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

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

(43) **International Publication Date**
6 June 2013 (06.06.2013)

WIPO | PCT

(10) **International Publication Number**
WO 2013/081441 Al

(51) **International Patent Classification:**
H04L 29/06 (2006.01) *G06F 21/00* (2013.01)

(21) **International Application Number:**
PCT/MY20 12/000160

(22) **International Filing Date:**
28 June 2012 (28.06.2012)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
PI 201 1005855 2 December 201 1 (02. 12.201 1) 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). **SHARIPAH, Setapa** [MY/MY]; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **MOHD, Aminud-in, Mohd, Khalid** [MY/MY]; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **KILAUSURIA, Abdullah** [MY/MY]; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY).

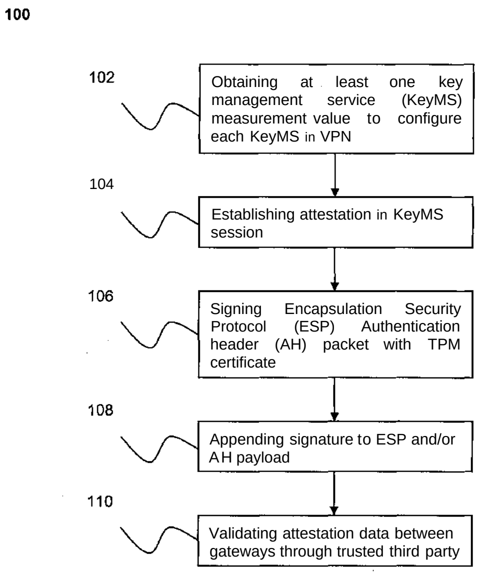
(74) **Agent: MIRANDAH, Patrick;** Patrick Mirandah Co. (Malaysia) sd. bhd, Suite 3B-19-3, Plaza Sentral, Jalan Stesen Sentral 5, 50470 Kuala Lumpur (MY).

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

(84) **Designated States** ***(unless otherwise indicated, for every kind 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:** A SYSTEM AND METHOD FOR ESTABLISHING MUTUAL REMOTE ATTESTATION IN INTERNET PROTOCOL SECURITY (IPSEC) BASED VIRTUAL PRIVATE NETWORK (VPN)


100
102
Obtaining at least one key management service (KeyMS) measurement value to configure each KeyMS in VPN
104
Establishing attestation in KeyMS session
106
Signing Encapsulation Security Protocol (ESP) Authentication header (AH) packet with TPM certificate
108
Appending signature to ESP and/or AH payload
110
Validating attestation data between gateways through trusted third party

(57) **Abstract:** The system and method of the present invention proposes an extension to the IPSec key exchange protocol by establishing properties-based attestation using key management service. The present invention protects integrity between network encryptor of sender-receiver/gateway to gateway platform machine by measuring properties which bundles with IPSec based VPN network. The system of the present invention comprising at least one sender and receiver platform; IPsec components extension; a plurality of properties of remote attestation modules (600); at least one signer mechanism (602); and at least one TPM (604). The methodology of the present invention establishes mutual remote attestation in IPSec based VPN by obtaining at least one key management service (KeyMS) measurement value to configure each KeyMS in VPN (102); establishing attestation in KeyMS session (104); signing Encapsulation Security Protocol (ESP) Authentication header (AH) packet with TPM certificate (106); appending signature to ESP and/or AH payload (108) and validating attestation data between gateways through trusted third party (110).

Declarations under Rule 4.17:

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

— *of inventorship (Rule 4.17(iv))*

Published:

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

A SYSTEM AND METHOD FOR ESTABLISHING MUTUAL REMOTE ATTESTATION IN INTERNET PROTOCOL SECURITY (IPSEC) BASED VIRTUAL PRIVATE NETWORK (VPN)

FIELD OF INVENTION

The present invention relates to a system and method for establishing mutual remote attestation in Internet Protocol security (IPSec) based virtual private network (VPN).

BACKGROUND ART

Secure communication between computer systems is typically established using secure channel technologies such as Secure Socket layer (SSL) or IPSec. While these protocols ensure secure transmission of data and authenticity of the communication at each gateway, they do not provide any guarantee on the integrity of the involved endpoints. It is highly desirable to ensure trustworthiness of the involved remote party, i.e., to have assurance that the remote system adapt to a defined policy.

Secure remote assessment of a remote system's state is called remote attestation. It involves a mutually trusted attestor to assure that the possibly compromised system cannot lie about its current state. The attestor vouches for the correctness of the attestation data transmitted in one or more attestation reports. The Trusted Computing Group (TCG) has introduced Trusted computing Infrastructure to solve this issue into the mainstream computer industry. Trusted Platform Module (TPM) is a security module which has been designed to securely store and report a record of system events as well as the key component in the remote attestation realization.

Attestation is closely related to authentication. In the network environment, anonymous authentication access could facilitate the security mechanism. Trusted Computing Platform (TCP) provides a mechanism that supports the attestation by its Platform Configuration Registers (PCR) which has become the integrity measurement of a platform. This PCR values are meant to be protected during the attestation transaction. Normally, we have to setup configuration before any communication establish. The configuration means any authorization mechanism such as username and password at host. Since everyone can use the host, so they can trace the username and password, hence change the configuration without notice by the owner of the host. Due to that, hosts still lack the capability to remotely verify the hardware, operating system, or other software running. This leads to host vulnerabilities in operating system. So, trusted platform module (TPM) by using attestation approach, attempts to solve this deficiency using secure hardware and public-private key-pair as well as module responsible in verifying the trustworthiness of the system.

