, liability for such security breaches would be distributed over each of the 1-N certificate authorities 12.

[0019] In view of the foregoing structural and functional features described above, example methodologies will be better appreciated with reference to FIGS. 2A, 2B, 3A and 3B. While, for purposes of simplicity of explanation, the example methods of FIGS. 2A, 2B, 3A and 3B are shown and described as executing serially, the present examples are not limited by the illustrated order, as some actions could in other examples occur in different orders and/or concurrently from that shown and described herein.

[0020] FIGS. 2A and 2B illustrate an example flowchart of an example method 200 that could be employed to generate a combined digital certificate, such as the combined digital certificate 3 illustrated in FIG. 1.

[0021] At 210, certificate generation can be initiated. The certificate initiation could be initiated, for example, by a certificate manager, such as the certificate manager 10 illustrated in FIG. 1. In such a situation, the certificate manager could be executing on a computer, such as a crypto processor. In the method 200, the combined certificate can be generated by employing techniques from ECC. However, other cryptographic techniques could additionally or alternatively be employed. In ECC, points along a curve E can define a finite field. In one example, Equation 1 can define the finite field employed for the method 200.

Equation 1: $$y^2 = x^3 + ax + b;$$

wherein $P=\{x_P,y_P\}$; $Q = \{XQ,VQ\}$; and P and Q are points on the curve E.

[0022] Additionally, in ECC, the number of points on the curve E can be represented as a finite integer 'n'. In such a situation, Equations 2 and 3 can represent a relationship between n, P and Q.

Equation 2: $nP = P + P + P ... + P$

Equation 3: $Q = nP$

[0023] At 220, N number of random numbers can be generated, for example, by a processing unit, such as the processing unit 8 illustrated in FIG. 1. Each of the N number of random numbers can be calculated as points on the curve E. For instance, in one example, the processing unit can generate a random number, r_i, where i is an integer between 1 and N. The processing unit can employ elliptic curve point multiplication to calculate $r_i.G$, where G is a number points on the curve E defined at a generator point G such that r;.G is a point on the curve E. At 230, the certificate manager can provide a random number r_i to a corresponding certificate authority i, which certificate authority i could be implemented as one of the 1-N certificate authorities 12 illustrated in FIG. 1. In such a situation, the certificate authority i can have a private key and noted as CcAi and a public key denoted as QcAi- In such a situation, Equation 4 can depict the relationship between CcAi and QcAi- It is noted that Equation 4 denotes elliptic curve multiplication.

Equation 4: $Q_{CAi} = c_{CAi}.G$

[0024] In one example, for each subscriber A, each certificate authority i can assign a different identity number (e.g., a unique ID). In such a situation, each identity number could be implemented as the sum of each identity number attributed by each of the N number of certificate authorities ($ID_A=\sum(ID_{Ai})$). Alternatively, a given one of the certificate authorities i can have on a unique identity number shared by the other certificate authorities i. At 240, certificate authority i can calculate ki.G, where ki is a random number within the interval [1, n-1]. At 250, the certificate authority i can employ Equation 5 to calculate Pi. It is noted that Equation 5 denotes elliptic curve addition.

Equation 5: $P_i = r_i . G + kj. G$

[0025] At 260, certificate authority i can employ Equation 6 to calculate e;.

Equation 6: $e_i = H(Pi||ID)$

wherein H is a one way hash function; P_i is the resulting point of the elliptic curve addition given in Equation 5; and ID is a unique identifier for the computer.

[0026] At 270, the certificate authority i can employ Equation 7 or alternatively Equation 8 to calculate s;.

Equation 7: $s_j = e_j . k_j - c_{CAi} (\mathrm{mod}\ n)$

Equation 8: $s_i = k_i - ei.CcAi\ (\mathrm{mod}\ n)$

[0027] At 280, the certificate authority i can provide a digital certificate i and other data to the certificate manager, such that at least Pi, s_i and e_i are provided to the certificate manager. At 290, a determination can be made as to whether i is less than or equal to N. If the determination is positive (e.g., YES), the method 200 can proceed to 300. If the determination is negative (e.g., NO), the method can proceed to 310 (FIG. 2B). At 300, the value of i can be increased by one and the method can return to 230.

[0028] At 310 of FIG. 2B, the certificate manager can calculate a private key for the associated computer, which private key can be denoted as "SKey." SKey can be stored, for example, in a secure memory of the computer. In examples where Equation 7 is employed to calculate s_i, the certificate manager can employ Equation 9 to calculate SKey. Alternatively, in situations where Equation 8 is employed to calculate s_i, the certificate manager can employ Equation 10 to calculate SKey.

Equation 9: $$SKey = \left(\sum_{i=1}^{N} s_i + r_i e_i\right)(\text{modn})$$

Equation 10: $$SKey = \left(\sum_{i=1}^{N} (s_i + r_i) \prod_{j \neq i} e_j\right)(\text{mod}\, n)$$

[0029] At 320, the certificate manager can determine public key data that can be employed (e.g., by a third party) to calculate a public key corresponding to SKey for the associated computer, which public key can be denoted as "PKey." In some examples, the public key data can include the P_i provided from each certificate authority i. In some examples, by employing Equations 11 and 12, the third party can employ the public key data to derive PKey. As shown in Equations 11 and 12, PKey can be based on **QCA**, which can be implemented as the sum of each **QcAi** received from the 1-N certificate authorities. In other examples, the third party can employ Equations 12 and 13 to compute PKey.

