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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 May 2012 (24.05.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/067487 A1

(51) International Patent Classification:
G06F 21/00 (2006.01) *H04L 9/00* (2006.01)
H04W 12/00 (2009.01)

(21) International Application Number:
PCT/MY2011/000109

(22) International Filing Date:
17 June 2011 (17.06.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 2010005380 16 November 2010 (16.11.2010) 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)*: **BIN MUBARAK, Mohd, Faizal** [MY/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **ABD MANAN, Jamalul-Lail** [MY/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **ABDU MUTHANA, Abdulrahman, Ahmed** [YE/MY]; 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,

[Continued on next page]

(54) Title: A SYSTEM AND METHOD FOR PROVIDING INTEGRITY VERIFICATION IN RADIO FREQUENCY IDENTIFICATION (RFID)

100

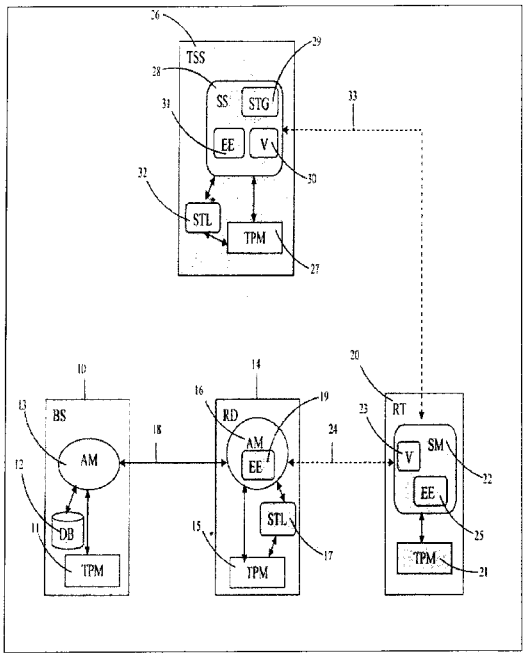

FIG. 1

(57) Abstract: The present invention provides a trusted Radio Frequency Identification (RFID) system for providing integrity verification using Trusted Platform Module (TPM). The system comprises a RFID tag, a Trusted Service Server (TSS), a RFID device and a Back End Server (BES), each comprising an embedded TPM storing the integrity values. The TSS also comprises a service ticket list, service ticket generator, verification engine and encryption engine. The integrity value of RFID device is sent to BES which is verified by comparing it to integrity value stored in BES. Then integrity value of BES is sent to RFID device, which is verified by comparing it to integrity value stored in RFID device. Then integrity value of RFID device is sent to RFID tag and is verified by comparing it to integrity value stored in RFID tag and requesting machine readable instructions as service from TSS by RFID tag.

WO 2012/067487 A1

EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *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))*

A SYSTEM AND METHOD FOR PROVIDING INTEGRITY VERIFICATION IN RADIO FREQUENCY IDENTIFICATION (RFID)

FIELD OF INVENTION

The present invention relates to a system and method for providing integrity verification in Radio Frequency Identification (RFID) using Trusted Platform Module (TPM).

BACKGROUND ART

Radio Frequency Identification (RFID) tags are intelligent bar codes that communicate information to a networked system and are applied to or incorporated into a tangible medium, such as, a product, animal, or person for the purpose of identification and tracking via radio waves. RFID system which does not provide for platform integrity verification is not trustable as it can be easily tampered and compromised by any adversary system. RFID system which does not provide for platform integrity verification is easily accessible by malware through machine instructions which exposed the application to security threats. In addition, security capabilities of the RFID tag is limited due to low resources in the tag.

Thus, establishing trusted Radio Frequency Identification (RFID) environment by embedding trusted platform module (TPM) in Radio Frequency Identification (RFID) system for integrity verification provides for a trusted environment. Trusted platform module (TPM) is tamper proof and produces encryption keys, identity keys and also providing integrity values. The ability of trusted platform module (TPM) as tamper proof security product is used to provide platforms integrity verifications in Radio Frequency Identification (RFID) system.

The system and method of the present invention establishes a trusted RFID environment by embedding a trusted platform module (TPM) in RFID system. Thereafter, integrity verification is performed on RFID device, tag and back end server. A trusted service server is providing services in RFID tag to compensate for limitation of resources within RFID tag.

The present invention also provides for protection of secret keys and data by sealing and storing the said data in the non-volatile memory of trusted platform module (TPM) in RFID tag, RFID device and back-end server. In addition, mutual attestation is provided between RFID device and back end server as well as between RFID device and RFID tag.

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 trusted Radio Frequency Identification (RFID) system (100) for providing integrity verification using Trusted Platform Module (TPM) The system (100) comprises at least one RFID tag, at least one Trusted Service Server (26), at least one RFID device (14) and at least one Back End Server (10). The at least one RFID tag (20) comprises at least one machine readable instruction module (22) and at least one embedded trusted platform module (21), the at least one machine readable instruction module (22) further comprises at least one verification engine (23) and at least one encryption engine (25).