IPSec is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. IPsec is more secure as it protects application traffic across IP network. However, the issue of embedded attestation for verification and validation is not being addressed in IPSec protocol family under network layer in Open System Interconnection (OSI) stack.

The present invention proposes an extension to the IPSec key exchange protocol by establishing properties-based attestation using key management service. An embedded attestation extension is provided in VPN communication such as IPSec protocol by establishing mutual properties based attestation using key management service (KeyMS) measurement value as properties. The present invention protects integrity between network encryptor of sender-receiver/gateway to gateway platform machine by measuring properties which bundles with IPSec based VPN network.

The value of Internet key Exchange (IKE) management service of the present invention is base on security policy database which was initiated and agreed by each endpoint. Then, it computes as integrity measurement value and store in Platform Configuration Register (PCR) at TPM. Before the Internet Key Exchange (IKE) session establish, remote attestation process (which generate TPM key/certificate, compute and compare the integrity measurement based on extended PCR) is running to check the accuracy of the attestation data of both involved parties. IPSec establishes connection with remote host when each host trusts each other.

During communication, the Encapsulation Security Protocol (ESP) auth field in ESP header and Authentication Header (AH) field in AH header are construct by signing with

TPM certificate. During data transfer, the desired fields are validated with any mechanism such as Privacy CA or DAA. The approach of the present invention resides in layer 3, the network layer of the OSI stack.

The subject matter claimed herein is not limited to embodiments that solve any 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

The present invention provides a system for establishing mutual remote attestation in IPSec based VPN. The system comprising at least one sender and receiver platform; IPsec components extension; a plurality of properties of remote attestation modules (600); at least one signer mechanism (602); and at least one TPM (604).

IPSec components extension of the VPN establishes mutual remote attestation by obtaining at least one key management service (KeyMS) measurement value to configure each KeyMS in VPN; establishing attestation in KeyMS session; signing Encapsulation Security Protocol (ESP) Authentication header (AH) packet with TPM certificate; appending signature to ESP and/or AH payload; and validating attestation data between gateways through trusted third party. The plurality of properties of remote attestation modules (600) establishes mutual remote attestation by initiating properties remote attestation to generate integrity measurement based on at least security policy database from KeyMS; generating trusted platform module (TPM) key based endorsement and platform certificate; computing integrity measurement of remote host by sending data to any signer for validation; and comparing integrity measurement between source and destination with any signing mechanism component during KeyMS negotiation process. The at least one signer mechanism (602) establishes mutual remote attestation by signing attestation data; and validating attestation data between respective gateways using trusted third party.

Another aspect of the present invention provides a method (100) for establishing mutual remote attestation in IPSec based VPN. The method comprising steps of obtaining at least one key management service (KeyMS) measurement value to configure each KeyMS in VPN (102); establishing attestation in KeyMS session (104); signing Encapsulation Security Protocol (ESP) Authentication header (AH) packet with TPM certificate (106); and appending signature to ESP and/or AH payload (108). The method of appending signature to ESP and/or AH payload further comprises validating attestation data between gateways through trusted third party (110).

A further aspect of the present invention is a method for obtaining at least one key management service (KeyMS) measurement value to configure each KeyMS in VPN. The said method further comprising generating core policy based on VPN tunnel configurations agreed by each gateway (202); generating core properties based attestation value based on said core policy (204); storing said core properties into PCR entend (204); encrypting core policy with any key (206); and storing encrypted core policy at secure storage by each gateway (206).

Another aspect of the present invention is a method for establishing attestation in KeyMS session. The said method further comprising initiating properties remote attestation to generate integrity measurement based on at least security policy database from KeyMS (302); generating trusted platform module (TPM) key based endorsement and platform certificate (304); computing integrity measurement of remote host by sending data to any signer for validation (306); and comparing integrity measurement between source and destination with any signing mechanism component during KeyMS negotiation process (308).

A further aspect of the present invention is a method for comparing integrity measurement between source and destination with any signing mechanism component during KeyMS negotiation process. The said method further comprising generating properties-based attestation hash value based on core policy if validation is valid (310); generating trusted platform module (TPM) key based endorsement and platform certificate (31 2); computing integrity measurement of remote gateway by sending data to any signer for validation (314); sending response to remote gateway if verification and validation are valid (316); sending final status to host gateway after verification (318); and establishing secure communication between gateways by signing IPSec based VPN through TPM cert (320).

A further aspect of the present invention is signing Encapsulation Security Protocol (ESP) Authentication header (AH) packet with TPM certificate. The said method further comprising verifying expiry of TPM certificate based on scheduler timestamp (402); maintaining establishment of attestation in KeyMS session if TPM certificate is expired (404); getting encrypted TPM from secure storage if TPM certificate is valid (406); signing IPSec data which consist of AH header and ESP header with TPM certificate (408); sending modified IPSec data and PCR hash value to remote gateway (410); verifying modified IPSec data and PCR hash value with signer at remote gateway (412); sending modified IPSec data to respond to host gateway while iterating step 402, 404 and 406 (414); verifying modified IPSec data and hash value with signer by host gateway (416); and accepting IPSec data from remote gateway if verification is valid (420).

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 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:

FIG. 1 is a flowchart illustrating a method for establishing mutual remote attestation in IPSec based VPN.

FIG. 2 is a flowchart illustrating a method for obtaining at least one key management service (KeyMS) measurement value to configure each KeyMS in VPN.