Equation 11: $$PKey = \sum_{i=1}^{N} e_i P_i - Q_{CA}$$

Equation 12: $$Q_{CA} = \sum_{\mathbf{i=i}}^{\mathbf{N}} \mathbf{QcAi}$$

Equation 13: $$PKey = \sum_{i=1}^{N} \left(P_i \prod_{j \neq i} e_j\right) - \left(\prod_{i=1}^{N} e_i\right) Q_{CA}$$

[0030] At 330, the combined digital certificate can be generated. The combined digital certificate can identify each certificate authority i employed to generate the combined digital certificate. Moreover, in some examples, the combined digital certificate can include the public key data. By employing the method 200, no interaction between each of the certificate authorities i is needed. Furthermore, by employing ECC, a significant reduction of memory usage can be achieved in comparison to other encryption schemes.

[0031] FIGS. 3A and 3B illustrate an example flowchart of another example of a method 400 that could be employed to generate a combined digital certificate, such as the combined digital certificate 3 illustrated in FIG. 1.

[0032] At 410, certificate generation can be initiated. The certificate initiation could be initiated, for example, by a certificate manager, such as the certificate manager 10 illustrated in FIG. 1. In such a situation, the certificate manager could be executing on a computer, such as a crypto processor. In the method 400, the combined digital certificate can be generated by employing techniques from ECC. However, other cryptographic techniques could be additionally or alternatively employed. In one example, Equation 1 can be employed to define a finite field for the method 400. In such an example, an elliptical curve E can have a finite number of points 'n'. Moreover, as noted in Equation 1, points **P** and **Q** can be points on the curve E. Further, Equations 2 and 3 can define a relationship between n, **P** and **Q.**

[0033] At 420, a random number can be generated, for example, by a processing unit, such as the processing unit 8 illustrated in FIG. 1. The random number can be calculated as a point on the curve E. For instance, in one example, the processing unit can generate a random number, r. The processing unit can employ elliptic curve point multiplication to calculate r.G, where G is a number of points on the curve E defined at a generator point G such that r.G is a point on the curve E. At 430, the certificate manager can provide the random number r.G to a certificate authority 1, which certificate authority i could be implemented as the certificate authority 1 illustrated in FIG. 1. In such a situation, the certificate authority 1 can have a private key, which private key can be referred to as **CCAI** and a public key denoted as **QCAI** - In such a situation, Equation 4 can depict the relationship between **CCAI** and **QCAI** - At 440, certificate authority 1 can calculate k_i.G, where k_i is a random number within the interval [1, n-1]. At 450, the certificate authority 1 can employ Equation 5 to calculate **Pi.** At 460, certificate authority 1 can employ Equation 14 to calculate s_i.

Equation 14: $s_i = k_1 + c_{CA1} \bmod n$

[0034] At 470, the certificate authority 1 can provide the certificate manager with data that includes at least si. At 475, certificate authority 1 can be authenticated by a certificate authority 2. Such an authentication can ensure that data provided from certificate authority 1 did in fact originate from certificate authority 1 and not from an unauthorized source (e.g., a hacker). At 480, the certificate authority 1 can provide the certificate authority 2 with Pi and s_i. At 490 (FIG. 3B), the certificate authority 2 can calculate k_2.G, where k_2 is a random number within the interval [1, n-1]. At 500, the certificate authority 2 can employ Equation 15 to calculate P. It is noted that Equation 15 employs elliptical point multiplication.

Equation 15: $P = k_2.G + P_1$

[0035] At 510, the certificate authority 2 can employ Equation 16 to calculate e.

Equation 16: $e = H(P||ID)$

wherein H is a one-way hash function; and ID is a unique identifier for the computer.

[0036] At 520, the certificate authority 2 can calculate s_2. In some examples, the certificate authority 2 can employ Equation 17 to calculate s_2.

Equation 17: $s_2 = e(k_2 + c_{CA2}) \bmod n$

[0037] At 530, the certificate authority can provide the certificate manager with a digital certificate that includes at least P (Equation 15). Additionally, the certificate authority can provide the certificate manager with s_2. At 540, the processing unit can calculate a private key for the computer, which private key can be denoted as "SKey." In examples where Equation 17 is employed to calculate s_2, the processing unit can employ Equation 18 to calculate SKey.

Equation 18: $SKey = e(s_1 + r) + s_2 \bmod n$

[0038] At 550, the certificate manager and/or the processing unit can determine public key data that can be employed to generate a public key for the associated computer, which public key can be denoted as "PKey." The public key data can include the P received from certificate authority 2. In this manner, a third party can employ the public key data to calculate PKey. For instance, in examples where Equation 18 is employed to calculate SKey, the third party can employ Equations 19 and 20 to calculate PKey.

Equation 19: $QCA = QCA_I + QcA2$

Equation 20: $PKey = e(P + Q_{CA})$

[0039] At 560, the certificate manager can generate and store the combined digital certificate. In some examples, the combined digital certificate can include the public key data. By employing the method 400, a reduction of the memory can be achieve since only one value for P needs to be stored at the computer. Moreover, additional memory saving can be achieved by employing ECC. Still further, the method allows an increase in security since the combined digital certificate is based on public keys QCA_I, and QCA_I of two different certificate authorities.