The said Trusted Service Server (26) comprises at least one machine readable instruction services (28), at least one service ticket list (32) and at least one embedded trusted platform module (27), the said machine readable instruction services (28) further comprises at least one service ticket generator (29), at least one verification engine (30) and at least one encryption engine (31).

The said RFID device (14) comprises at least one attestation module (16), at least one service ticket list (17) and at least one embedded trusted platform module, the said attestation module (16) further comprises at least one encryption engine (19) and the said Back End Server (10) comprises at least one attestation module (13), at least one database (12) and at least one embedded trusted platform module (11).

Another aspect of the present invention provides a method (200) for providing integrity verification in Radio Frequency Identification (RFID) system using Trusted Platform Module. The method (200) comprising steps of sending integrity value of RFID device (14) to Back End Server (10) (202), verifying integrity value of RFID device (14) (204), comparing integrity value of RFID device (14) to integrity value stored in Back End Server (10) (206), sending integrity value of Back End Server (10) to RFID device (14) when integrity value of RFID device (14) matches integrity value stored in Back End Server (10) (208) else verification is terminated, verifying integrity value of Back End Server (10) (210), comparing integrity value of Back End Server (10) to the integrity value stored in RFID device (14) (212) else verification is terminated, sending integrity value of RFID device (14) to RFID tag (20) when integrity value of RFID device (14)

matches integrity value stored in RFID tag (20) (214) else verification is terminated, verifying integrity value of the RFID device (216), comparing integrity value of RFID device (14) to integrity value stored in RFID tag (20) (218) and requesting machine readable instructions as service from Trusted Service Server (26) by RFID tag (20) when integrity value of RFID device matches integrity value stored in RFID tag (20) (220).

A further aspect of the present invention provides a further method (300) for providing integrity verification in Radio Frequency Identification (RFID) system using Trusted Platform Module. The method (300) comprising steps of verifying service ticket of RFID tag (20) to value stored in Trusted Service Server (26) (302), comparing service ticket value of RFID tag (RT) to value stored in Trusted Service Server (26) (304), connecting RFID tag (20) to Trusted Service Server (26) when service ticket value of RFID tag (20) matches value stored in Trusted Service Server (26) (306) else verification is terminated, measuring components of RFID tag (20) and storing the said measurements in trusted platform module (27) of Trusted Service Server (26) (308), sending service ticket and integrity value of RFID tag (20) to RFID device (14) (310), verifying service ticket of RFID tag (20) (312), comparing value of service ticket of RFID tag (20) with value stored in RFID device (14) (314), sending integrity value of RFID tag (20) to Back End Server (10) when value of service ticket of RFID tag (20) matches value stored in RFID device (14) (316) else verification is terminated, verifying integrity value of RFID tag (20) (318), and comparing integrity value of RFID tag (20) to integrity value stored in Back End Server (10) (320). Back End Server (10) trust RFID tag (RT) when integrity value of RFID tag matches (20) integrity value stored in Back End Server (10) (322), else Back End Server (10) does not trust RFID tag (20) when integrity value of RFID tag does not match (20) integrity value stored in Back End Server (10) (324).

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 illustrates the Radio Frequency Identification (RFID) attestation system using trusted platform module (TPM).

FIG. 2 is a flowchart illustrating a method for providing integrity verification in Radio Frequency Identification (RFID) system using Trusted Platform Module (TPM).

FIG.3 is a flowchart illustrating a further embodiment of the method of FIG. 2.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention provides a system and method for providing integrity verification in Radio Frequency Identification (RFID) using Trusted Platform Module (TPM). 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 Radio Frequency Identification (RFID) attestation system using trusted platform module (TPM). Attestation is closely related to authentication wherein attestation is a process of assuring that information is accurate for trusted platform. This is such that trust in the system is based on taking measurements and checking measurements. As illustrated in FIG. 1, a trusted Radio Frequency Identification (RFID) system (100) for providing integrity verification using trusted platform module (TPM) comprising at least one RFID tag (RT) (20), at least one Trusted Service Server (TSS) (26), at least one RFID device (RD) (14) and at least one Back End Server (BS) (10).

The at least one RFID tag (RT) (20) comprises at least one machine readable instruction module (SM) (22) and at least one embedded trusted platform module (TPM) (21). The at least one machine readable instruction module (SM) (22) further comprises at least one verification engine (V) (23) and at least one encryption engine (EE) (25).

The at least one Trusted Service Server (TSS) (26) comprises at least one machine readable instruction services (SS) (28), at least one service ticket list (STL) (32) and at least one embedded trusted platform module (TPM) (27). The at least one machine readable instruction services (SS) (28) further comprises at least one service ticket generator (STG) (29), at least one verification engine (V) (30) and at least one encryption engine (EE) (31).

The at least one RFID device (RD) (14) comprises at least one attestation module (AM) (16), at least one service ticket list (STL) (17) and at least one embedded trusted

platform module (TPM), the at least one attestation module (AM) (16) further comprises at least one encryption engine (EE) (19) and the at least one Back End Server (BS) (10) comprises at least one attestation module (AM) (13), at least one database (DB) (12) and at least one embedded trusted platform module (TPM) (11).