FIG. 3 is a flowchart illustrating a method for establishing attestation in KeyMS session.

FIG. 4 is a flowchart illustrating a method for signing Encapsulation Security Protocol (ESP) Authentication header (AH) packet with TPM certificate.

FIG. 5 illustrates the present invention which resides in the network layer (layer 3) of the OSI Stack.

FIG. 6 illustrates attestation service module in IPSec based VPN attestation service module in IPSec based VPN.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention provides a system and method for establishing mutual remote attestation in Internet Protocol Security (IPSec) based virtual private network (VPN). 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. 5 and FIG. 6 respectively. FIG. 1 is a flowchart illustrating a method for establishing mutual remote attestation in IPSec based VPN while FIG. 5 illustrates the present invention which resides in the network layer (layer 3) of the open systems interconnection (OSI) Stack and FIG. 6 illustrates attestation service module in IPSec based VPN attestation service module in IPSec based VPN. As illustrated in FIG. 5, the present invention proposes an extension to the IPSec key exchange protocol by establishing properties-based attestation using key management service which resides in layer 3 (network layer) of the OSI stack. The system of the present invention comprising at least one sender and receiver platform; IPsec components extension; a plurality of properties of remote attestation modules (600); at least one signer mechanism (602); and at least one trusted platform module (TPM) (604).

The system and method for establishing mutual remote attestation through IPSec components extension of the VPN in IPSec based VPN begins by obtaining at least one key management service (KeyMS) measurement value to configure each KeyMS in VPN (102). Thereafter, attestation is established in KeyMS session (104). Encapsulation Security Protocol (ESP) Authentication header (AH) packet is signed with TPM certificate (106) and signature is appended to ESP and/or AH payload (108). Thereafter, attestation data is validated between gateways through trusted third party (110).

Reference is now being made to FIG. 2. FIG. 2 is a flowchart illustrating a method for obtaining at least one key management service (KeyMS) measurement value to configure each KeyMS in VPN. The process starts by generating core policy based on VPN tunnel configurations using key management service (KeyMS) (202). The said core policy is generated based on system environment and requirement of each platform, hence it is agreed by each platform. After generating core policy, core properties based attestation value is automatically generated based on the core policy and store the hash value into platform configuration register (PCR) extend at trusted platform module (TPM)/virtual trusted platform module (vTPM) (204). The core policy must be encrypted by each host with any generated key either using TPM/vTPM. Thereafter, the encrypted core policy is stored at secure storage at each gateway or specifically stores it only at third party signer (206).

Reference is now being made to FIG. 3. FIG. 3 is a flowchart illustrating a method for establishing attestation in KeyMS session. A plurality of properties of remote attestation modules establish mutual remote attestation by initiating properties remote attestation to generate integrity measurement based on at least security policy database from KeyMS (302). Hash property value is based on core` policy and needs to be verified with any signer which compares it with the core properties hash value. If the verification is valid, gateway receives TPM certificate while IKE launches negotiation by sending request of gateway network ID (NeID), nonce and the properties hash values.

Thereafter, trusted platform module (TPM) key based endorsement and platform certificate is generated (304) in which all data is encrypted with TPM certificate before sending to other gateway (i.e. Gateway B). Integrity measurement of remote host is computed by sending data to any signer for validation (306) wherein Gateway B sends data to any signer for validation purposes. The signer consist of trusted third party or TPM/vTPM itself and comparing integrity measurement between source and destination with any signing mechanism component during KeyMS negotiation process (308). At least one signer mechanism establishes mutual remote attestation by signing attestation data and validating attestation data between respective gateways using trusted third party.

Gateway B generates its own properties-based attestation hash value based on core policy if validation is valid (310). Thereafter, trusted platform module (TPM) key based endorsement and platform certificate is generated (312) in which all data is encrypted with TPM certificate before sending to other gateway (i.e. Gateway A). Gateway A computes integrity measurement of remote gateway by sending data to any signer for validation (314). If verification and validation are valid, then Gateway A sends response to remote gateway (i.e. Gateway B). Final status is sent to host gateway (i.e. Gateway A) after verification (318) and secure communication is establish between gateways by signing IPSec based VPN through TPM cert (320).

Reference is now being made to FIG. 4. FIG. 4 is a flowchart illustrating a method for signing Encapsulation Security Protocol (ESP) Authentication header (AH) packet with TPM certificate. The validation and verification process through IPSec communication channel is illustrated in FIG. 4. Expiry of TPM certificate is verified based on scheduler timestamp at Gateway A (402). If TPM certificate is expired, the establishment of attestation in KeyMS session (320-320) continues.

Else, the process continues by getting encrypted TPM from secure storage if TPM certificate is valid (406). Thereafter, it will be signed with IPSec data which consist of AH header and ESP header with TPM certificate (408). The modified IPSec data and PCR hash value is sent to the remote gateway (i.e. Gateway B) (410). Modified IPSec data and PCR hash value is verified with signer at remote gateway (i.e. Gateway B) (412). If the verification is valid, repeat process (402, 404 and 406) and send modified IPSec data to respond to host gateway (414).

At Gateway A, signer verifies modified IPSec data and hash value (416) and if the verification is not valid, fail status will be sent. If the verification is valid, Gateway A accepts IPSec data from remote gateway (i.e. Gateway B)(420).

