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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 August 2020 (27.08.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/171997 A1

(51) International Patent Classification:
H04N 21/266 (2011.01) *H04N 21/658* (2011.01)
H04N 21/418 (2011.01) *H04N 21/43* (2011.01)
H04N 21/4367 (2011.01) *G06F 21/12* (2013.01)
H04N 21/4623 (2011.01) *G06F 21/72* (2013.01)
H04N 21/6543 (2011.01)

(21) International Application Number:
PCT/US2020/017476

(22) International Filing Date:
10 February 2020 (10.02.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/807,287 19 February 2019 (19.02.2019) US

(71) Applicant: **ARRIS ENTERPRISES LLC** [US/US]; 3871 Lakefield Drive, Suwanee, Georgia 30024 (US).

(72) Inventors: **MEDVINSKY, Alexander**; 8873 Hampe Court, San Diego, California 92129 (US). **PETTY, Douglas M.**; 16393 Alipaz Ct., San Diego, California 92127 (US).

(74) Agent: **GATES, George H.**; Gates & Cooper LLP, 6060 Center Drive, Suite 830, Los Angeles, California 90045 (US).

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

(54) **Title:** ENTITLEMENT MANAGEMENT MESSAGE EPOCH AS AN EXTERNAL TRUSTED TIME SOURCE

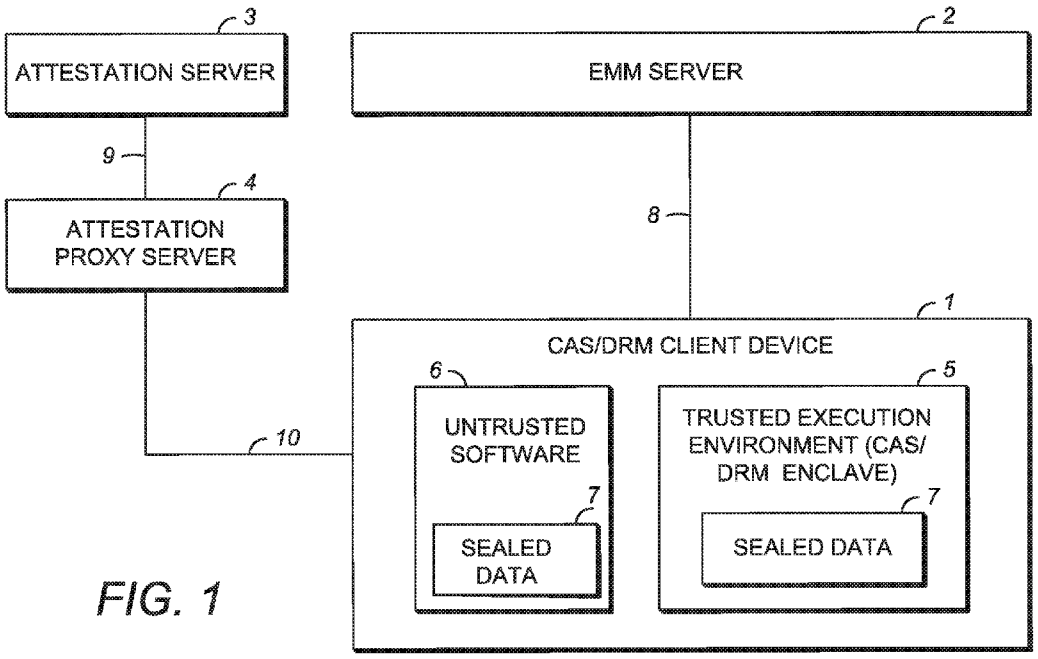

FIG. 1

(57) **Abstract:** An external trusted time source is implemented over a network for conditional access system (CAS)/digital rights management (DRM) client devices. A client device includes untrusted software and a trusted execution environment (TEE) for processing an entitlement management message (EMM) that includes an epoch sequence number (ESN) transmitted from an EMM server using a first network connection. A remaining client key set (CKS) lifetime value is stored and updated in the TEE based on the ESN processed.

WO 2020/171997 A1

[Continued on next page]

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, KM, ML, MR, NE, SN, TD, TG).

Published:

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

ENTITLEMENT MANAGEMENT MESSAGE EPOCH AS AN EXTERNAL TRUSTED TIME SOURCE

Inventors:
Sasha Medvinsky
Douglas Petty

Cross Reference to Related Application

[0001] This Application claims priority under 35 U.S.C. §119(e) from earlier filed United States Provisional Application Serial No. 62/807,287, filed February 19, 2019 which is incorporated herein by reference.

Background

Technical Field

[0002] The subject matter of the present disclosure relates generally to the protection of an external secure time source when verifying limited lifetimes of CAS or DRM client keys over a network using a trusted execution environment.