[0040] FIG. 4 illustrates another example of a system 600 for generating and managing a combined digital certificate 602. The system 600 can include a host computer 604 with a crypto processor 606 stored thereon. The crypto processor 606 could be implemented, in a manner similar to the computer 4 illustrated in FIG. 1. For instance, the crypto processor 606 could be implemented as a dedicated computer on a chip or microprocessor for carrying out cryptographic operations, embedded in a packaging with multiple physical security measures, thereby providing the crypto processor 606 with a degree of tamper resistance. In one example, the crypto processor 606 could be implemented as a trusted platform module (TPM). The host computer 604 can include a memory 607 (e.g., a non-transitory computer readable medium, such as RAM, flash memory, a hard drive or the like) for storing machine-readable instructions. The host computer 604 can also include a processing unit 608 to access the memory 607 and execute the machine-readable instructions. The processing unit 608 can include a processor core. In some examples, the host computer 604 could be implemented as a smart phone, a desktop computer, a laptop computer, a server or the like.

[0041] The host computer 604 can communicate with N number of certificate authorities 610 via a network 612. The network 612 could be implemented, for example, as the Internet, a private network or a combination thereof. In FIG. 4, the components of certificate authority 1 are shown in detail. It is to be understood that 2-N certificate authorities 610 could be implemented in a similar manner. Certificate authority 1 can be implemented as a computer, such as a trusted issuer of digital certificates.

[0042] Certificate authority 1 can include a memory 614 for storing machine-readable instructions. The memory 614 could be implemented, for example, as RAM, flash memory, a hard drive or the like. The certificate authority 1 can also include a processing unit 618 for accessing the memory 614 and executing machine readable instructions. The memory 614 can include a private key, **CCAI** 620 for the certificate authority 1. The certificate authority 1 can also include a public key, **QCAI** 622 for the certificate authority 1.

[0043] The memory 607 of the host computer 604 can include a certificate manager 616 that can initiate generation of the combined digital certificate 602. Initiation of the generation of the combined digital certificate 602 can be in response to user input. In response to initiation of the generation of the combined digital certificate 602, the certificate manager 616 can request that the crypto processor 606 generate one or more random numbers, such as described with respect to FIGS. 2A, 2B, 3A and 3B.

[0044] As described with respect to the methods 200 or 400 illustrated in FIGS. 2A, 2B, 3A and 3B, in response to initiation of the generation of the combined digital certificate 602, the certificate manager 616 can receive at least K digital certificates 624 from 1-N certificate authorities 610, where K is an integer greater than or equal to one, as well as data from each of the 1-N certificate authorities 610 (e.g., Si ...s_n). The certificate manager 616 can provide the crypto processor 606 with data (e.g., certificate data) to generate a private key (SKey) 626 and public key data 628 for generating a corresponding public key (PKey) 629 for the crypto processor 606 based on data provided from the 1-N certificate authorities 610 (e.g., $\mathrm{si}\ldots s_n$ and **Pi**$\ldots P_n$). Additionally, the crypto processor 606 can employ the data provided by the certificate manager 616 to generate the combined certificate 602 In some examples, the combined certificate 602 can include the public key data 628. The combined certificate 602 can include, for example, an identification of each of the N number of certificate authorities 610 on which the combined digital certificate 602 is based.

[0045] At some point in time, the host computer 604 can employ the combined certificate to digitally sign a document 630. In such a situation, the certificate manager 616 can provide the document 630 to the crypto processor 606 along with a request for the digital signature 632. In one example, the crypto processor 606 can employ a digest algorithm to create a digest comprised of a portion of the document 630. The crypto processor 606 can employ the SKey 626 to sign the digest of the document 630, which signed digest can be the digital signature 632.

[0046] A third-party 634 (e.g., a computer system) can request the document 630. The document 630, the combined certificate 602 along with the digital signature 632 and a public key (Qc_Ai) of a given certificate authority 610 of the N number of certificate authorities 610 can be provided to the third-party 634. The combined certificate can also include the digest algorithm employed for calculating the digest of the document 630. Additionally, the third party 634 can generate PKey 629 based on the public key data 628.

[0047] The third-party 634 can communicate with the given certificate authority 610 to validate the public key (Qc_Ai) of the given certificate authority 610. In this manner, the third-party 634 can trust that PKey 629 was generated based on the private key (cc_Ai) of the given certificate authority 610. Additionally, the third-party 634 can employ the digest algorithm to regenerate the digest of the document 630. The third-party 634 can verify the digital signature 632 with the PKey 629 included in the combined digital certificate 602, which can result in a verified digest. The third party 634 can compare the regenerated digital digest with the verified digest to ensure that the document 630 was signed by the crypto processor 606 and that the document 630 had not changed since the digital signature 632 for the document 630 was generated.

[0048] Those skilled in the art to which the invention relates will appreciate that modifications may be made to the described examples, and also that many other embodiments are possible, within the scope of the claimed invention.

CLAIMS

What is claimed is:

1. A method for generating a combined digital certificate comprising:

generating, at a computer, N number of random values, wherein N is an integer greater or equal to two;

providing, from the computer, a request that includes a given one of the of the N number of random values to a corresponding certificate authority of N number of certificate authorities;

receiving, at the computer, a digital certificate from each of the N number of certificate authorities in response to the request;

generating, at the computer, a private key for the computer based on a combination of data received from each of the N number of certificate authorities; and

generating, at the computer, a combined digital certificate based on a combination of each digital certificate received from each of the N number of certificate authorities.

2. The method of claim 1, wherein each digital certificate received from each of the N number of certificate authorities is generated based on elliptical curve cryptography.