The at least one encryption engine (EE) (19, 25, 31) encrypts transaction of RFID device (RD) (14), RFID tag (RT) (20) and Trusted Service Server (TSS) (26). In addition, the at least one encryption engine (19, 25, 31) is of Advance Encryption Standard (AES) platform or its equivalent. In addition, the at least one service ticket list (STL) (17,32) stores value for verification of service ticket.

The integrity values of RFID device (RD) (14) and RFID tag (RT) (20) are stored in database (DB) (12) inside the Back End Server (BS) (10). Trusted platform module (TPM) is embedded in RFID tag (RT) (20) to improve integrity measurement and reporting capabilities of the tag. Attestation module (AM) (16) of RFID device (14) retrieves integrity value from TPM (15), encrypts the data and thereafter sends it to the back-end server (BS) (10) for verification. The Back End Server (BS) receives integrity value of the RFID device (RD) through the (14) attestation module (AM) (13) and verifies it with the integrity value stored in the database (DB) (12). The integrity verification is successful if the integrity value of RFID device matches the integrity value stored in the database (DB) (12) that provides for a trusted RFID device (RD) (14) where the back-end server can trust the RFID device (RD) (14).

The RFID device (RD) (14) is installed by integrity value of Back End Server (BS) (10) and RFID tag (RT) (20) service ticket list (STL) (17) in the non-volatile memory of trusted platform module (TPM) (15). The attestation module (AM) (13) retrieves integrity value from trusted platform module (TPM) (11), encrypts data and thereafter sends it to RFID device (RD) (14) for verification. RFID device (RD) (14) receives integrity value of Back End Server (BS) (10) and verifies it with value in trusted platform module (TPM). Integrity verification is successful if the integrity value of Back End Server matches the integrity value of Back End Server which is stored in in the TPM (15) inside RFID device which provides for trusted Back End Server (BS) (10) wherein RFID device (RD) (14) can trust the Back End Server (BS) (10).

RFID tag (RT) (20) is installed with integrity values of Back End Server and RFID device (RD) (14) in the non-volatile memory of the TPM (21). RFID device (RD) (14) receives integrity value from trusted platform module (TPM) (15) and integrity value of Back End Server (BS) (10). Both integrity values of RFID device and Back End Server are encrypted using encryption engine (EE) (19) inside RFID device. Thereafter, integrity values are sent to RFID tag (RT) (20) for verification. RFID tag (RT) (20) receives RFID device (RD) (14) and Back End Server (BS) (10) integrity values through verification engine (V) (23) of machine readable instruction module (SM) (22) and verifies it with integrity values of RFID device and Back End Server which is stored in trusted platform module (TPM) (21) inside RFID tag. The integrity verification is successful if integrity values of RFID device and Back End Server matches to the integrity values stored in the TPM (15) inside RFID tag which means that RFID device (RD) (14) and back-end server (BS) (10) verification is successful and provides for a trusted RFID device (RD) (14) and back-end server (BS) (10) wherein the RFID tag (RT) (20) can trust the RFID device (RD) (14) and back-end server (BS) (10).

The RFID tag (RT) (20) is installed with a service ticket from the Service Ticket Generator (STG) (29) in the trusted service server (TSS) (26). The RFID tag (20) requests for service from trusted service server (TSS) (26). RFID tag (RT) (20) retrieves service ticket from trusted platform module (TPM) (21) through machine readable instruction module (SM) (22). Thereafter, machine readable instruction module (SM) (22) encrypts service ticket through encryption engine (EE) (25) and sends it to trusted service server (TSS) (26) for verification. Trusted service server (TSS) (26) receives RFID tag (RT) (20) service ticket through machine readable instruction service (SS) (28) and thereafter verify service ticket through verification engine (V) (30) based on value from service ticket list (STL) (32). The RFID tag (RT) (20) verification is successful if service ticket from RFID tag matches service ticket in service ticket list (STL) (32) wherein Trusted service server (TSS) (26) can provide services to RFID tag (RT) (20).

Machine readable instruction services (SS) (28) from Trusted Service Server (TSS) (26) measures machine readable instruction module (SM) (22) and configurations and stores measurement value in trusted platform module (TPM) (21). Service ticket generator (STG) (29) generates new service ticket from RFID tag (RT) (20) and stores it in trusted platform module (TPM) (21).

RFID tag (RT) (20) through machine readable instruction module (SM) (22) retrieves service ticket and integrity value from trusted platform module (TPM) (21). Thereafter, machine readable instruction (SM) (22) encrypts the same through encryption engine (EE) and sends it to RFID device (RD) (14) and Back End Server (10) for verification.