Related Art

[0003] Conditional access systems (CAS) or Digital Rights Management (DRM) use a trusted execution environment such as an Intel® SGX Enclave to protect client key sets and other secure data across platform reboots. These client keys in some cases have a limited lifetime and need to expire after some number of months or years after first being installed on a client system. A secure and trusted time source is helpful in this situation. There are additional needs for a secure time implemented inside trusted execution environments such as an Intel® SGX Enclave, such as the enclave software may need to be periodically validated by an Attestation Server, to verify the software includes the latest security patches.

[0004] Thus, it would be advantageous and an improvement over the relevant technology to provide an apparatus and/or a method that is capable of protecting an external secure time source that cannot be manipulated when verifying limited lifetimes of CAS or DRM client keys and software versions over a network using a trusted execution environment such as an Intel® SGX Enclave in a network.

Summary

[0005] Embodiments described in the present disclosure provide methods to implement an entitlement management message epoch as an external trusted time source over a network to a conditional access system (CAS) client device. The methods include transmitting an entitlement management message (EMM) to a trusted execution environment (TEE) within a client device from an EMM server using a first network connection, the EMM including an epoch sequence number (ESN); generating an updated remaining client key set (CKS) lifetime value in the TEE based on an initial lifetime duration value for the CKS, and the ESN value in the EMM; sealing the CKS, updated ESN value in the EMM, and updated remaining CKS lifetime value as unit information; and delivering the updated remaining CKS lifetime value and updated ESN value in the EMM from the TEE to untrusted software in the CAS client device, and storing the updated remaining CKS lifetime value and updated ESN value.

Embodiments described in the present disclosure provide an apparatus to implement the external trusted time source over a network for a CAS client device.

The apparatus includes a non-transitory memory configured to store one or more programs, untrusted software, and a trusted execution environment (TEE); a hardware processor configured to execute the one or more programs to perform operations of the untrusted software and the TEE; and a network interface configured to establish communication with a network using a network connection, wherein when the one or more programs are executed by the hardware processor: the TEE of the CAS client device receives an entitlement management message (EMM) from an EMM server using the network connection, wherein the EMM includes an epoch sequence number (ESN), the TEE generates an updated remaining client key set (CKS) lifetime value based on an initial lifetime duration value for the CKS, and the ESN value in the EMM, the TEE seals the CKS, updated ESN value in the EMM, and updated remaining CKS lifetime value as unit information, and the TEE delivers the updated remaining CKS lifetime value to untrusted software in the CAS client server, and stores the updated remaining CKS lifetime value.

[0006] Embodiments described in the present disclosure provide a non-transitory computer-readable recording medium in each of the client device and the EMM server for implementing an entitlement management message epoch as

an external trusted time source over a network to a CAS client device. Each non-transitory computer-readable recording medium stores one or more programs which when executed by a respective processor performs the steps of the method described above.

Brief Description of the Drawings

[0007] In the drawings, like reference numbers generally indicate identical, functionally similar, and/or structurally similar elements.

[0008] Fig. 1 is a schematic diagram of a system for implementing an entitlement management message epoch as an external trusted time source according to an embodiment of the present disclosure;

[0009] Fig. 2 is a schematic diagram of a system for implementing an entitlement management message epoch as an external trusted time source according to an embodiment of the present disclosure;

[0010] Fig. 3 illustrates a method for initializing the entitlement management message epoch as an external trusted time source using the system of Fig. 1 or Fig. 2 according to an embodiment of the present disclosure;

[0011] Fig. 4 illustrates a portion of the method performed by the trusted execution environment for processing the epoch from the initial entitlement management message according to an embodiment of the present disclosure shown in Fig. 3;

[0012] Fig. 5 illustrates a method for implementing the entitlement management message epoch during ongoing transmission of EMMs as an external trusted time source using the system of Fig. 1 or Fig. 2 according to an embodiment of the present disclosure;

[0013] Fig. 6 illustrates a portion of the method performed by the trusted execution environment for processing the entitlement management message epoch according to an embodiment of the present disclosure shown in Fig. 5;

[0014] Fig. 7 illustrates a method for implementing the entitlement management message epoch as an external trusted time source when a large change in the ESN value occurs using the system of Fig. 1 or Fig. 2 according to an embodiment of the present disclosure;

[0015] Fig. 8 illustrates a portion of the method performed by the trusted execution environment for processing the entitlement management message epoch according to an embodiment of the present disclosure shown in Fig. 7;

[0016] Fig. 9 illustrates a method for implementing the entitlement management message epoch as an external trusted time source with multiple TEE instances using the system of Fig. 1 or Fig. 2 according to an embodiment of the present disclosure;

[0017] Fig. 10A illustrates a portion of the method performed by the trusted execution environment for processing the entitlement management message epoch according to an embodiment of the present disclosure shown in Fig. 9;