3. The method of claim 2, wherein each of the N number of random values characterizes a point on an elliptical curve.

4. The method of claim 3, wherein a given digital certificate from the N number of certificate authorities comprises a set of numbers characterizing a point on the elliptical curve, wherein the point on the elliptical curve is calculated based on the given one of the of the N number of random values.

5. The method of claim 2, wherein the private key for the computer is configured such that:

$$SKey = \left(\sum_{i=1}^{N} s_i + r_i e_i \right) (\mathrm{mod}\, n) \text{ or}$$

$$SKey = \left(\sum_{i=1}^{N} (s_i + r_i) \prod_{j \neq i} e_j \right) (\mathrm{mod}\, n)$$

wherein:

SKey denotes the private key for the computer;

ri denotes the given one of the N random values generated by the computer;

e_i denotes results of a hash function executed at a certificate authority i of the N number of certificate authorities;

si denotes an integer provided from the certificate authority i; and

n denotes a number of points on the elliptical curve.

6. The method of claim 1, wherein the given one of the N number of random values is generated at a time of manufacture of the computer and a remainder of the N number of random value is generated after activation of the computer.

7. The method of claim 1, wherein each digital certificate received from each of the N number of certificate authorities is generated independently from each other.

8. A method for generating a combined digital certificate comprising:

generating, at a computer, a random value;

providing the random value to a first of two certificate authorities;

receiving, at the computer, a digital certificate from a second of the two certificate authorities, wherein the digital certificate is based on a digital certificate generated at the first certificate authority;

generating, at the computer, a private key for the computer based on a number from each of the two certificate authorities; and generating, at the computer, a combined digital certificate based on data included in the digital certificate received at the computer.

9. The method of claim 8, further comprising generating a public key for the computer corresponding to the private key for the computer, wherein the public key is based on a public key of each of the two certificate authorities.

10. The method of claim 8, wherein the digital certificate received from the second of the two certificate authorities is based on elliptical curve cryptography.

11. The method of claim 10, wherein the private key for the computer is configured such that:

SKey = $e(s_1 + r) + s_2$ mod n;

wherein:

SKey denotes the private key for the computer;

r denotes the random value generated by the computer;

si denotes an integer provided from the first certificate authority of the two certificate authorities;

s2 denotes an integer provided from the second certificate authority of the two certificate authorities;

e denotes results of a hash function executed at the second certificate authority of the two certificate authorities; and

n denotes a number of points in an elliptical curve employed to calculate si and s2.

12. The method of claim 18, further comprising generating, at a third party, a public key corresponding to Skey.

13. A system comprising:

a memory storing computer readable instructions; and

a processing unit to access the memory and to execute the computer readable instructions;

wherein the computer readable instructions comprise:

a certificate manager configured to:

request generation of N number of random values, where N is an integer greater than or equal to one;

request a digital certificate from at least one certificate authority of at least two different certificate authorities, wherein the request includes a given one of the N number of random values; and

generate a private key of a public-private key pair, wherein the private key is generated based on a private key of each of the at least two different certificate authorities.

14. The system of claim 13, wherein the certificate manager employs elliptic curve cryptography to generate the private key.

15. The system of claim 13, wherein the at least two different certificate authorities comprises at least three different certificate authorities.

16. The system of claim 13, wherein certificate manager is further configured to request another digital certificate from another of the at least two certificate authorities and wherein the digital certificate generated by each of the at least two different certificate authorities for the certificate manager are generated independently of each other.

17. The system of claim 13, wherein a digital certificate generated by another certificate authority of the at least two different certificate authorities is generated based on data received from the given certificate authority of the at least two different certificate authorities.

18. The system of claim 13, wherein the system is a crypto processor.

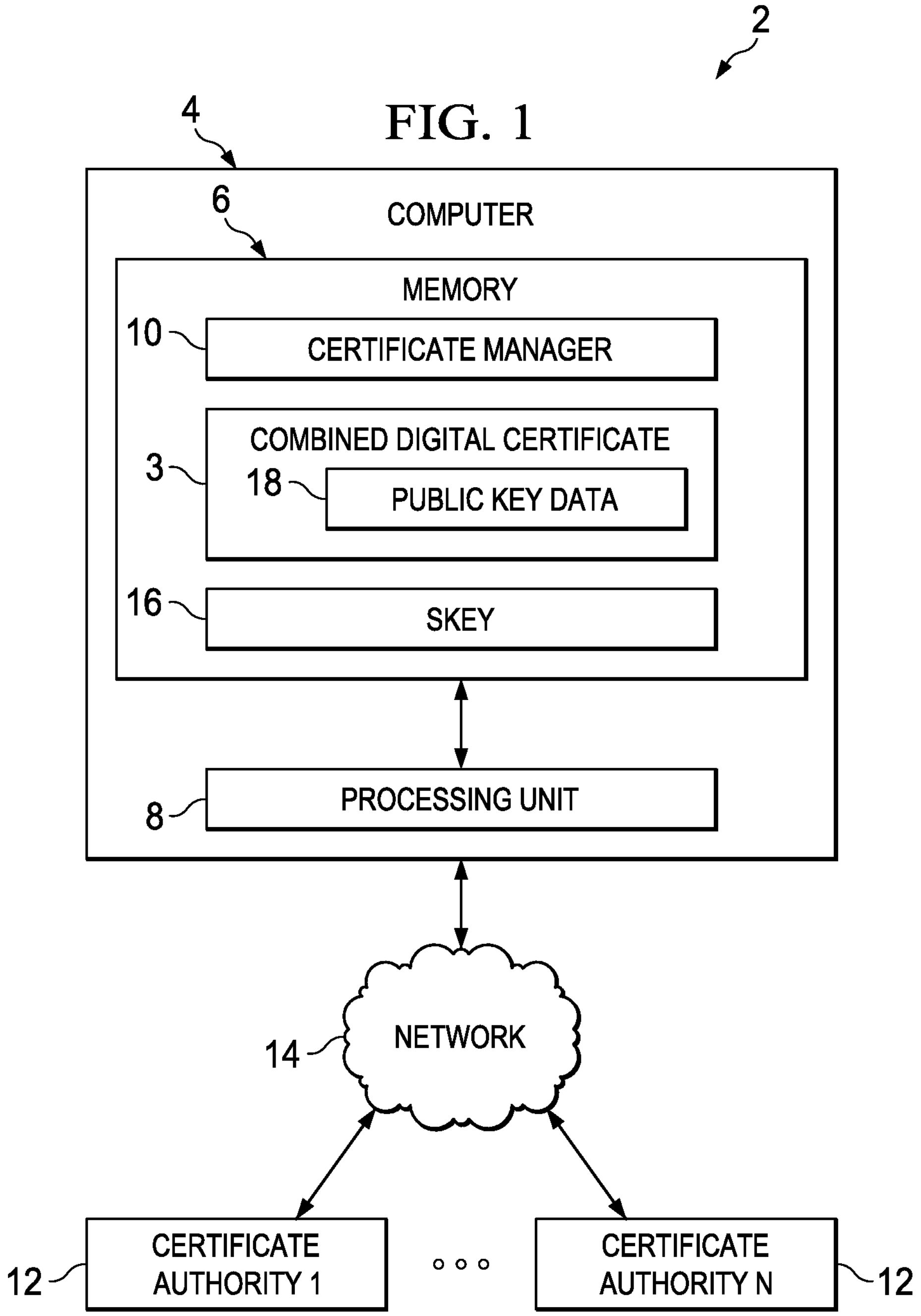
19. A non-transitory computer readable medium having computer executable instructions for performing a method, the method comprising:

requesting generation of N number of random values, where N is an integer greater than or equal to one;

requesting a digital certificate from at least one certificate authority of at least two different certificate authorities, wherein the request includes a given one of the N number of random values; and

requesting generation of a private key of a public-private key pair, wherein the private key is generated based on a private key of each of the at least two different certificate authorities.

FIG. 1


2
4
6
COMPUTER
MEMORY
10
CERTIFICATE MANAGER
COMBINED DIGITAL CERTIFICATE
3
18
PUBLIC KEY DATA
16
SKEY
PROCESSING UNIT
8
NETWORK
14
CERTIFICATE AUTHORITY 1
12
CERTIFICATE AUTHORITY N
12

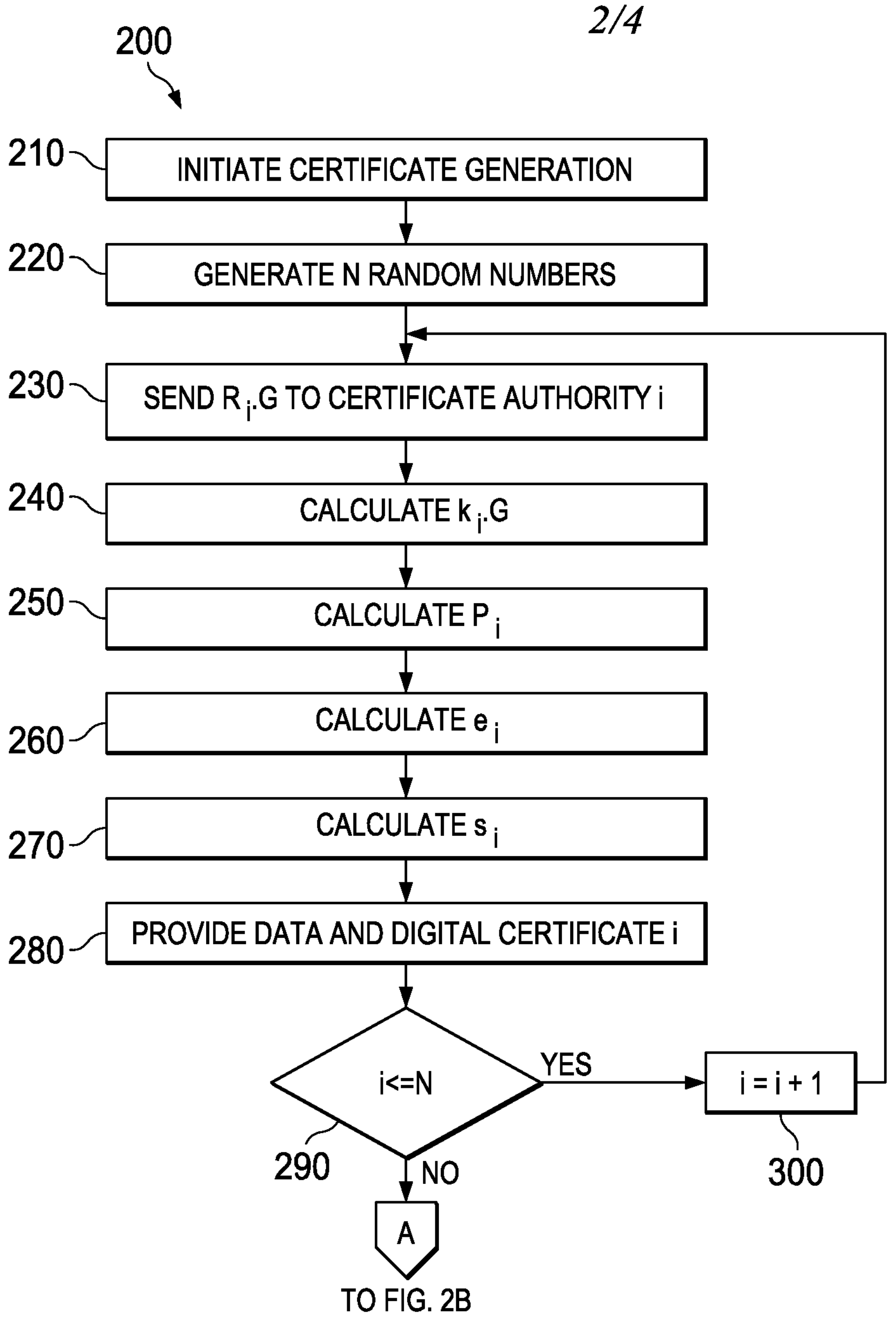

200
210
INITIATE CERTIFICATE GENERATION
220
GENERATE N RANDOM NUMBERS
230
SEND $R_i.G$ TO CERTIFICATE AUTHORITY i
240
CALCULATE $k_i.G$
250
CALCULATE P_i
260
CALCULATE e_i
270
CALCULATE s_i
280
PROVIDE DATA AND DIGITAL CERTIFICATE i
i<=N
290
YES
i = i + 1
300
NO
A
TO FIG. 2B

FIG. 2A

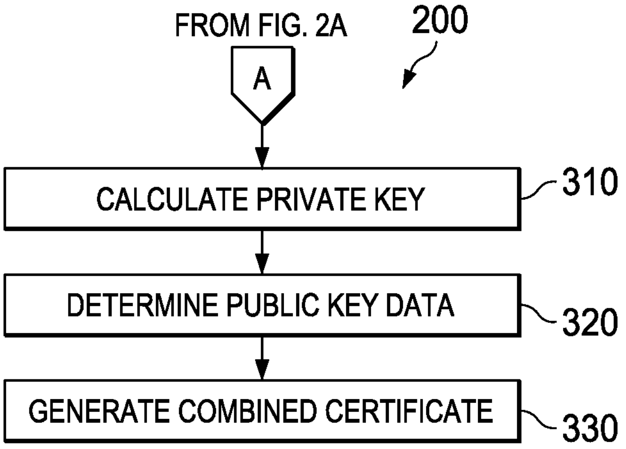

FROM FIG. 2A
200
A
CALCULATE PRIVATE KEY
310
DETERMINE PUBLIC KEY DATA
320
GENERATE COMBINED CERTIFICATE
330

FIG. 2B

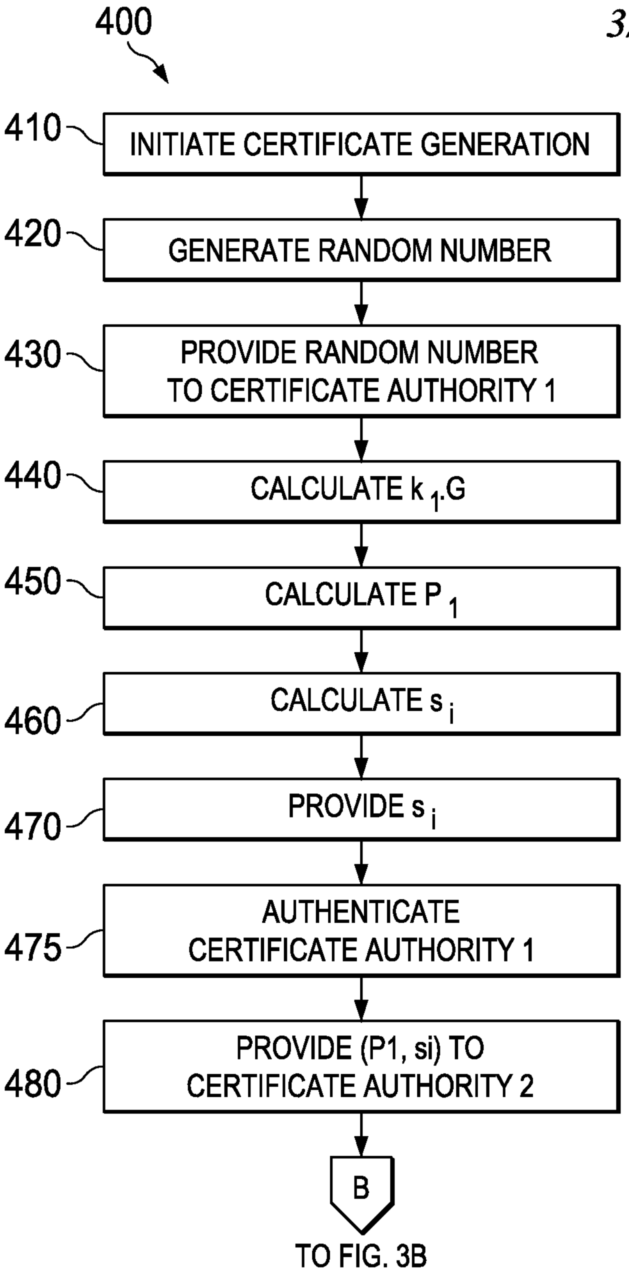

400
410 INITIATE CERTIFICATE GENERATION
420 GENERATE RANDOM NUMBER
430 PROVIDE RANDOM NUMBER TO CERTIFICATE AUTHORITY 1
440 CALCULATE k_1.G
450 CALCULATE P_1
460 CALCULATE s_i
470 PROVIDE s_i
475 AUTHENTICATE CERTIFICATE AUTHORITY 1
480 PROVIDE (P1, si) TO CERTIFICATE AUTHORITY 2
B
TO FIG. 3B

FIG. 3A

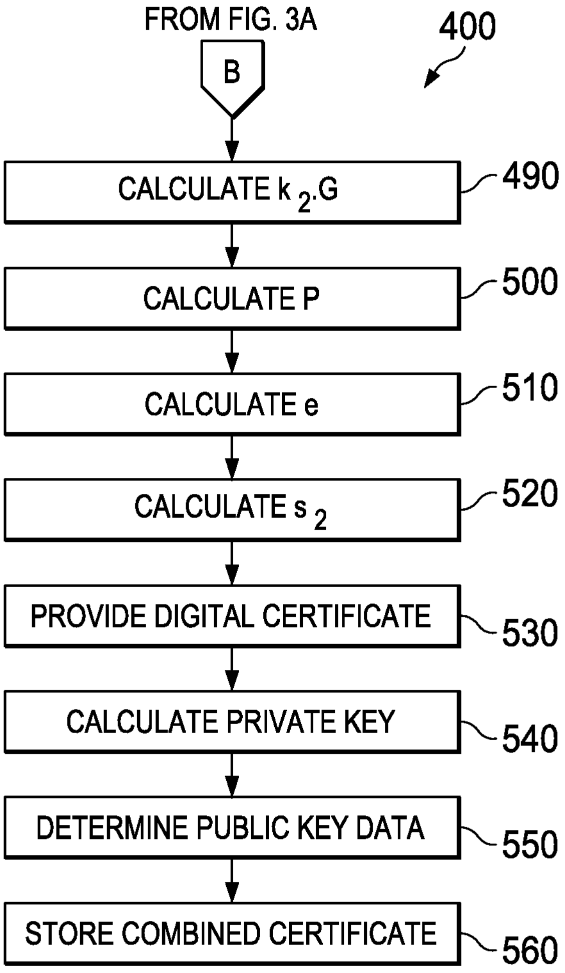

FROM FIG. 3A
B
400
490 CALCULATE k_2.G
500 CALCULATE P
510 CALCULATE e
520 CALCULATE s_2
530 PROVIDE DIGITAL CERTIFICATE
540 CALCULATE PRIVATE KEY
550 DETERMINE PUBLIC KEY DATA
560 STORE COMBINED CERTIFICATE