RFID device (RD) (14) receives RFID tag (20) service ticket and verifies service ticket from RFID tag with service ticket from service ticket list (STL) (17) inside RFID device. The RFID tag (RT) (20) ticket verification is successful if service ticket from RFID tag matches service ticket in service ticket list (STL) (17) wherein RFID device (RD) (14) sends integrity value of RFID tag (20) to be verified by Back End Server (10). Back End Server (10) receives integrity value of RFID tag (20) and verifies it with value in database (DB) (12). RFID tag (RT) (20) verification is successful if integrity value of RFID tag matches the integrity value in database (DB)(12) which provides for Back End Server (BS) (10) to trust RFID tag (RT) (20).

Reference is now being made to FIGs. 2 and 3 respectively. FIG. 2 is a flowchart illustrating a method for providing integrity verification in Radio Frequency Identification (RFID) system using Trusted Platform Module (TPM) and FIG.3 is a flowchart illustrating a further embodiment of the method of FIG. 2. As illustrated in FIG. 2 and FIG. 3, RFID device (RD) (14) sends integrity value to Back End Server (BS) (10) (202). Thereafter, integrity value of RFID device (RD) (14) is verified (204) and integrity value of RFID device (RD) (14) is compared to integrity value stored in Back End Server (BS) (10) (206). Integrity value of Back End Server (BS) (10) is sent to RFID device (RD) (14) when integrity value of RFID device (RD) (14) matches integrity value stored in Back End Server (BS) (10) (208).Verification is terminated if a match is not found.

Subsequently, integrity value of Back End Server (BS) (10) is verified (210) and integrity value of Back End Server (BS) (10) is compared to integrity value stored in RFID device (RD) (14) (212). Integrity value of RFID device (RD) (14) is sent to RFID tag (RT) (20) when integrity value of RFID device (RD) (14) matches integrity value stored in RFID tag (RT) (20) (214) else verification is terminated. Integrity value of RFID device is thereafter being verified (216). Integrity value of RFID device (RD) (14) is compared to integrity

value stored in RFID tag (RT) (20) (218) and machine readable instructions is requested as service from Trusted Service Server (TSS) (26) by RFID tag (RT) (20) when integrity value of RFID device (RD) matches integrity value stored in RFID tag (RT) (20) (220).

Further, as illustrated in FIG. 3, service ticket of RFID tag (RT) (20) is verified to value stored in Trusted Service Server (TSS) (26) (302). The service ticket value of RFID tag (RT) (20) is compared to service ticket stored in Trusted Service Server (TSS) (26) (304). RFID tag (RT) (20) is connected to Trusted Service Server (TSS) (26) when service ticket value of RFID tag (RT) (20) matches service ticket stored in Trusted Service Server (TSS) (26) (306) else verification is terminated.

Subsequently, components of RFID tag (RT) (20) is measured and stored in trusted platform module (TPM) (27) of Trusted Service Server (TSS) (26) (308). Service ticket and integrity value of RFID tag (RT) (20) is sent to RFID device (RD) (14) (310). Thereafter, service ticket of RFID tag (RT) (20) is verified (312) and value of service ticket of RFID tag (RT) (20) is compared to service ticket stored in RFID device (RD) (14) (314). Integrity value of RFID tag (RT) (20) is sent to Back End Server (BS) (10) when value of service ticket of RFID tag (RT) (20) matches service ticket stored in RFID device (RD) (14) (316) else verification is terminated. Integrity value of RFID tag (RT) (20) (318) is verified and integrity value of RFID tag (RT) (20) is compared to integrity value stored in Back End Server (BS) (10) (320).

Back End Server (BS) (10) trust RFID tag (RT) (20) when integrity value of RFID tag (RT) matches (20) integrity value stored in Back End Server (BS) (10) (322) and Back End Server (BS) (10) does not trust RFID tag (RT) (20) when integrity value of RFID tag (RT) does not match (20) integrity stored in Back End Server (BS) (10) (324). Integrity value of the present invention is measured at boot time.

The system and method of the present invention establishes a trusted RFID environment by embedding a trusted platform module (TPM) in RFID system. Thereafter, integrity verification is performed on RFID device, tag and back end server. A trusted service server is provided to provide services in RFID tag to compensate for limitation of resources within RFID tag.

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 trusted Radio Frequency Identification (RFID) system (100) for providing integrity verification using Trusted Platform Module comprising:

at least one RFID tag (20);

at least one Trusted Service Server (26);

at least one RFID device (14); and

at least one Back End Server (10);

wherein the at least one RFID tag (20) comprises at least one machine readable instruction module (22) and at least one embedded trusted platform module (21), the at least one machine readable instruction module (22) further comprises at least one verification engine (23) and at least one encryption engine (25);

the at least one Trusted Service Server (26) comprises at least one machine readable instruction services (28), at least one service ticket list (32) and at least one embedded trusted platform module (27), the at least one machine readable instruction services (28) further comprises at least one service ticket generator (29), at least one verification engine (30) and at least one encryption engine (31);

the at least one RFID device (14) comprises at least one attestation module (16), at least one service ticket list (17) and at least one embedded trusted platform module, the at least one attestation module (16) further comprises at least one encryption engine (19); and

the at least one Back End Server (10) comprises at least one attestation module (13), at least one database (12) and at least one embedded trusted platform module (11).