[0018] Fig. 10B illustrates a portion of the method performed by a second trusted execution environment for processing a separate entitlement management message epoch according to an embodiment of the present disclosure shown in Fig. 9;

[0019] Fig. 11 illustrates a method for implementing the entitlement management message epoch as an external trusted time source and verifying with

an attestation server using the system of Fig. 1 or Fig. 2 according to an embodiment of the present disclosure;

[0020] Fig. 12 illustrates a method for implementing the entitlement management message epoch as an external trusted time source and verifying with an attestation server with persistently stored ESN using the system of Fig. 1 or Fig. 2 according to another embodiment of the present disclosure;

[0021] Fig. 13 illustrates a method performed by the trusted execution environment for processing the epoch from the subsequent entitlement management message according to an embodiment of the present disclosure;

[0022] Fig. 14 is a schematic diagram of an exemplary client device according to an embodiment of the present disclosure; and

[0023] Fig. 15 is a schematic diagram of an exemplary server according to an embodiment of the present disclosure.

Detailed Description

[0024] Fig. 1 is a schematic diagram of a system for implementing an entitlement management message epoch as an external trusted time source. As

shown in Fig. 1, the system includes a conditional access system/digital rights management (CAS) client device 1, an attestation proxy server (APS) 4, an attestation server 3, and an entitelement management message (EMM) server 2. The CASDRM client device may be referenced as a CAS client device, however, DRM client devices can also be used in these environments. Fig. 2 is also a schematic diagram of the same system for implementing an entitlement management message epoch as an external trusted time source. References to Fig. 1 throughout the disclosure also reflect the system in Fig. 2 with the exception of where sealed data 7 is stored. Discusisons of sealed data 7 will distinguish between Fig. 1 and Fig. 2, otherwise reference to Fig. 1 can reflect both the Fig. 1 and Fig. 2 system.

[0025] An explanation of exemplary internal components of the CAS client device 1 and servers 2, 3, 4 shown in Fig. 1 will be provided in the discussion of Figs. 14 and 15. However, in general, it is contemplated by the present disclosure that the CAS client device 1 and servers 2, 3, 4 include electronic components or electronic computing devices operable to receive, transmit, process, store, and/or manage data and information associated with the system,

which encompasses any suitable processing device adapted to perform computing tasks consistent with the execution of computer-readable instructions stored in a memory or a computer-readable recording medium.

[0026] Further, any, all, or some of the computing devices in the CAS client device 1 and the servers 2, 3, 4 may be adapted to execute any operating system, including Linux, UNIX, Windows Server, etc., as well as virtual machines adapted to virtualize execution of a particular operating system, including customized and proprietary operating systems. The CAS client device 1 and servers 2, 3, 4 are further equipped with components to facilitate communication with other computing devices over the one or more network connections 8, 9, 10. The network connections 8, 9, 10 include connections to local and wide area networks, wireless and wired networks, public and private networks, and any other communication network enabling communication in the system.

[0027] In Fig. 1, the CAS client device 1 is a personal computer, laptop, smartphone, tablet computer, personal digital assistant, set top box, in-vehicle computing systems, or other similar computing device. The CAS client device 1 includes one or more memories or memory locations for storing the software

components, which include untrusted software 6 and a trusted execution environment (TEE) 5. The one or more memories in the CAS client device 1 include, but are not limited to, random access memory (RAM), dynamic random access memory (DRAM), read only memory (ROM), logic blocks of a field programmable gate array (FPGA), erasable programmable read only memory (EPROM), and electrically erasable programmable ROM (EEPROM).

[0028] The untrusted software 6 facilitates communication with the TEE 5 and other components of the CAS client device 1 as well as communication between the TEE 5 and the network servers 2, 3, 4. The untrusted software 6 can include sealed data 7, such as sealed unit information, that can be attached to a message or a request generated (e.g., updated unit information) to certify that it originated from the untrusted software 6 as shown in Fig. 2. The untrusted software 6 can be stored in non-volatile memory, RAM, or other similar memory in the CAS client device 1 maintained separate from the TEE 5.

[0029] The TEE 5 is, for example, an Intel® SGX Enclave stored in a special protected memory region such as a processor reserved memory of DRAM of the CAS client device 1. The TEE 5 is a protected environment for trusted

execution that contains code and data pertaining to a security-sensitive computation. The TEE 5 protects the confidentiality and integrity of computations performed inside the TEE 5 from attacks by malicious computing devices and/or software. The TEE 5 can include sealed data 7, such as sealed unit information, that can be attached to a message or a request generated (e.g., updated unit information) to certify that it originated from the TEE 5. The sealed data 7 is further described below.