After establishing the attestation process, IKE service A or IKE service B can send data to each other. IPsec communication starts using TPM key in its ESP header and AH header. IKE service A or IKE service B verifies the TPM cert each time data arrives. The finger print of payload is signed with TPM key to generate signature as shown below:

$$\boxed{\text{sign(hash(payload), } \text{TPM}_{\text{KEY}}\text{)}}$$

For deployment, the Integrity Check Value in Authentication header and Encapsulation Security Protocol support multiple of 32 bits. Alternatively, translator is used to encapsulate IPSec with attestation within normal packet and de-capsulate to obtain IPSec with attestation packet.

The system and method of the present invention proposes an extension to the IPSec key exchange protocol by establishing properties-based attestation using key management service. An embedded attestation extension is provided in VPN communication such as IPSec protocol by establishing mutual properties based attestation using key management service (KeyMS) measurement value as properties. The present invention protects integrity between network encryptor of sender-receiver/gateway to gateway platform machine by measuring properties which bundles with IPSec based VPN network.

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 within the meaning and range of equivalency of the claims, are to be embraced within their scope.

CLAIMS

1. A method (100) for establishing mutual remote attestation in IPSec based VPN, the method comprising steps of:

   obtaining at least one key management service (KeyMS) measurement value to configure each KeyMS in VPN (102);

   establishing attestation in KeyMS session (104);

   signing Encapsulation Security Protocol (ESP) Authentication header (AH) packet with TPM certificate (106); and

   appending signature to ESP and/or AH payload (108)

   characterized in that

   appending signature to ESP and/or AH payload further comprises validating attestation data between gateways through trusted third party (110).

2. A method according to claim 1, wherein obtaining at least one key management service (KeyMS) measurement value to configure each KeyMS in VPN further comprising:

   generating core policy based on VPN tunnel configurations agreed by each gateway (202);

   generating core properties based attestation value based on said core policy (204);

   storing said core properties into PCR extend (204);

   encrypting core policy with any key (206); and

   storing encrypted core policy at secure storage by each gateway (206).

3. A method according to claim 1, wherein establishing attestation in KeyMS session further comprising:

   initiating properties remote attestation to generate integrity measurement based on at least security policy database from KeyMS (302);

   generating trusted platform module (TPM) key based endorsement and platform certificate (304);

   computing integrity measurement of remote host by sending data to any signer for validation (306); and comparing integrity measurement between source and destination with any signing mechanism component during KeyMS negotiation process (308).

4. A method according to claim 3 wherein comparing integrity measurement between source and destination with any signing mechanism component during KeyMS negotiation process further comprising:

generating properties-based attestation hash value based on core policy if validation is valid (310);

generating trusted platform module (TPM) key based endorsement and platform certificate (312);

computing integrity measurement of remote gateway by sending data to any signer for validation (314);

sending response to remote gateway if verification and validation are valid (316);

sending final status to host gateway after verification (318); and

establishing secure communication between gateways by signing IPSec based VPN through TPM cert (320).

5. A method according to claim 1, wherein signing Encapsulation Security Protocol (ESP) Authentication header (AH) packet with TPM certificate further comprising:

verifying expiry of TPM certificate based on scheduler timestamp (402);

maintaining establishment of attestation in KeyMS session if TPM certificate is expired (404);

getting encrypted TPM from secure storage if TPM certificate is valid (406);

signing IPSec data which consist of AH header and ESP header with TPM certificate (408);

sending modified IPSec data and PCR hash value to remote gateway (410);

verifying modified IPSec data and PCR hash value with signer at remote gateway (412);

sending modified IPSec data to respond to host gateway while iterating step 402, 404 and 406 (414);

verifying modified IPSec data and hash value with signer by host gateway (416); and

accepting IPSec data from remote gateway if verification is valid (420).

6. A method according to claim 1, wherein KeyMS configuration consist of security policy for IPSec tunnel.

7. A system for establishing mutual remote attestation in IPSec based VPN, the system comprising:

at least one sender and receiver platform;

IPsec components extension;

a plurality of properties of remote attestation modules (600);

at least one signer mechanism (602); and

at least one TPM (604).

8. A system according to claim 6, wherein IPSec components extension of the VPN establish mutual remote attestation by:

obtaining at least one key management service (KeyMS) measurement value to configure each KeyMS in VPN;

establishing attestation in KeyMS session;

signing Encapsulation Security Protocol (ESP) Authentication header (AH) packet with TPM certificate;

appending signature to ESP and/or AH payload; and

validating attestation data between gateways through trusted third party.

9. A system according to claim 6, wherein a plurality of properties of remote attestation modules (600) establish mutual remote attestation by:

initiating properties remote attestation to generate integrity measurement based on at least security policy database from KeyMS;

generating trusted platform module (TPM) key based endorsement and platform certificate;

computing integrity measurement of remote host by sending data to any signer for validation; and comparing integrity measurement between source and destination with any signing mechanism component during KeyMS negotiation process.

10. A system according to claim 6, wherein at least one signer mechanism (602) establish mutual remote attestation by:

signing attestation data; and

validating attestation data between respective gateways using trusted third party.