2. The at least one RFID tag (20) according to Claim 1 wherein the at least one machine readable instruction module (22) retrieves service ticket and integrity values from the at least one embedded trusted platform module (21);

the at least one verification engine (23) verifies integrity values of the at least one RFID device (14) and the at least one back-end server (10) of which integrity values are stored in trusted platform module (11, 21); verifies integrity value of Trusted Service Server (26) by retrieving the said integrity value from trusted platform module (27); and

the at least one encryption engine encrypts transaction of the at least one RFID tag (20).

3. The at least one Trusted Service Server (26) according to Claim 1 wherein the at least one machine readable instruction services (28) measures components of the at least one RFID tag (20) and stores it in trusted platform module (27);

the at least one service ticket list (32) stores value for verification of service ticket;

the at least one service ticket generator (29) generates service ticket from RFID tag (20) and stores service ticket in trusted platform module (21);

the at least one encryption engine (31) encrypts transaction of the at least one Trusted Service Server (26);

the at least one verification engine (30) verifies service ticket of RFID tag (20) with value of service ticket list (32) which is stored in trusted platform module;

wherein RFID tag (20) ticket verification is successful when value of service ticket of RFID tag (20) matches value of service ticket list (32) and further enables Trusted Service Server (26) to provide machine readable instruction services to RFID tag (20).

4. The at least one RFID device (14) according to Claim 1 wherein the at least one attestation module (16) receives integrity value of Back End Server (10) and verifies it with value stored in trusted platform module (15);

integrity verification of Back End Server (10) is successful when integrity value of Back End Server (10) matches value stored in trusted platform module (15) which indicates that RFID device (14) can trust Back End Server (10);

receives service ticket of RFID tag (20) and verifies service ticket with value from service ticket list (17);

verification of RFID tag (20) ticket is successful when service ticket matches with value from service ticket list (17) which further allows device (14) to send integrity value of RFID tag (20) for verification of Back End Server (10);

the at least one encryption engine (19) encrypts transaction of the at least one RFID device (14); and

the at least one service ticket list (17) stores value for verification of service ticket.

5. The at least one Back End Server (10) according to Claim 1 wherein the at least one attestation module (13) receives integrity value of RFID device (14) and verifies integrity value with value stored in database (12);

integrity verification is successful when integrity value of RFID device (14) matches integrity value stored in database (12) which indicates that Back End Server (10) can trust RFID device (14).

6. The system according to Claim 1, wherein the at least one Trusted Service Server (26) can be implemented in trusted platform module based machine or virtual trusted platform module .

7. The system according to Claim 1, wherein the at least one encryption engine (19, 25, 31) is of Advanced Encryption Standard (AES) platform or its equivalent.

8. A method (200) for providing integrity verification in Radio Frequency Identification (RFID) system using Trusted Platform Module comprising steps of:

sending integrity value of RFID device (14) to Back End Server (10) (202);

verifying integrity value of RFID device (14) (204);

comparing integrity value of RFID device (14) to integrity value stored in Back End Server (10) (206);

sending integrity value of Back End Server (10) to RFID device (14) when integrity value of RFID device (14) matches integrity value stored in Back End Server (10) (208) else verification is terminated;

verifying integrity value of Back End Server (10) (210);

comparing integrity value of Back End Server (10) to integrity value stored in RFID device (14) (212);

sending integrity value of RFID device (14) to RFID tag (20) when integrity value of RFID device (14) matches integrity value of RFID tag (RT) (214) else verification is terminated;

verifying integrity value of the RFID device (216);

comparing integrity value of RFID device (14) to integrity value stored in RFID tag (20) (218); and

requesting machine readable instructions as service from Trusted Service Server (26) by RFID tag (20) when integrity value of RFID device matches integrity value stored in RFID tag (20) (220).

9. The method (300) according to Claim 8 further comprising steps of:

verifying service ticket of RFID tag (20) to service ticket stored in Trusted Service Server (26) (302);

comparing service ticket value of RFID tag (20) to service ticket stored in Trusted Service Server (26) (304);

connecting RFID tag (20) to Trusted Service Server (26) when service

ticket value of RFID tag (20) matches service ticket stored in Trusted Service Server (26) (306) else verification is terminated;

measuring components of RFID tag (20) and storing the said measurements in trusted platform module (27) of Trusted Service Server (26) (308);

sending service ticket and integrity value of RFID tag (20) to RFID device (RD) (310);

verifying service ticket of RFID tag (20) (312);

comparing value of service ticket of RFID tag (20) to service ticket stored inRFID device (14) (314);

sending integrity value of RFID tag (20) to Back End Server (10) when value of service ticket of RFID tag (20) matches service ticket stored in RFID device (14) (316) else verification is terminated;

verifying integrity value of RFID tag (20) (318);

comparing integrity value of RFID tag (20) to integrity value stored in Back End Server (10) (320);

Back End Server (10) trust RFID tag (20) when integrity value of RFID tag matches(20) integrity value stored in Back End Server (10) (322); else

Back End Server (10) does not trust RFID tag (20) when integrity value of RFID tag (20) does not match integrity value stored in Back End Server (10) (324).