[0030] The CAS client device 1 can include a user interface such as a key board, mouse, touchscreen display, network connection between user and client, or the like to allow a user to view and interact with the applications, tools, services, and other software of the CAS client device 1. While only one CAS client device 1 is shown, the present disclosure contemplates that more than one CAS client device 1 can be implemented.

[0031] The untrusted software 6 establishes communications with the APS 4 using a network connection 10. It is contemplated by the present disclosure that communications between the TEE 5 or the untrusted software 6 of the CAS client device 1 and the APS 4 via the network connection 10 are authenticated using,

for example, a server authenticated transport layer security (TLS) to secure all communications between the APS 4 and the CAS client device 1. The APS 4 is a network server that provides verification that a software version or data generated (e.g., an attestation check request) from the TEE 5 is the correct version or has not been modified after leaving the CAS client device 1.

[0032] The attestation server 3 is a network server providing attestation services such as those provided by an Intel® Attestation Service. The attestation server 3 communicates with the APS 4 using a network connection 9. It is contemplated by the present disclosure that communications between the APS 4 and the attestation server 3 via network connection 9 are authenticated using, for example, mutually authenticated TLS to secure all communications between the APS 4 and the attestation server 3. The attestation server 3 utilizes technology, such as the Intel EPID technology, to provide verification of the information provided from the CAS client device 1 via the APS 4. For example, the software of the CAS client device 1 can be verified by the attestation server 3 and the results returned to the attestation proxy 4 using the network connection 9.

[0033] The entitlement management message (EMM) server 2 is a network server that communicates with the CAS client device 1 using a network connection 8. It is contemplated by the present disclosure that communications between the CAS client device 1 and the EMM server 2 via network connection 8 are implemented using, for example, a transmission control protocol/Internet protocol (TCP/IP). As shown in Fig. 1, the EMM server 2 stores EMMs and sends EMMs. EMMs can be utilized by a CAS and DRM system to deliver both digital content authorizations and group keys to clients, when both content authorizations and group keys are required for a client to obtain access to a particular broadcast program or category of content.

[0034] Each EMM can include a sequential integer value called an epoch that is incremented by "M", where "M" is >= 1, every time there is a change to a group key from the EMM server 2. The epoch is incremented by M on a periodic basis using a known interval (e.g. monthly). The EMM may include the epoch increment with a change in group keys, or the like. In order to track these increment transitions of the epoch and translate these transitions to a "time", the most recently seen epoch sequence number (ESN) is identified. The

communication from the EMM server 2 may pass through the untrusted software 6. The EMM is encrypted and authenticated to ensure that the epoch has not been tampered.

[0035] The enclave platform, such as an Intel® SGX platform, allows for a secure file storage for saving secure data encrypted with a device-unique sealing key across platform reboots. Once sealed, the secured data, refered to as sealed data 7, can be saved in any storage, including unprotected storage in the untrusted software 6. Fig. 1 and Fig. 2 illustrate locations where the sealed data 7 can be stored, i.e. in either the untrusted software 6 and a copy in the TEE 5 in Fig. 1 or the TEE 5 in Fig. 2. In certain embodiments, the sealed data 7 can be persistently stored in the untrusted software 6 in an encrypted form and then copied into the TEE 5 and decrypted there when the sealed data 7 is used. Additionally, the sealed data 7 can be only in the TEE 5 in a persistent memory such as in a secure flash. Further, the sealed data 7 can be persistently stored in the untrusted software 6. The act of sealing or encrypting this data can only be preformed within the TEE 5, the only place where the sealing key is accessible. Likewise, decrypting the sealing data 7 and being able to read the clear values

within it can only be accomplished by the TEE 5 because it has access to the sealing key used for decryption. The sealed data 7 is used to persistently store a client key set (CKS). To track time elapsed, the most recently seen ESN and remaining CKS lifetime values also need to be placed in the sealed data 7.

[0036] Fig. 3 illustrates a method for implementing the entitlement management message epoch as an external trusted time source using the system of Fig. 1.

[0037] In step S1, the EMM is delivered to the TEE 5 of the CAS client device 1. In certain embodiments, the EMM is transmitted through the untrusted software 6. The EMM includes the current ESN.