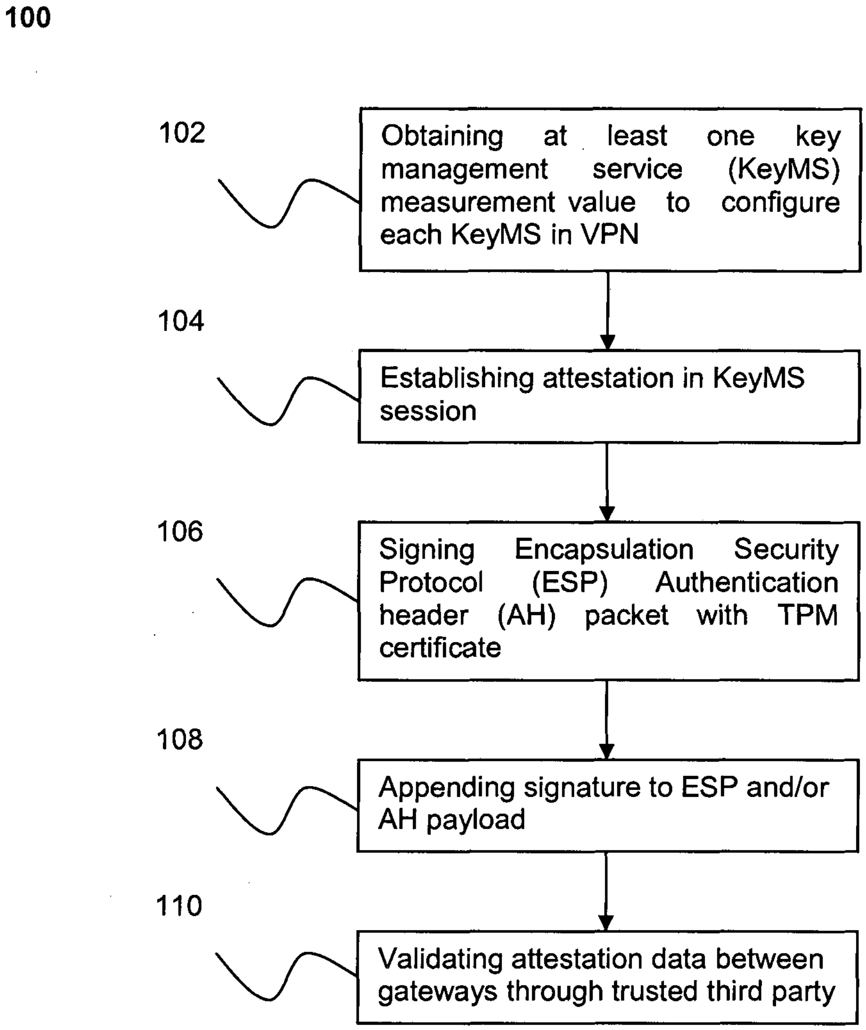

100
102
Obtaining at least one key management service (KeyMS) measurement value to configure each KeyMS in VPN
104
Establishing attestation in KeyMS session
106
Signing Encapsulation Security Protocol (ESP) Authentication header (AH) packet with TPM certificate
108
Appending signature to ESP and/or AH payload
110
Validating attestation data between gateways through trusted third party