10. The method according to Claim 8 and 9, wherein integrity value is measured at boot time.

100

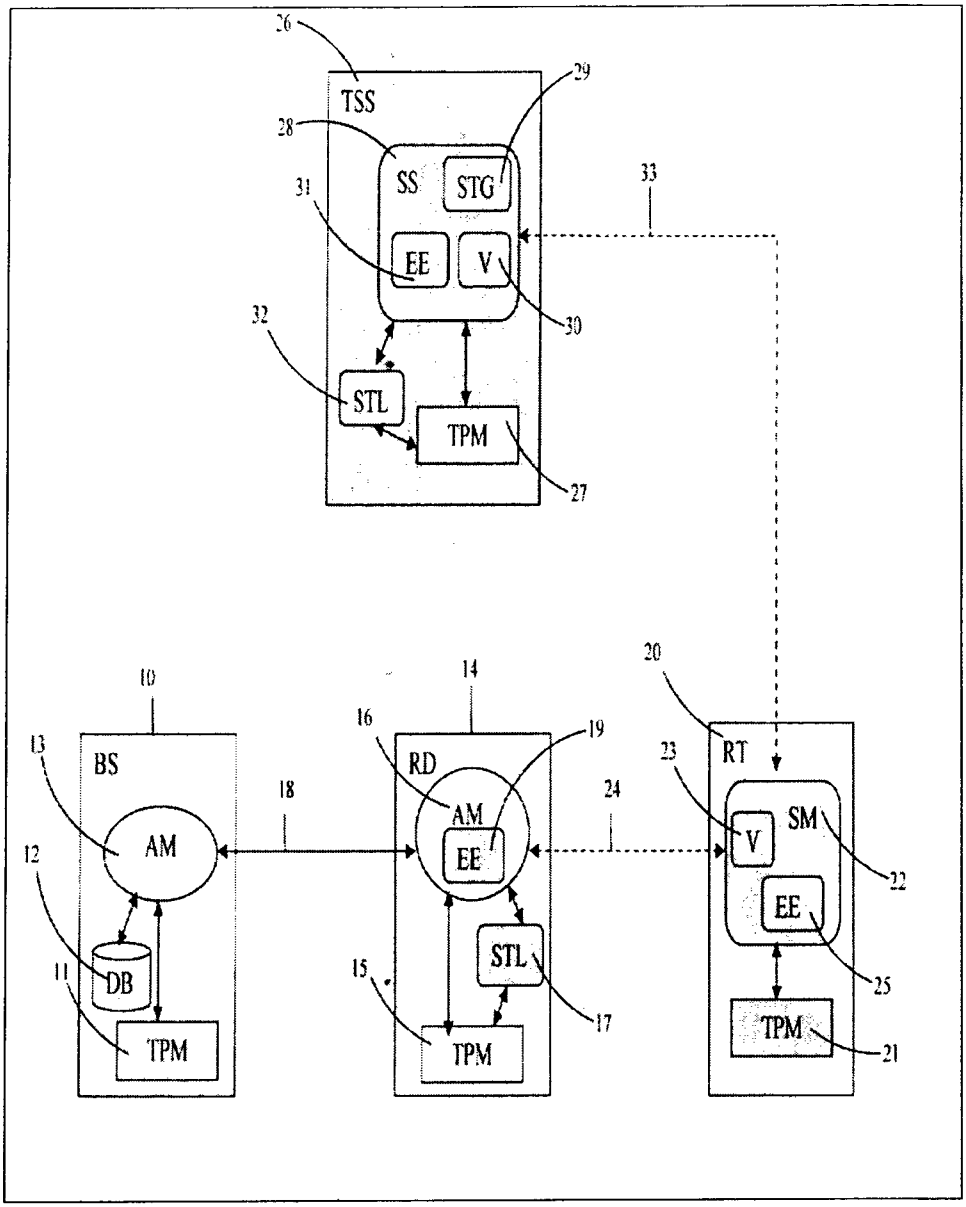
26
TSS
29
28
SS
STG
33
31
EE
V
30
32
STL
TPM
27
10
14
20
13
BS
16
RD
19
RT
23
18
24
AM
AM
V
SM
22
12
EE
EE
DB
STL
25
11
15
17
TPM
TPM
TPM
21