Steps S2 through S4, shown in Fig. 4, include the receiving of the initial EMM in the TEE 5 in step S2. If the EMM has been tampered with, the TEE 5 can detect and in some embodiments, an alarm may be initiated. During an initial receipt of the EMM, which is after obtaining the CKS, the TEE 5 initializes remaining CKS lifetime value and the ESN value by identifing an initial lifetime duration of a CKS in step S3. The initial lifetime duration of a CKS can be a hardcoded default value, or provisioned with each CKS. In other words, the initial lifetime

duration of a CKS can be delivered to each device as part of CKS or the initial lifetime duration of a CKS is a pre-configured value that is part of a CAS client implementation. The initial lifetime duration of a CKS may be ignored after the initializing of the remaining CKS lifetime value. In some embodiments, the initial lifetime duration of a CKS can be optionally stored and/or sealed. Step S4 has the TEE 5 sealing the field values from the EMM (ESN and remaining CKS lifetime value) in addition to the CKS, initial lifetime duration value (optionally) as unit information in the sealed data 7. A lower bound is identified for the remaining CKS lifetime value. In step 5, the TEE 5 delivers the updated sealed unit information including the most recently seen ESN and the remaining CKS lifetime values to the untrusted software 6 in Fig. 3. As mentioned above, if it is an initial EMM transmission as is represented in Figs. 3 and 4, then these values are initialized within the TEE 5 using the ESN from the initial EMM. If this is not an initial EMM transmission, then the values are updated based on the EMM received as will be discussed below. In the case of a reboot, the TEE does not accept the sealed unit information unless it also contains an EMM related remaining CKS lifetime value and ESN value.

Addtionally, the updated sealed unit information can be stored in the untrusted software for the client reboot.

[0038] Fig. 5 illustrates a method for implementing the entitlement management message epoch as an external trusted time source using the system of Fig. 1 and Fig. 2. Fig. 3 refers to a first transmission of the EMM to the CAS client deivce 1 after the CKS is obtained. Figs. 5 and 6 refer to an ongoing transmission of the EMM.

[0039] Over a specific amount of time that is a pre-defined epoch period, the EMM server moves to a next epoch transition. During this epoch transition, the ESN in the EMM is incremented by a value of M. In Fig. 5, step S6, the EMM is delivered to the TEE 5 of the CAS client device 1. Fig. 6 shows steps S7-S15 which include the process through the TEE 5. In step S7, when the TEE 5 receives the EMM, the TEE 5 increments the ESN by M, matching the ESN increment in the received EMM. In step S8, the TEE 5 verifies the remaining CKS lifetime value and decrements the remaining CKS lifetime value by N in step S9. The remaining CKS lifetime value may be at the lower bound prior to the processing of the EMM and decrement of the remaining CKS lifetime value.

In step S10, it is determined if the remaining CKS lifetime value is already at a lower bound value. If the remaining CKS lifetime value is already at the lower bound value, then the EMM is not processed in step S15. In step S11, it is determined if the remaining CKS lifetime value is at the lower bound value after the remaining CKS lifetime value decremented. If the remaining CKS lifetime is at the lower bound value after decrement, then EMM is deleted or ignored and the sealed unit information is sent with the remaining CKS lifetime value at the lower bound in step S14. Step S12 illustrates if the remaining CKS lifetime value is not at the lower bound, the fields (ESN and remaining CKS lifetime values) are updated. The sealed updated fields are added to the unit information in step S13. Fig. 5 shows step S16 where the TEE delivers the updated sealed unit information including the ESN+M value and the remaining CKS lifetime value-N.

[0040] The ESN has a finite limit and after the ESN reaches its maximum value of Max-ESN, the next time it is incremented, the ESN wraps around to a value of 0. Therefore, in the cases when the ESN value inside a received EMM (EMM-ESN) is less than the currently saved ESN value (sealed-ESN), that

implies that the ESN in the latest EMM generated by the EMM server 2 has wrapped around. In these cases, the value of M is calculated as follows: M = (Max-ESN – sealed-ESN + 1) + EMM-ESN. Additionally, N is determined based on the above relationship between M and N.

[0041] Fig. 7 illustrates a method for implementing the entitlement management message epoch as an external trusted time source using the system of Fig. 1 and Fig. 2. Fig. 7 illustrates a situation where there may have been a large change in the ESN value between the ESN in a new EMM and the ESN that is stored by the TEE 5 from the last EMM processed. These situations can occur when the CAS client device 1 has been powered down for months and has not received any EMMs during that timeframe. Another situation where there may be a large change in the ESN values is when the CAS client device 1 has been moved, for example, to support a different CAS security domain. Additionally, another situation with a large jump in the ESN is where a hacker deliberately saves and then restores an old copy of the sealed unit information, in an attempt to set the clock backwards and re-use the same CKS for a longer period of time.

[0042] With the delivery of the EMM in step S17, the TEE 5 has to evaluate the ESN in the EMM. Fig. 8 illustrates where the TEE 5 detects a change in the ESN and identifies an increment of X in step S18. In step S19, the TEE 5 verifies the remaining CKS lifetime value. The TEE 5 then, based on the increments of ESN by X, decrements the remaining CKS lifetime value by a value Y in step S20. The value X is a multiple of M and the value Y is the same multiple of N, e.g. X = i*M and Y = i*N where X, Y, I, M, N are all positive integers.