FIG. 1

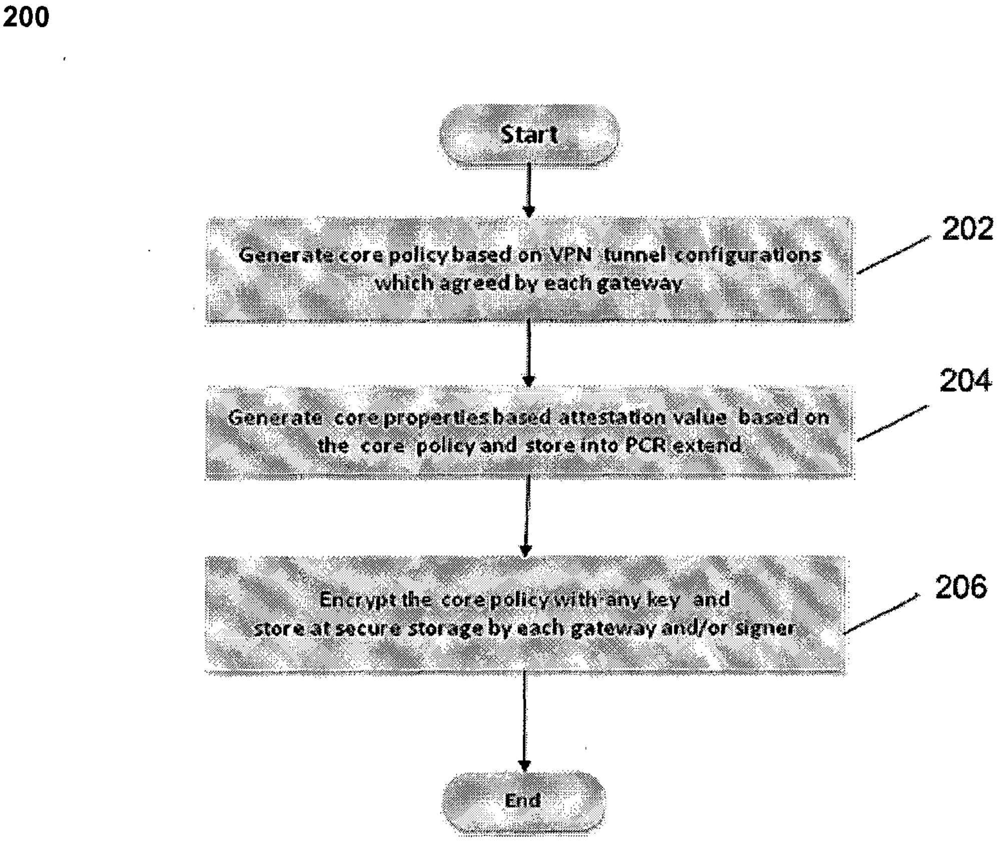
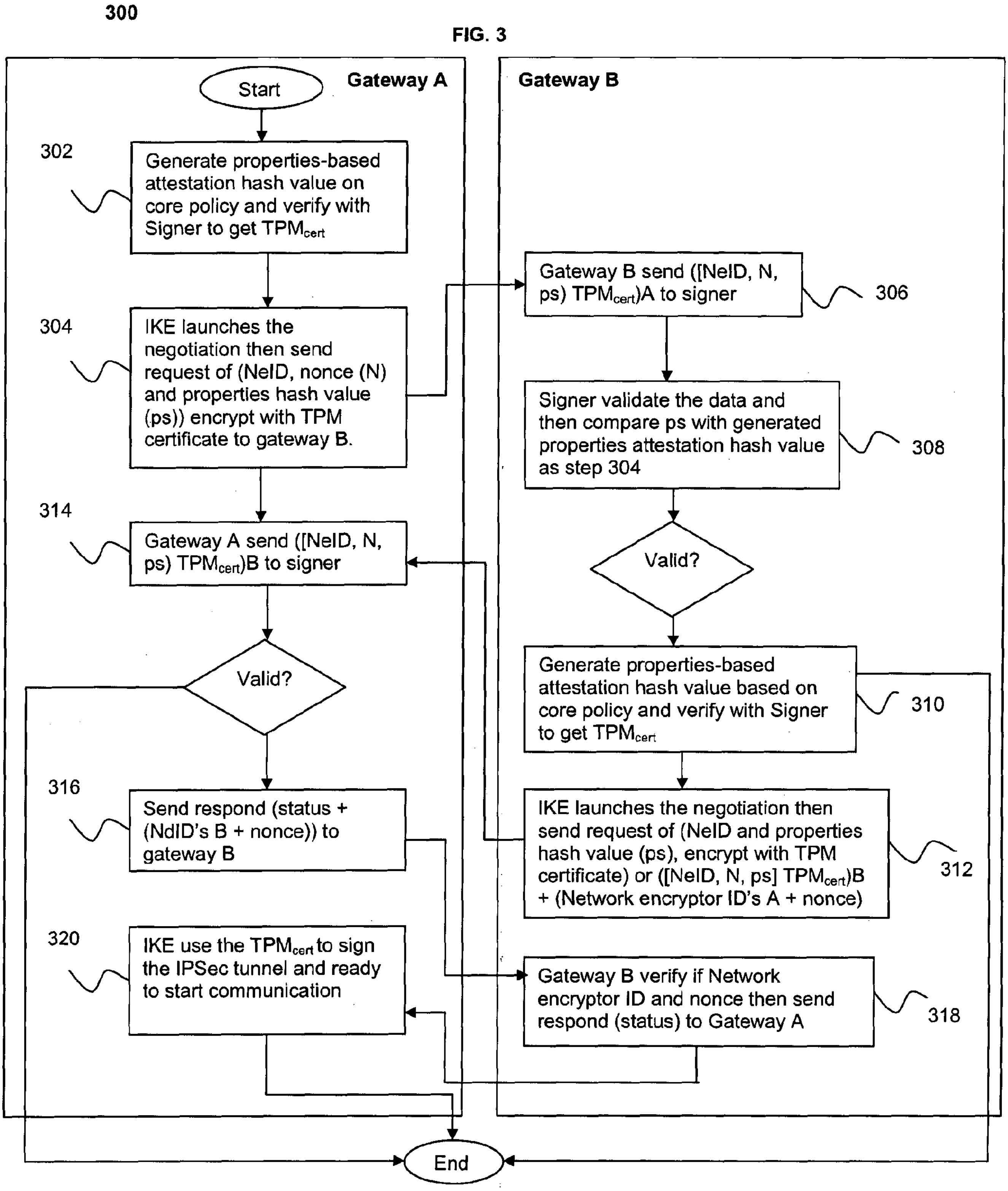

200
Start
Generate core policy based on VPN tunnel configurations which agreed by each gateway
202
Generate core properties based attestation value based on the core policy and store into PCR extend
204
Encrypt the core policy with any key and store at secure storage by each gateway and/or signer
206
End

FIG. 2

FIG. 3


300
Gateway A
Gateway B
Start
302
Generate properties-based attestation hash value on core policy and verify with Signer to get TPM_{cert}
304
IKE launches the negotiation then send request of (NeID, nonce (N) and properties hash value (ps)) encrypt with TPM certificate to gateway B.
306
Gateway B send ([NeID, N, ps) TPM_{cert})A to signer
308
Signer validate the data and then compare ps with generated properties attestation hash value as step 304
Valid?
310
Generate properties-based attestation hash value based on core policy and verify with Signer to get TPM_{cert}
312
IKE launches the negotiation then send request of (NeID and properties hash value (ps), encrypt with TPM certificate) or ([NeID, N, ps] TPM_{cert})B + (Network encryptor ID's A + nonce)
314
Gateway A send ([NeID, N, ps) TPM_{cert})B to signer
Valid?
316
Send respond (status + (NdID's B + nonce)) to gateway B
318
Gateway B verify if Network encryptor ID and nonce then send respond (status) to Gateway A
320
IKE use the TPM_{cert} to sign the IPSec tunnel and ready to start communication
End

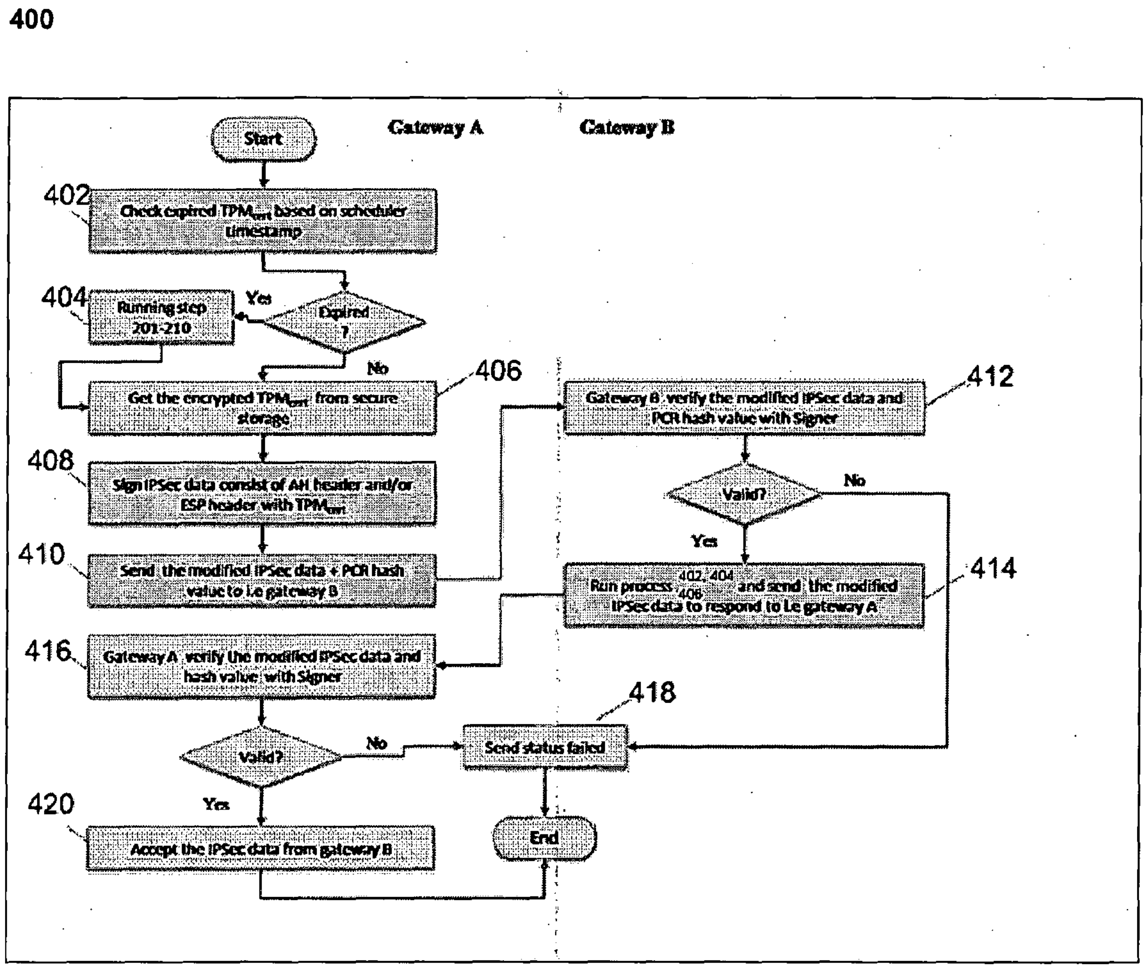

400
Gateway A
Gateway B
Start
402
Check expired TPM$_{cert}$ based on scheduler timestamp
Expired ?
Yes
404
Running step 201-210
No
406
Get the encrypted TPM$_{cert}$ from secure storage
408
Sign IPSec data consist of AH header and/or ESP header with TPM$_{cert}$
410
Send the modified IPSec data + PCR hash value to i.e gateway B
412
Gateway B verify the modified IPSec data and PCR hash value with Signer
Valid?
No
Yes
414
Run process 402, 404 406 and send the modified IPSec data to respond to i.e gateway A
416
Gateway A verify the modified IPSec data and hash value with Signer
Valid?
No
418
Send status failed
Yes
420
Accept the IPSec data from gateway B
End

FIG. 4

500

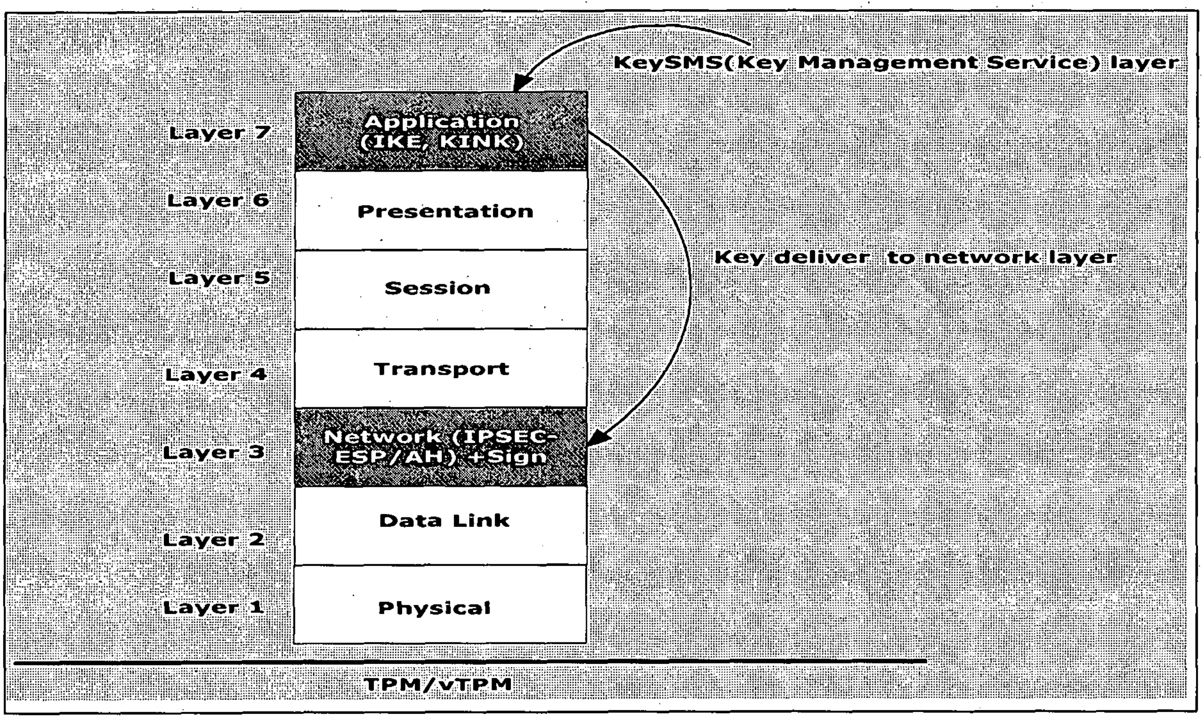

KeySMS(Key Management Service) layer
Layer 7
Application (IKE, KINK)
Layer 6
Presentation
Layer 5
Session
Layer 4
Transport
Layer 3
Network (IPSEC-ESP/AH) +Sign
Layer 2
Data Link
Layer 1
Physical
Key deliver to network layer
TPM/vTPM

FIG. 5

600

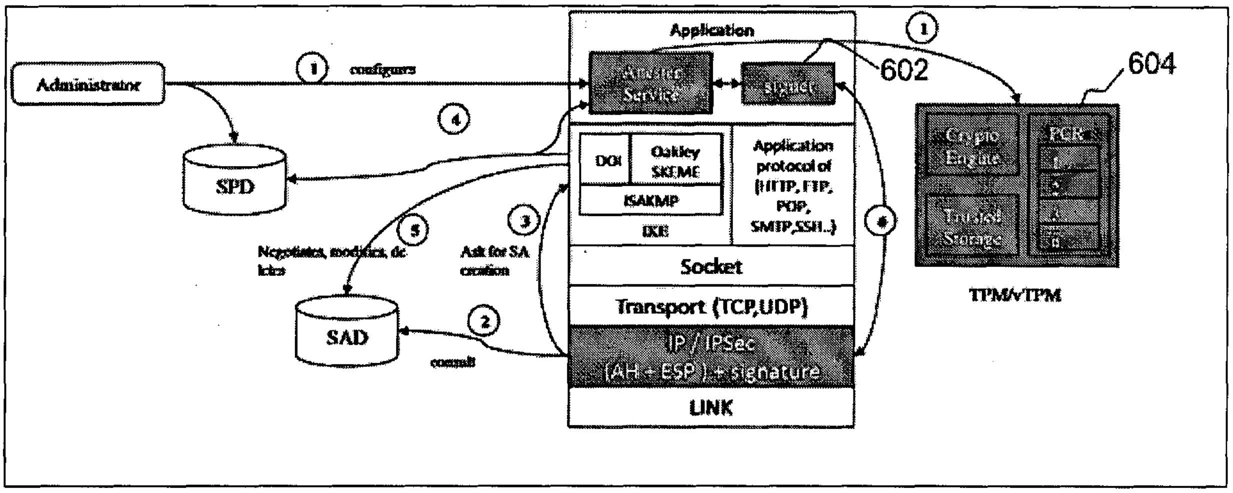

Administrator
1
configures
Application
Attester Service
Signer
602
1
604
4
SPD
DOI
Oakley SKEME
ISAKMP
IKE
Application protocol of (HTTP, FTP, POP, SMTP,SSH..)
5
Negotiates, modifies, deletes
3
Ask for SA creation
6
Socket
Transport (TCP,UDP)
SAD
2
commit
IP / IPSec (AH + ESP) + signature
LINK
Crypto Engine
Trusted Storage
PCR
1
2
3
n
TPM/vTPM

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No

PCT/MY2012/0O016O

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L29/06 G06F21/0O

ADD.

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 G06F

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

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

EPO-Internal , WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	AHMAD-REZA SADEGHI ET AL: "Extending IPsec for Efficient Remote Attestation", 25 January 2010 (2010-01-25), FINANCIAL CRYPTOGRAPHY AND DATA SECURITY, SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 150 - 165, XP019148479, ISBN: 978-3-642-14991-7	7,9, 10
A	abstract; figures 3-4 page 150, line 1 - page 152, line 23 page 155, line 12 - page 159, line 25 page 160, line 1 - line 12 page 163, 1ine 17 - 1ine 29 ----- -/--	1-6,8

☒ 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) orwhich is cited to establish the publication date of another 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 9 November 2012	Date of mailing of the international search report 21/11/2012
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Lebas, Yves

INTERNATIONAL SEARCH REPORT

International application No
PCT/MY2012/00Q160

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	INGO BENTE ET AL: "Interoperable Remote Attestation for VPN Environments", 1 January 2011 (2011-01-01), TRUSTED SYSTEMS, SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 302 - 315, XP019169937, ISBN: 978-3-642-25282-2	7,9, 10
A	page 305, line 4 - page 311, line 25; figures 1-3 page 313, line 19 - line 37 -----	1-6,8