FIG. 1

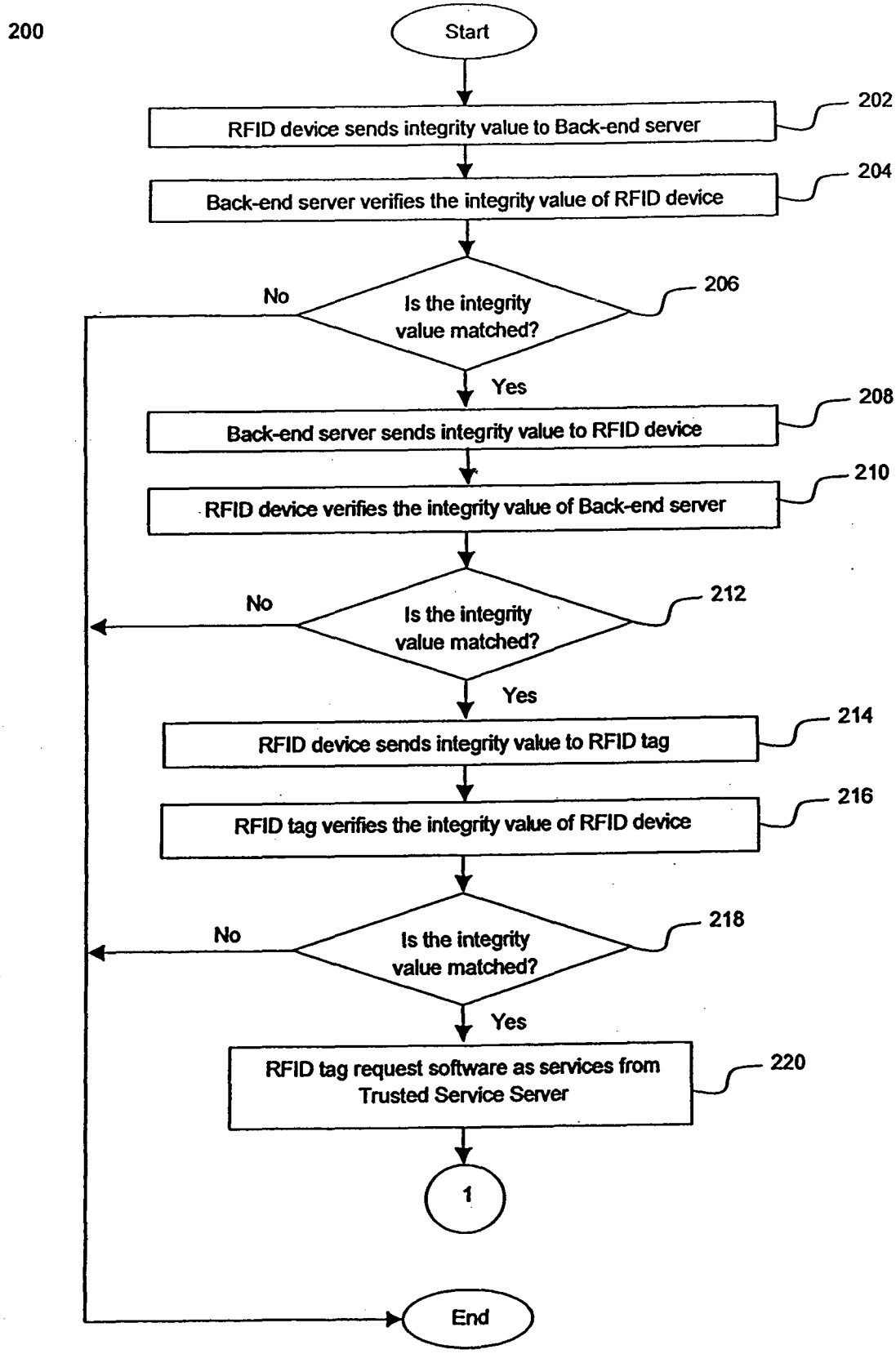
200
Start
RFID device sends integrity value to Back-end server
202
Back-end server verifies the integrity value of RFID device
204
Is the integrity value matched?
206
No
Yes
Back-end server sends integrity value to RFID device
208
RFID device verifies the integrity value of Back-end server
210
Is the integrity value matched?
212
No
Yes
RFID device sends integrity value to RFID tag
214
RFID tag verifies the integrity value of RFID device
216
Is the integrity value matched?
218
No
Yes
RFID tag request software as services from Trusted Service Server
220
1
End