[0043] As mentioned above, the ESN has a finite limit and after the ESN reaches its maximum value of Max-ESN, the next time it is incremented, the ESN wraps around to a value of 0. Therefore, in the cases when the ESN value inside a received EMM (EMM-ESN) is less than the currently saved ESN value (sealed-ESN), that implies that the ESN in the latest EMM generated by the EMM server 2 has wrapped around. In these cases, the value of X is calculated as follows: X = (Max-ESN – sealed-ESN + 1) + EMM-ESN. Additionally, Y is determined based on the above relationship between X and Y.

[0044] The remaining CKS lifetime value may be at the lower bound prior to the processing of the EMM and decrement of the remaining CKS lifetime value. In step S21, it is determined if the remaining CKS lifetime value is already at a lower bound value. If the remaining CKS lifetime value is already at the lower bound value, then the EMM is not processed in step S25. In step S22, it is determined if the remaining CKS lifetime value is at the lower bound value after the remaining CKS lifetime value decremented. If the remaining CKS lifetime is at the lower bound value after the decrement, then EMM is deleted or ignored and the sealed unit information is sent with the remaining CKS lifetime value at the lower bound in step S26. Step S23 illustrates if the remaining CKS lifetime value is not at the lower bound, the fields (ESN and remaining CKS lifetime values) are updated. The sealed updated fields are added to the unit information in step S24. Fig. 7 shows step S27 where the TEE delivers the updated sealed unit information including the ESN+X value and the remaining CKS lifetime value-Y.

[0045] Fig. 9 illustrates a method for implementing the entitlement management message epoch as an external trusted time source using the system

of Fig. 1 and Fig. 2 where there are a plurality of instances of TEEs 5, 5A, etc., each TEE including a different installed CKS. Fig. 9 illustrates two instances, however, there may be more instances within the embodiment copying the steps for the second instance TEE 5A. The TEE 5 that has so far been referenced is referred to the first instance TEE and at least one more instance of TEE, a second instance TEE 5A, is added. The EMM is delivered to the TEE 5 of the CAS client device 1 and a separate EMM is delivered to each instance of TEE 5, 5A, etc. in steps S27 and S32. In certain embodiments, the EMM is transmitted through the untrusted software 6. The first and second instance TEE both receive that particular instance EMM in Figs. 10A step S28 and 10B step S33 respectively. The second instance TEE 5A generates an updated remaining CKS lifetime value based on the CKS key for the second instance TEE 5A, the initial lifetime duration value for the CKS of the second instance TEE 5A, and the ESN value in the EMM for the second instance TEE 5A. If an initial transmission of the EMM, the second instance TEE 5A initializes the remaining CKS lifetime value and ESN value for the second instance TEE 5A in step S34. The second instance TEE 5A then seals the CKS, the initial lifetime duration value

(optionally), updated ESN value, and updated CKS lifetime value as unit information in step S35. During this time, the first instance TEE also runs through the same process with the values for the first instance TEE in steps S28-S30. Fig. 9 then shows both the first instance TEE and the second instance TEE 5A delivering the updated sealed unit information including ESN and remaining CKS lifetime value for each instance in step S31 and step S36.

[0046] To ensure additional security of the external trusted source and the CAS client device 1 itself, a periodic attestation verification can take place, illustrated in Figs. 11 through 13. An attestation check request is transmitted from the untrusted software 6 to the attestation proxy server (APS) 4 using a second network connection 10 in steps S39 or S45. The APS 4 transmits the attestation check response from the APS 4 to the untrusted software 6 in steps S42 or S48.

[0047] Additionally, the APS 4 can further transmit the attestation check message to the attestation server 3 in steps S40 or S46 using a third network connection 9 to verify authenticity. The attestation server 3 can then transmit a result as the verification result back to the APS 4 in steps S41 or S47.

[0048] The attestation check message can be transmitted each time there is a change in the ESN value processed by the TEE 5. In this embodiment, there is a delivery of the EMM from the EMM server 2 via the untrusted software 6 to the TEE 5 in steps S37 or S43 (the EMM server 2 illustrated in Fig. 1 and Fig. 2). The TEE 5 detects an epoch transition and generates a request that is sent to the untrusted software 6 to verify software in steps S38 or S44.

[0049] In an embodiment, if the verification result is negative, the failure is logged by the CAS client device 1 and an alarm is initiated. The alarm, or failure log can be initiated after one or multiple negative verification results. Optionally, EMMs are no longer processed until a positive attestation verification result is achieved.

[0050] In certain embodiments as is shown in Fig. 12 and Fig. 13, the ESN value during the last successful verification result is persistently stored in step S49. As each EMM is processed, the ESN value from that EMM is compared to the sealed value of the ESN from the last successful verification result in steps S50-S52. In certain embodiments, an error occurs if the difference is beyond a desired threshold, i.e. if the EMM ESN value is larger than the sealed value of

the ESN by the desired threshold, the EMM is deleted or ignored and the CAS client device 1 is no longer authorized for any services.

[0051] In the case that the previous ESN value is not persistently stored, the TEE's reception of the first EMM will enforce that the attestation request S38 in Fig. 11 occurs during this instance of reception of the EMM. Alternatively, the ESN value is included in the persistently saved sealed unit information. In this embodiment, the TEE of Fig. 12 compares the ESN in the received EMM with the ESN in the sealed unit information. If the new ESN in the received EMM is greater than the saved value, step S44 of Fig. 12 will occur.

[0052] Fig. 14 is a schematic diagram of an exemplary CAS client device according to an embodiment of the present disclosure. It is contemplated by the present disclosure that the CAS client device 1 include electronic components or electronic computing devices operable to receive, transmit, process, store, and/or manage data and information associated with the systems and methods previously described, which encompasses any suitable processing device adapted to perform computing tasks consistent with the execution of computer-readable instructions stored in memory or computer-readable recording medium.

[0053] As shown in Fig. 14, the exemplary CAS client device 1 includes one or memories or memory locations including a main memory 30 and a protected memory 31 as well as an I/O interface 32, a user interface 33, a network interface 34, and one or more processors 35. The main memory 30 can be a random access memory (RAM), a memory buffer, a hard drive, a database, an erasable programmable read only memory (EPROM), an electrically erasable programmable read only memory (EEPROM), a read only memory (ROM), a flash memory, hard disk or any other various layers of memory hierarchy. The protected memory 31 is, for example, a processor reserved memory of dynamic random access memory (DRAM) or other reserved memory module or secure memory location maintained separate from the main memory 30.

[0054] The main memory 30 can be used to store any type of instructions associated with algorithms, processes, or operations for controlling the general functions of the CAS client device 1 including the operations of the untrusted software 7 as well as any operating system such as Linux, UNIX, Windows Server, or other customized and proprietary operating systems. The protected memory 31 on the other hand is used to store the TEE 5 and its associated

parameters such as device key sets, digital keys, certificates, and the like. The I/O interface 32 can be an interface for enabling the transfer of information between CAS client device 1 and external devices such as peripherals connected to the CAS client device 1 that need special communication links for interfacing with the one or more processors 35. The I/O interface 32 can be implemented to accommodate various connections to the CAS client device 1 that include, but is not limited to, a universal serial bus (USB) connection, parallel connection, a serial connection, coaxial connection, a High-Definition Multimedia Interface (HDMI) connection, or other known connection in the art connecting to external devices.

[0055] The user interface 33 is implemented for allowing communication between a user and the CAS client device 1. The user interface 33 includes, but is not limited to, a mouse, a keyboard, a liquid crystal display (LCD), cathode ray tube (CRT), thin film transistor (TFT), light-emitting diode (LED), high definition (HD) or other similar display device with touch screen capabilities. The network interface 34 is a software and/or hardware interface implemented to establish a connection between the CAS client device 1 and the servers 2, 3, 4 in

the system described in Fig. 1. It is contemplated by the present disclosure that that network interface 34 includes software and/or hardware interface circuitry for establishing communication connections with the rest of the system using both wired and wireless connections for establishing connections to, for example, a local area networks (LANs), wide area networks (WANs), metropolitan area networks (MANs) personal area networks (PANs), and wireless local area networks (WLANs), system area networks (SANs), and other similar networks.

[0056] The one or more processors 35 are used for controlling the general operations of the CAS client device 1. Each one or the one or more processors 35 can be, but are not limited to, a central processing unit (CPU), a hardware microprocessor, a multi-core processor, a single core processor, a field programmable gate array (FPGA), an application specific integrated circuit (ASIC), a digital signal processor (DSP), or other similar processing device capable of executing any type of instructions, algorithms, or software for controlling the operation of the CAS client device 1. Communication between the components of the CAS client device 1 (e.g., 30-35) are established using an internal bus 37.

[0057] Fig. 15 is a schematic diagram of an exemplary system server according to an embodiment. It is contemplated by the present disclosure that the server 40 shown in Fig. 15 is representative of the systems servers 2, 3, 4 shown in Fig. 1. It is also contemplated by the present disclosure that the server 40 includes electronic components or electronic computing devices operable to receive, transmit, process, store, and/or manage data and information associated with the systems and methods previously described, which encompasses any suitable processing device adapted to perform computing tasks consistent with the execution of computer-readable instructions stored in memory or computer-readable recording medium.