FIG. 3B

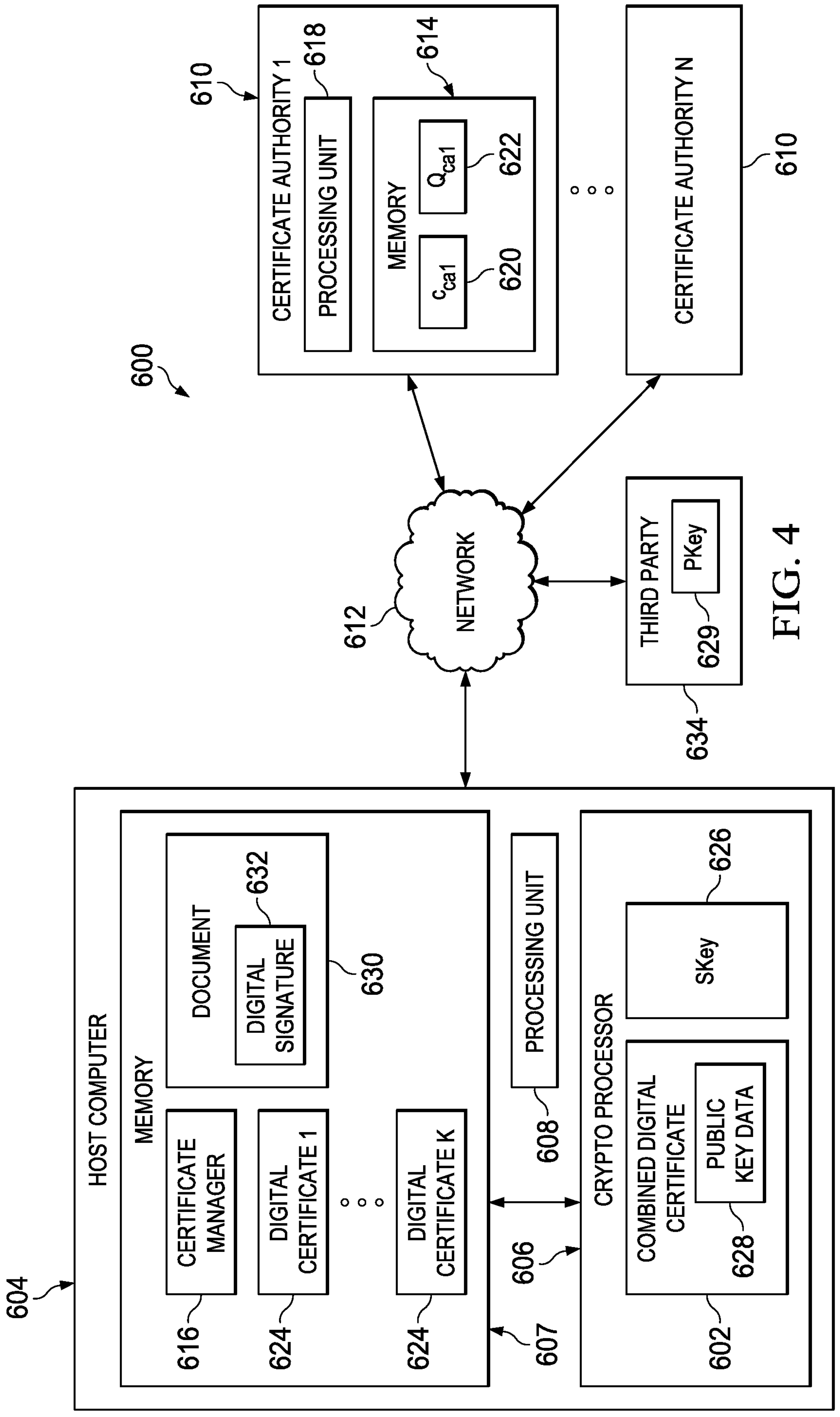

600
610
CERTIFICATE AUTHORITY 1
618
PROCESSING UNIT
614
MEMORY
c_{ca1}
620
Q_{ca1}
622
CERTIFICATE AUTHORITY N
610
612
NETWORK
THIRD PARTY
PKey
629
634
604
HOST COMPUTER
MEMORY
CERTIFICATE MANAGER
616
DIGITAL CERTIFICATE 1
624
DIGITAL CERTIFICATE K
624
DOCUMENT
DIGITAL SIGNATURE
632
630
PROCESSING UNIT
608
607
606
CRYPTO PROCESSOR
SKey
626
COMBINED DIGITAL CERTIFICATE
PUBLIC KEY DATA
628
602

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/070014

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i, H04L 9/20(2006.01)1

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 9/32; H04L 9/08; G06F 3/00; 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: random value, multiple, certificate authority, private key, combined, certificate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2011-0087883 Al (MATTHEW JOHN CAMPAGNA et al.) 14 April 2011 See paragraphs 10-31, 48, 51, 63-71; and figs. 1, 3, 5.	1-19
A	US 2002-0184491 Al (STEPHEN PAUL MORGAN et al.) 05 December 2002 See paragraphs 26-28, 32-38; and figs. 1-5.	1-19
A	US 2003-0115457 Al (MICHAEL ANDREW WILDISH et al.) 19 June 2003 See paragraphs 19-32; and figs. 2, 4, 5.	1-19
A	US 2010-0166188 Al (MINGHUA QU et al.) 01 July 2010 See paragraphs 27-35, 157-163; and figs. 1, 2.	1-19
A	US 2009-0319783 Al (RUSSELL S. THORNTON et al.) 24 December 2009 See paragraphs 23-25, 31, 35-45; and figs. 1, 6, 11.	1-19

□ 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
11 April 2013 (11.04.2013)

Date of mailing of the international search report
12 April 2013 (12.04.2013)

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
KANG, Hee Gok
Telephone No. 82-42-481-8264

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2012/070014

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011-0087883 A1	14.04.2011	CA 2760934 A1	11.11.2010
		EP 2427996 A1	14.03.2012
		WO 2010-129694 A1	11.11.2010
US 2002-0184491 A1	05.12.2002	us 7096362 B2	22.08.2006
US 2003-0115457 A1	19.06.2003	CA 2365441 A1	19.06.2003
		CA 2365441 C	16.02.2010
		US 7103774 B2	05.09.2006
US 2010-0166188 A1	01.07.2010	AU 1999-28235 A1	18.10.1999
		AU 1999-28235 B2	13.03.2003
		CA 2235359 A1	23.09.1999
		CA 2235359 C	10.04.2012
		CA 2320457 A1	24.03.2001
		CA 2320457 C	15.01.2008
		DE 69918818 D1	26.08.2004
		DE 69918818 T2	25.08.2005
		EP 1066699 A1	10.01.2001
		EP 1066699 B1	21.07.2004
		EP 1087148 A1	28.03.2001
		EP 1087148 B1	21.05.2003
		EP 1087148 B9	22.10.2003
		IL 138660 DO	31.10.2001
		JP 03676630 B2	27.07.2005
		JP 03737001 B2	18.01.2006
		JP 04588874 B2	01.12.2010
		JP 2001-090721 A	03.04.2001
		JP 2001-099119 A	10.04.2001
		JP 2001-159412 A	12.06.2001
		JP 2002-508529 A	19.03.2002
		JP 2010-097236 A	30.04.2010
		US 2005-0114651 A1	26.05.2005
		US 2009-0041238 A1	12.02.2009
		US 6334747 B1	01.01.2002
		US 6792530 B1	14.09.2004
		US 7391868 B2	24.06.2008
		US 7653201 B2	26.01.2010
		US 8270601 B2	18.09.2012
		WO 99-49612 A1	30.09.1999
US 2009-0319783 A1	24.12.2009	us 2005-0069136 A1	31.03.2005
		us 2005-0076205 A1	07.04.2005
		us 2005-0081025 A1	14.04.2005
		us 2005-0081027 A1	14.04.2005
		us 2005-0081028 A1	14.04.2005
		us 7568095 B2	28.07.2009
		us 7650496 B2	19.01.2010
		us 7650497 B2	19.01.2010

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2012/070014

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		US 7653810 B2	26.01.2010
		US 7698549 B2	13.04.2010
		US 7937583 B2	03.05.2011