Fig. 2

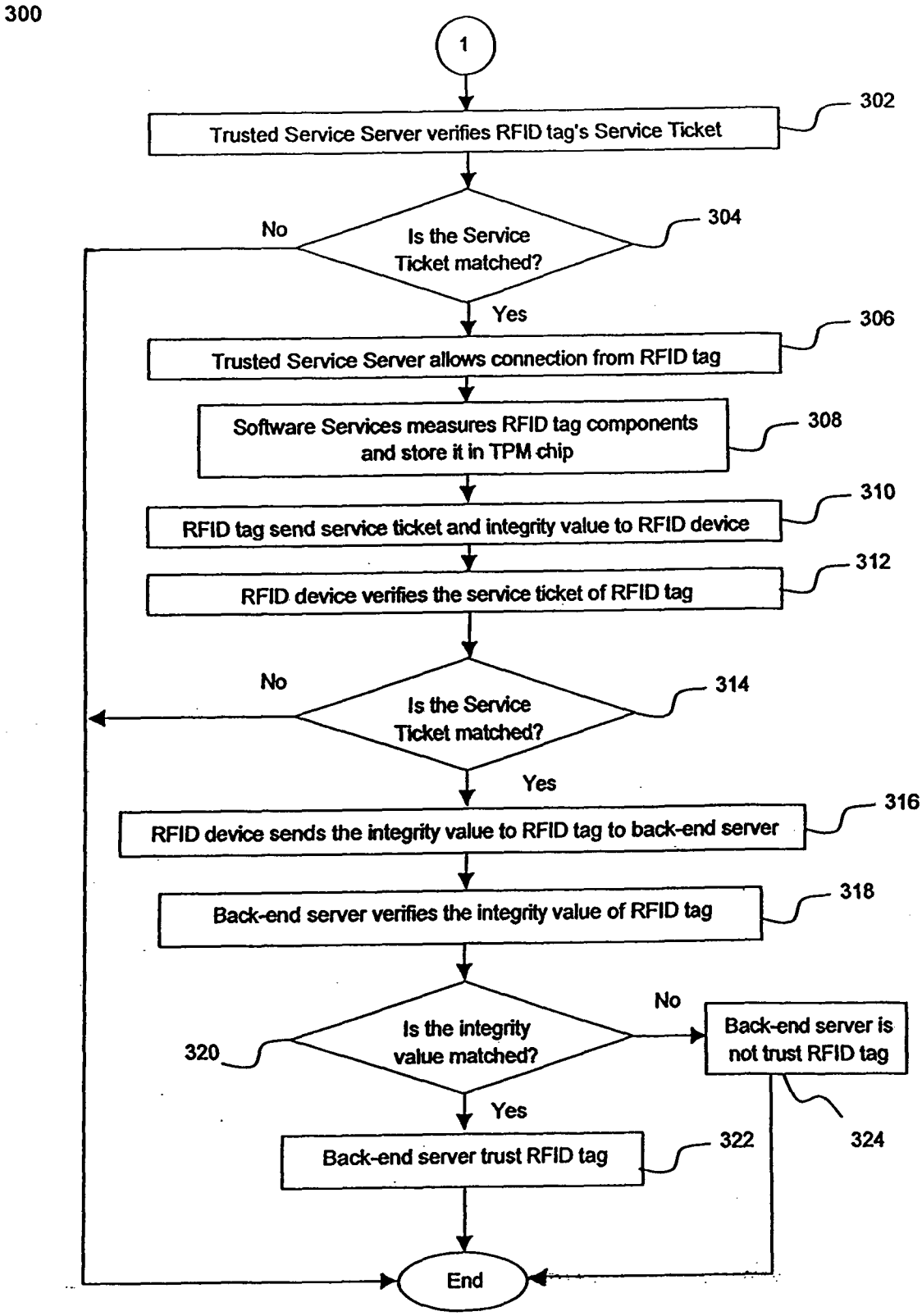
300
1
Trusted Service Server verifies RFID tag's Service Ticket
302
Is the Service Ticket matched?
304
No
Yes
Trusted Service Server allows connection from RFID tag
306
Software Services measures RFID tag components and store it in TPM chip
308
RFID tag send service ticket and integrity value to RFID device
310
RFID device verifies the service ticket of RFID tag
312
Is the Service Ticket matched?
314
No
Yes
RFID device sends the integrity value to RFID tag to back-end server
316
Back-end server verifies the integrity value of RFID tag
318
Is the integrity value matched?
320
No
Back-end server is not trust RFID tag
324
Yes
Back-end server trust RFID tag
322
End

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/MY2011/000109

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

G06F 21/00 (2006.01) ***H04W 12/00*** (2009.01) ***H04L 9/00*** (2006.01)

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

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)
WPI, Google and Patent Lens: Keywords (RFID, TPM, integrity, verify, match, compare, service ticket and like terms)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MUBARAK, M et al., "Mutual Attestation Using TPM for Trusted RFID Protocol", 2010 Second International Conference on Network Applications, Protocols and Services, 22-23 Sept. 2010, pages 153-158 Abstract, Fig 1	
A	WO 2007/027302 A2 (SKYETEK, INC) 8 March 2007 The Whole Document	

☐ 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 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	Date of mailing of the international search report
16 September 2011	28/09/2011
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. +61 2 6283 7999	Authorized officer **AMARDEEP SINGH** AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No : +61 2 6283 2803

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/MY2011/000109

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
WO	2007027302	EP	1872308	EP	1872594	EP	1872597
		EP	1872598	EP	1872599	EP	1872600
		EP	1872601	EP	1872602	EP	1929450
		EP	1929796	EP	1932124	EP	1932370
		EP	1977402	EP	2009574	EP	2017761
		EP	2051194	US	2007182558	US	7456746
		US	2007159330	US	7570164	US	2007207792
		US	7659819	US	2006238302	US	2006238303
		US	2006238304	US	2006238305	US	2006238306
		US	2006253415	US	2007046431	US	2007046434
		US	2007046467	US	2007206786	US	2007206797
		US	2008001752	US	2008022160	US	2008042830
		WO	2006116012	WO	2006116084	WO	2006116085
		WO	2006116086	WO	2006116235	WO	2006116236
		WO	2006116237	WO	2006116238	WO	2007027220
		WO	2007027297	WO	2007027885	WO	2007078329

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX