



(51) International Patent Classification:
G06F 11/22 (2006.01) **G06F 11/30** (2006.01)

(21) International Application Number:
PCT/MY2010/000192

(22) International Filing Date:
30 September 2010 (30.09.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 2010001586 9 April 2010 (09.04.2010) MY

(71) Applicant (for all designated States except US): **MIMOS BERHAD** [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **NORAZAH, Abd Aziz** [MY/MY]; C/O Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **LUCYANTIE, Mazalan** [MY/MY]; C/O Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **MOHD, Az-zudin Parman** [MY/MY]; C/O Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **ABDUL, Muzairie Abdul Mutalib** [MY/MY]; C/O Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **PUTRI, Shahnim Khalid** [MY/MY]; C/O Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(74) Agent: **MIRANDAH, Patrick**; Patrick Mirandah CO. (Malaysia) SDN BHD, Suite 3B-19-3 Plaza Sentral, Jalan Stesen Sentral 5, 50470 Kuala Lumpur (MY).

(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.

(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, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))

Published:

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

(54) Title: A METHOD AND SYSTEM FOR A REMOTE ATTESTATION IN A TRUSTED FOUNDATION PLATFORM

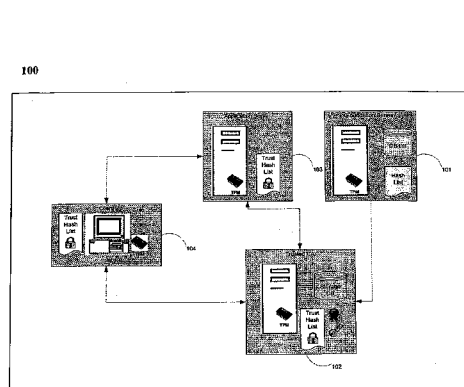


FIG. 1

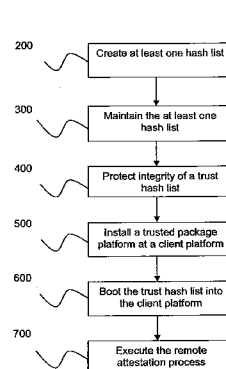


FIG. 2

(57) Abstract: A method and system (100) for providing a remote attestation in a trusted foundation platform through the use of a trust hash list. The system comprising at least one foundation server (101), at least one trusted certificate authority (102), at least one client platform (104) and at least one application server (103). The at least one foundation server (101) having means for creating at least one hash list and maintaining the at least one hash list. The at least one trusted certificate authority (102) having means for protecting integrity of a trust hash list through a certification process available in an installation media package. The at least one client platform (104) having means for installing a trusted package platform and booting the trust hash list. The at least one application server (103) having means for executing the remote attestation process.

A METHOD AND SYSTEM FOR A REMOTE ATTESTATION IN A TRUSTED FOUNDATION PLATFORM

FIELD OF INVENTION

5

The present invention relates to a method and a system for providing a remote attestation in a trusted foundation platform through the use of a trust hash list.

BACKGROUND ART

10

Existing computing platforms stand under various security problems because of the weaknesses in the complexity of the architectural of the configuration of the hardware and software. Thus, Trusted Computing Group (TCG) which develops trusted computing technology came out with a new approach of computing platforms in order to enhance the security of the hardware and software building block.

15

Remote attestation is recommended as an essential feature in Trusted Platform Module (TPM). Remote attestation allows changes to the user's computing platform to be detected by authorized parties wherein the hardware generates a certificate which states the type of software which is currently running. The said computer platform then presents the certificate to a remote party as a proof that the software has not been tampered with. In addition, remote attestation is usually combined with public-key encryption which allows information sent to be read by the programs that presented and requested the attestation and not by a third party (i.e. an eavesdropper).

20

In general, attestation is a process of assuring that information is accurate and is critical for the trusted platform. If a system is not able to attest the accuracy of that information, then the trust to the platform does not exist. Attestation is closely related to authentication. In a networked environment, anonymous authentication access would facilitate the security mechanism. The authentication concept performed by the access requestor requires an access to the facilities without necessarily revealing their identities to external parties. This requirement stems from the possible need for each individual to

25

30

maintain some degree of plausible deniability. One of the approaches to perform this requirement is by using protocols proposed by the said Trusted Computing Group.

The protocol of remote attestation implementation is necessary in order to guarantee the trustworthiness of trusted platform as well as vouching the accuracy of the information
5 and protecting the privacy of the host platform.

The approach of the present invention is an enhanced system and protocol for remote attestation which guarantees the trustworthiness and privacy of remote platform. The present invention involves the creation of the trust hash list.

The subject matter claimed herein is not limited to embodiments that solve any
10 disadvantages or that operate only in environments such as those described above. Rather, this background is only provided to illustrate one exemplary technology area where some embodiments described herein may be practice.

SUMMARY OF INVENTION

One aspect of the present invention is a method for providing a remote attestation in a trusted foundation platform through the use of a trust hash list. The method comprising the steps of creating at least one hash list (200), maintaining the at least one hash list (300), protecting integrity of a trust hash list through a certification process available in an installation media package (400), installing a trusted package platform at a client platform (500), booting the trust hash list into the client platform (600) and executing the remote attestation process (700). The method for maintaining the at least one hash list further comprises the steps of storing the created hash list (302), comparing the hash list with an untrust hash list through a hash operation (304) and removing black list which exists in the hash list to obtain a trust hash list indicating a clean platform (306).

Preferably, the trusted package platform further comprises booting information from the installation media package (502), extracting an endorsement public key from a Trusted Platform Module (504), requesting an endorsement key certificate from a trusted certificate authority (506), receiving the endorsement key certificate and the trust hash list license key (508) and sealing the endorsement key certificate with the client's trusted platform module key (510).

Another aspect of the present invention is a system (100) for providing a remote attestation in a trusted foundation platform through the use of a trust hash list. The system comprising at least one foundation server (101), at least one trusted certificate authority (102), at least one client platform (104) and at least one application server (103). The at least one foundation server (101) having means for creating at least one hash list and maintaining the at least one hash list. The at least one trusted certificate authority (102) having means for protecting integrity of a trust hash list through a certification process available in an installation media package. The at least one client platform (104) having means for installing a trusted package platform and booting the trust hash list. The at least one application server (103) having means for executing the remote attestation process.

Preferably the foundation server (101) further comprises means for storing the created hash list, comparing the hash list with an untrust hash list through a hash operation and

removing black list which exists in the hash list to obtain a trust hash list indicating a clean platform.

5 The present invention consists of features and a combination of parts hereinafter fully described and illustrated in the accompanying drawings, it being understood that various changes in the details may be made without departing from the scope of the invention or sacrificing any of the advantages of the present invention.

BRIEF DESCRIPTION OF ACCOMPANYING DRAWINGS

To further clarify various aspects of some embodiments of the present invention, a more particular description of the invention will be rendered by references to specific embodiments thereof, which are illustrated in the appended drawings. It is appreciated
5 that these drawings depict only typical embodiments of the invention and are therefore not to be considered limiting of its scope. The invention will be described and explained with additional specificity and detail through the accompanying drawings in which:

10 FIG. 1 illustrates system architecture for remote attestation in a trusted foundation platform.

FIG. 2 is a flowchart illustrating a method for providing a remote attestation in a trusted foundation platform through the use of a trust hash list.

15 FIG. 3 is a flowchart illustrating a method for maintaining the at least one hash list.

FIG. 4 is a flowchart illustrating a method for installing a trusted package platform at a client platform.

20 FIG. 5 is a flowchart illustrating a method for booting the trust hash list into the client platform.

FIG. 6 is a flowchart illustrating a method for executing a remote attestation process.

25 FIG. 7 is a flowchart illustrating a method for verifying validity of the remote attestation process.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The invention relate to a method and system for providing a remote attestation in a trusted foundation platform through the use of a trust hash list. Hereinafter, this specification will describe the present invention according to the preferred embodiments. It is to be understood that limiting the description to the preferred embodiments of the invention is merely to facilitate discussion of the present invention and it is envisioned without departing from the scope of the appended claims.

Reference is first being made to FIG. 1. FIG. 1 illustrates architecture of a system for remote attestation in a trusted foundation platform. The system arrangement for remote attestation in a trusted foundation platform comprises four major parts, a Foundation Server (101), a Trusted Certificate Authority (102), a Client Platform (104) and an Application Server (103).

The Foundation Server (101) comprises of a Database List which stores blacklisted data which contains the Database List to store all blacklisted data while the deployment positions a Trusted Certificate Authority (Trusted CA) (102) which contains a Storage Database (Storage DB) to maintain the latest trust hash list, PCR data and certificate for each client platform. A Trusted Platform Module (TPM) is embedded in multiple machine platforms which communicate through a secured channel.

Trust hash list is typically a list of hashes of data blocks in a file or set of files used for different purposes, such as fast table lookup (hash tables) and distributed databases (distributed hash tables) to guarantee data integrity.

Trusted Certificate Authority is a trusted third party provider. Certificate Authorities are characteristic of infrastructure schemes. The present disclosure deploys a Trusted Certificate Authority (102) which functions to manage the mechanism of handling the interoperability and accuracy of the configuration of a computing platform as well as signing the Endorsement Key of trusted platform clients and validates all certificates involved in the attestation process. The attestation mechanism implements a system to maintain the accuracy and interoperability of computing platform configuration by having

the foundation server which interacts with the Trusted Certificate Authority (102) as an entity which handles the trust hash list of an uncompromised foundation server.

The Trusted Certificate Authority (102) comprises a Storage Database which maintains the latest trust hash list, Platform Configuration Registers (PCR) data and certificate for
5 each client platform. Each embodiment may have Trusted Platform Module (TPM) and with communicate each other by a secure channel.

Reference is now being made to FIG. 2 and FIG. 3 collectively. FIG. 2 is a flowchart illustrating a method for providing a remote attestation in a trusted foundation platform through the use of a trust hash list while FIG.3 is a flowchart illustrating a method for
10 maintaining the at least one hash list. The method (100) for providing a remote attestation in a trusted foundation platform through the use of a trust hash list comprising the steps of creating at least one hash list (200), maintaining the at least one hash list (300), protecting integrity of a trust hash list through a certification process available in an installation media package (400), installing a trusted package platform at a client platform
15 (500), booting the trust hash list into the client platform (600) and executing the remote attestation process (700). The method for maintaining the at least one hash list further comprises storing the created hash list (302), comparing the hash list with an untrust hash list through a hash operation (304) and removing black list which exists in the hash list to obtain a trust hash list indicating a clean platform (306). The removal of all
20 blacklisted entries from the database list provides a 'trusted hash' indicating a clean platform. The trust hash list is further sealed and signed by the Trusted Certificate Authority to protect the integrity of the said list.

Reference is now being made to FIG. 4. FIG. 4 is a flowchart illustrating a method for installing a trusted package platform at a client platform. The method for installing a
25 trusted package platform at a client platform further comprises booting information from the installation media package (502). The booting process will invoke a trusted application to extract the endorsement public key from the trusted platform module (504). The application will request for an endorsement certificate (506) by providing an endorsement public key, PCR values of a trusted platform module and serial numbers of
30 the registers to the Trusted Certificate Authority. Subsequently, the endorsement key certificate and the trust hash list license key are sent to the client machine (508).

Thereafter, the endorsement key certificate is sealed with the client's trusted platform module key (510).

Validation of an application is based on a trust hash list which begins when the client platform attempts to execute the application. The installed module will check and
5 compare the hash value of a running application with the hash value of the trust hash list. Reference is now being made to FIG. 5. FIG. 5 is a flowchart illustrating a method for booting the trust hash list into the client platform. If the hash value of that application is listed in the trust hash list then the remote attestation module will initiate the remote attestation process (602). The application can only execute after the module receives the
10 success status of remote attestation. If the matching hash value procedure fails wherein the hash value in the client platform is not in the trust hash list, the module will check the policy regarding severity of hash value and will report the failure of the hash value if (604). Thereafter, the booting process will be terminated if the hash value in the client platform is not in the trust hash list (606).

Reference is now being made to FIG.6 and FIG.7 collectively. FIG. 6 is a flowchart illustrating a method for executing a remote attestation process while FIG. 7 is a flowchart illustrating a method for verifying validity of the remote attestation process. The method for executing a remote attestation process comprises generating attestation parameters at the client platform and a server platform based on information of the endorsement
20 public key (702), forwarding attestation parameters to the trusted certificate authority for endorsement (704), forwarding endorsed attestation parameters to the application server for an attestation process (706) and verifying validity of the remote attestation process (708). The method for verifying validity of the remote attestation process further comprises receiving attestation parameters of the application server (802), identifying a
25 status of the attestation parameters of the application server with the trusted certificate authority (804), reiterating a status check of the attestation parameters of the application server if an invalid status is obtained (806) and terminating the remote attestation process if the status check is invalid (808).

The methodology and system for providing a remote attestation in a trusted foundation
30 platform lies in the content of the trust hash list which is created by comparing a list of data (in the physical machine) against a database of blacklisted data.

The present invention may be embodied in other specific forms without departing from its essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore indicated by the appended claims rather than by the foregoing description. All changes, which come
5 within the meaning and range of equivalency of the claims, are to be embraced within their scope.

CLAIMS

1. A method (100) for providing a remote attestation in a trusted foundation platform through the use of a trust hash list, the method comprising the steps of:

5 creating at least one hash list (200);

 maintaining the at least one hash list (300);

 protecting integrity of a trust hash list through a certification process available in an installation media package (400);

 installing a trusted package platform at a client platform (500);

10 booting the trust hash list into the client platform (600); and

 executing the remote attestation process (700).

characterized in that

maintaining the at least one hash list further comprises the steps of:

 storing the created hash list (302);

15 comparing the hash list with an untrust hash list through a hash operation (304); and

 removing black list which exists in the hash list to obtain a trust hash list indicating a clean platform (306).

- 20 2. A method according to claim 1, wherein installing a trusted package platform at a client platform further comprises the following steps:

 booting information from the installation media package (502);

 extracting an endorsement public key from a Trusted Platform Module (504);

requesting an endorsement key certificate from a trusted certificate authority (506);

receiving the endorsement key certificate and the trust hash list license key (508); and

5 sealing the endorsement key certificate with the client's trusted platform module key (510).

3. A method according to claim 1, wherein booting the trust hash list into the client platform further comprises the following steps:

10 initiating the remote attestation process if the hash value in the client platform is in the trust hash list (602);

reporting failure of the hash value if the hash value in the client platform is not in the trust hash list (604); and

15 terminating the booting process if the hash value in the client platform is not in the trust hash list (606).

4. A method according to claim 1 wherein executing a remote attestation process further comprises the steps of:

20 generating attestation parameters at the client platform and a server platform based on information of the endorsement public key (702);

forwarding attestation parameters to the trusted certificate authority for endorsement (704);

forwarding endorsed attestation parameters to the application server for an attestation process (706); and

25 verifying validity of the remote attestation process (708).

5. A method according to claim 4 wherein verifying validity of the remote attestation process further comprises the steps of:

receiving attestation parameters of the application server (802);

identifying a status of the attestation parameters of the application server with the trusted certificate authority (804);

reiterating a status check of the attestation parameters of the application server if an invalid status is obtained (806); and

terminating the remote attestation process if the status check is invalid (808).

6. A method according to claim 1 wherein the step involve creating multiple hash list and maintaining multiple hash list.

7. A system (100) for providing a remote attestation in a trusted foundation platform through the use of a trust hash list, the system comprising:

at least one foundation server (101);

at least one trusted certificate authority (102);

at least one client platform (104); and

at least one application server (103).

characterized in that

the at least one foundation server (101) having means for:

creating at least one hash list; and

maintaining the at least one hash list.

the at least one trusted certificate authority (102) having means for protecting integrity of a trust hash list through a certification process available in an installation media package;

the at least one client platform (104) having means for:

5 installing a trusted package platform; and

booting the trust hash list.

the at least one application server (103) having means for executing the remote attestation process.

10 8. A system (100) according to claim 7 wherein the at least one foundation server (101) further comprises means for:

storing the created hash list;

comparing the hash list with an untrust hash list through a hash operation; and

15 removing black list which exists in the hash list to obtain a trust hash list indicating a clean platform.

9. A system according to claim 7 wherein the at least one client platform (104) having means for:

20 booting information from the installation media package;

extracting an endorsement public key from a Trusted Platform Module;

requesting an endorsement key certificate from a trusted certificate authority;

25 receiving the endorsement key certificate and the trust hash list license key; and

sealing the endorsement key certificate with the client's trusted platform module key.

10. A system according to claim 7 wherein the at least one client platform (104)
5 further comprises means for:

generating attestation parameters based on information of the endorsement public key;

forwarding attestation parameters to the trusted certificate authority for endorsement;

10 forwarding endorsed attestation parameters to the application server for an attestation process; and

verifying validity of the remote attestation process.

11. A system according to claim 7 wherein the at least one trusted certificate authority
15 (102) further comprises means for:

receiving attestation parameters of the application server;

identifying a status of the attestation parameters of the application server with the trusted certificate authority;

20 reiterating a status check of the attestation parameters of the application server if an invalid status is obtained; and

terminating the remote attestation process if the status check is invalid.

12. The system according to claim 7 and claim 9 wherein the at least one client platform (104) further comprising means for:

initiating the remote attestation process if the hash value in the client platform is in the trust hash list;

5 reporting failure of the hash value if the hash value in the client platform is not in the trust hash list; and

terminating the booting process if the hash value in the client platform is not in the trust hash list.

10 13. A system according to claim 7 wherein the step involve creating multiple hash list and maintaining multiple hash list.

1/5

100

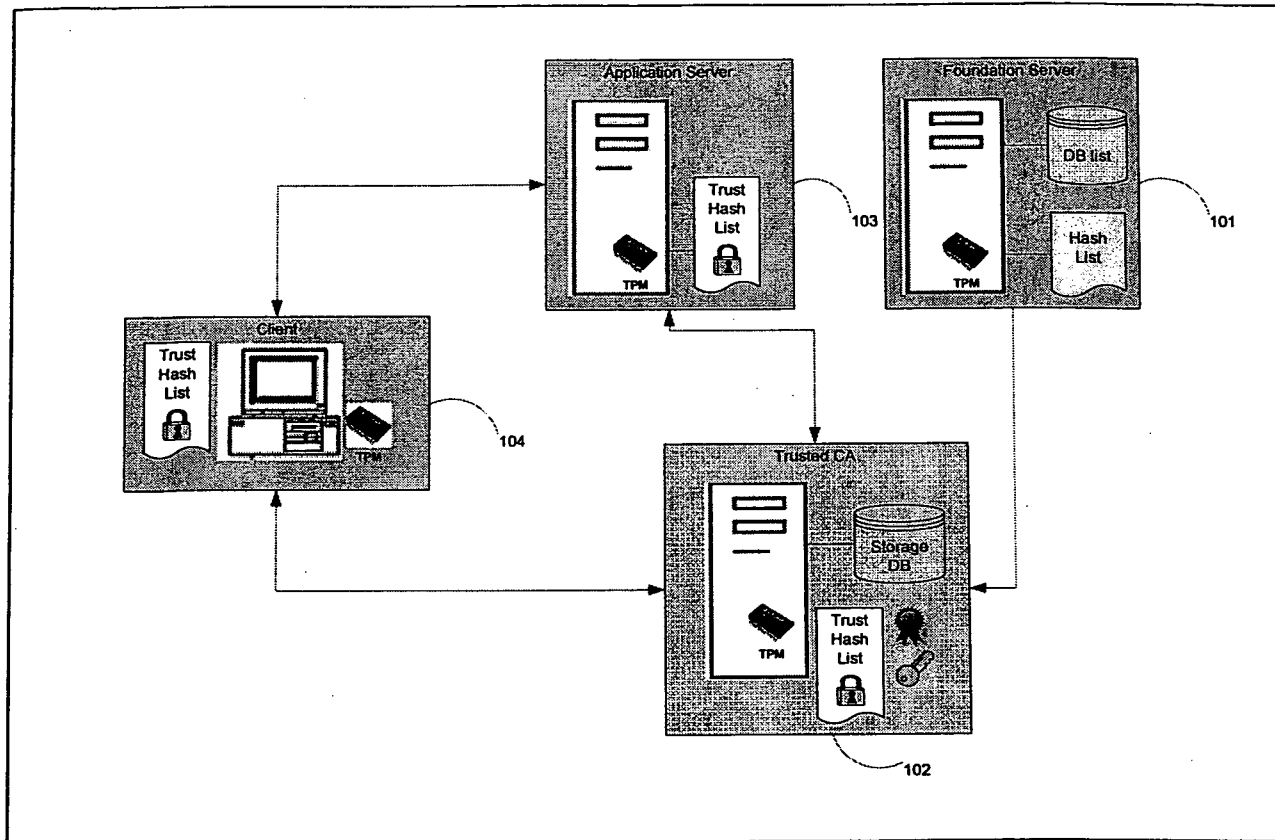


FIG.1

2/5

100

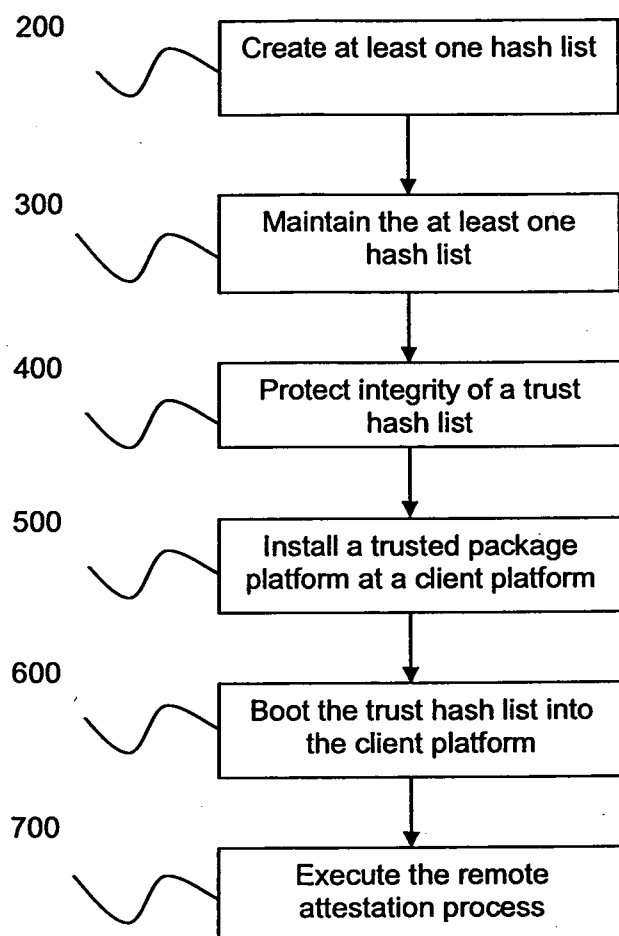


FIG. 2

3/5

300

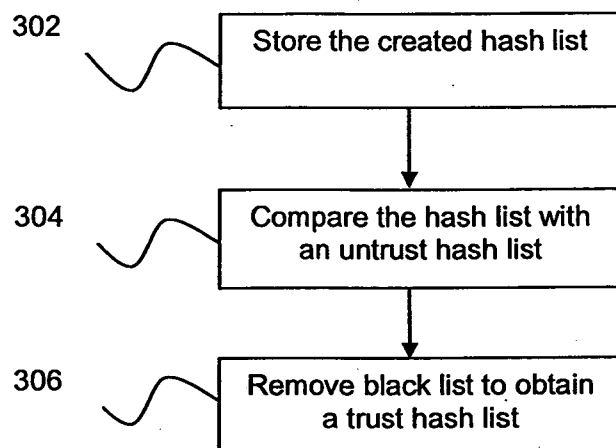


FIG. 3

500

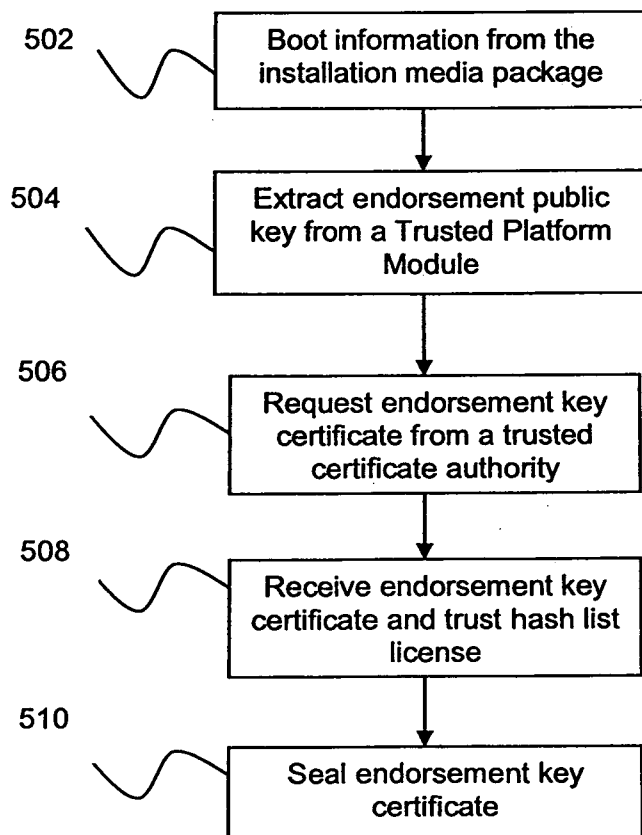


FIG. 4

4/5

600

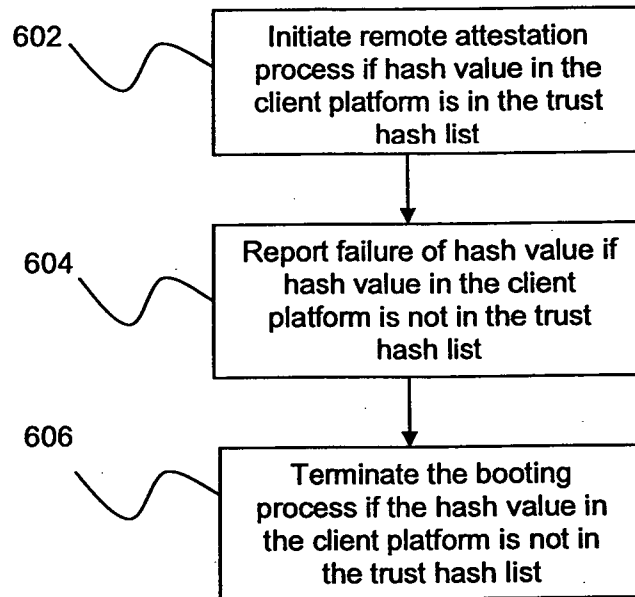


FIG. 5

700

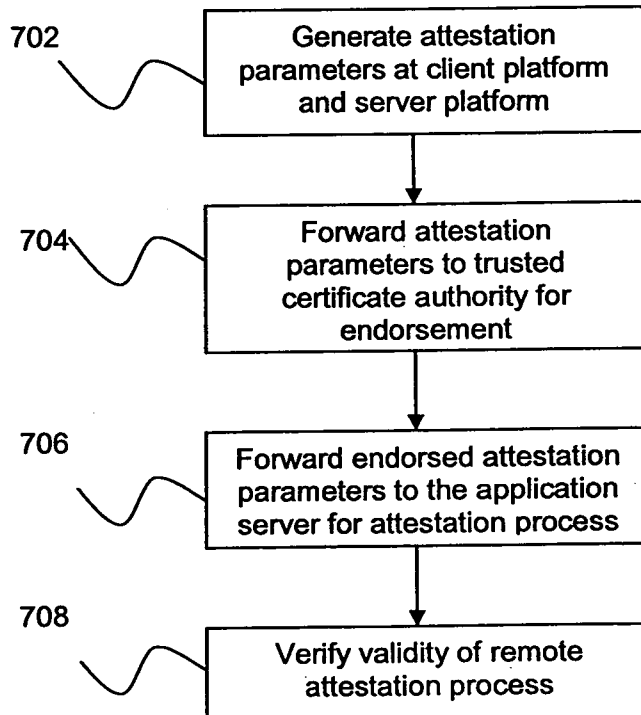


FIG. 6

5/5

800

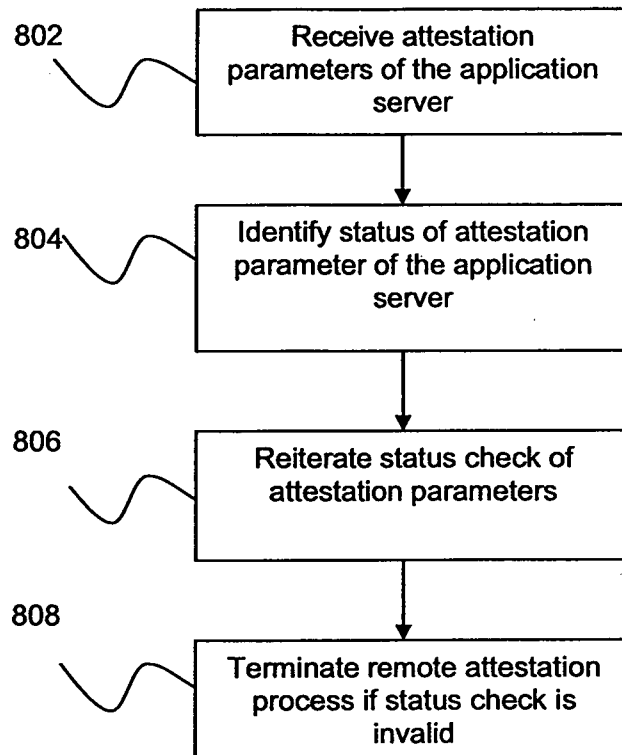


FIG. 7

A. CLASSIFICATION OF SUBJECT MATTER**G06F 11/22(2006.01)i, G06F 11/30(2006.01)i**

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 11/22; G06F 7/00; H04L 9/00; G06F 9/00; G08B 23/00; G06F 21/00

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: hash list, black list, certification, client, server

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2007-0136814 A1 (MICHAEL LEE et al.) 14 June 2007 See abstract; paragraph 10 - paragraph 23 and figures 1-4	1-13
A	US 6574729 B1 (PAUL ERNEST FINK et al.) 03 June 2003 See abstract; column 3 line 31 - column 5 line 27 and figures 1,2	1-13
A	US 2006-0005009 A1 (CHARLES D. BALL et al.) 05 January 2006 See abstract; paragraph 24 - paragraph 42 and figures 1,2	1-13
A	US 2010-0058431 A1 (BRUCE MCCORKENDALE et al.) 04 March 2010 See abstract; paragraph 9 - paragraph 13 and figure 1	1-13



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

03 MAY 2011 (03.05.2011)

Date of mailing of the international search report

01 JUNE 2011 (01.06.2011)

Name and mailing address of the ISA/KR

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

Facsimile No. 82-42-472-7140

Authorized officer

KIM, JONG TAEK

Telephone No. 042 481 5983



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/MY2010/000192

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007-0136814 A1	14.06.2007	None	
US 6574729 B1	03.06.2003	US 2003-0140266 A1	24.07.2003
US 2006-0005009 A1	05.01.2006	None	
US 2010-0058431 A1	04.03.2010	EP 2164016 A1	17.03.2010
		JP 2010-113705 A	20.05.2010