[0058] As shown in Fig. 15, the exemplary server 40 includes a main memory 41, an I/O interface 42, a user interface 43, a network interface 44, and one or more processors 45. The main memory 41 can be a random access memory (RAM), a memory buffer, a hard drive, a database, an erasable programmable read only memory (EPROM), an electrically erasable programmable read only memory (EEPROM), a read only memory (ROM), a flash memory, hard disk or any other various layers of memory hierarchy.

[0059] The main memory 41 can be used to store any type of instructions associated with algorithms, processes, or operations for controlling the general functions of the server 40 as well as any operating system such as Linux, UNIX, Windows Server, or other customized and proprietary operating systems. The I/O interface 42 can be an interface for enabling the transfer of information between server 40 and external devices such as peripherals connected to the server 40 that need special communication links for interfacing with the one or more processors 45. The I/O interface 42 can be implemented to accommodate various connections to the server 40 that include, but is not limited to, a universal serial bus (USB) connection, parallel connection, a serial connection, coaxial connection, a High-Definition Multimedia Interface (HDMI) connection, or other known connection in the art connecting to external devices.

[0060] The user interface 43 is implemented for allowing communication between a user and the server 40. The user interface 43 includes, but is not limited to, a mouse, a keyboard, a liquid crystal display (LCD), cathode ray tube (CRT), thin film transistor (TFT), light-emitting diode (LED), high definition (HD) or other similar display device with touch screen capabilities. The network

interface 44 is a software and/or hardware interface implemented to establish a connection between the server 40, and other servers in the system as well as well as with the CAS client device 1, as described in Fig. 1. It is contemplated by the present disclosure that that network interface 44 includes software and/or hardware interface circuitry for establishing communication connections with the rest of the system using both wired and wireless connections for establishing connections to, for example, a local area networks (LANs), wide area networks (WANs), metropolitan area networks (MANs) personal area networks (PANs), and wireless local area networks (WLANs), system area networks (SANs), and other similar networks.

[0061] The one or more processors 45 are used for controlling the general operations of the server 40. Each one or the one or more processors 45 can be, but are not limited to, a central processing unit (CPU), a hardware microprocessor, a multi-core processor, a single core processor, a field programmable gate array (FPGA), an application specific integrated circuit (ASIC), a digital signal processor (DSP), or other similar processing device capable of executing any type of instructions, algorithms, or software for

controlling the operation of the CAS client device 1. Communication between the components of the server 40 (e.g., 41-45) are established using an internal bus 46.

[0062] The present disclosure may be implemented as any combination of an apparatus, a system, an integrated circuit, and a computer program on a non-transitory computer readable recording medium. The one more processors may be implemented as an integrated circuit (IC), an application specific integrated circuit (ASIC), or large scale integrated circuit (LSI), system LSI, super LSI, or ultra LSI components which perform a part or all of the functions of the secure conditional access architecture.

[0063] The present disclosure includes the use of computer programs or algorithms. The programs or algorithms can be stored on a non-transitory computer-readable medium for causing a computer, such as the one or more processors, to execute the steps described in Figs 1-13. For example, the one or more memories stores software or algorithms with executable instructions and the one or more processors can execute a set of instructions of the software or

algorithms in association with executing generating, processing provisioning requests and provisioning messages, as described in Figs. 1-13.

[0064] The computer programs, which can also be referred to as programs, software, software applications, applications, components, or code, include machine instructions for a programmable processor, and can be implemented in a high-level procedural language, an object-oriented programming language, a functional programming language, a logical programming language, or an assembly language or machine language. The term computer-readable recording medium refers to any computer program product, apparatus or device, such as a magnetic disk, optical disk, solid-state storage device, memory, and programmable logic devices (PLDs), used to provide machine instructions or data to a programmable data processor, including a computer-readable recording medium that receives machine instructions as a computer-readable signal.

[0065] By way of example, a computer-readable medium can comprise DRAM, RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium that can be used to carry or store desired computer-readable program code in the

form of instructions or data structures and that can be accessed by a general-purpose or special-purpose computer, or a general-purpose or special-purpose processor. Disk or disc, as used herein, include compact disc (CD), laser disc, optical disc, digital versatile disc (DVD), floppy disk and Blu-ray disc where disks usually reproduce data magnetically, while discs reproduce data optically with lasers. Combinations of the above are also included within the scope of computer-readable media.

[0066] Use of the phrases "capable of," "capable to," "operable to," or "configured to" in one or more embodiments, refers to some apparatus, logic, hardware, and/or element designed in such a way to enable use of the apparatus, logic, hardware, and/or element in a specified manner.

[0067] The subject matter of the present disclosure is provided as examples of apparatus, systems, methods, and programs for performing the features of the secure conditional access architecture. However, further features or variations are contemplated in addition to the features described above. It is contemplated that the implementation of the components and functions of the present

disclosure can be done with any newly arising technology that may replace any of the above implemented technologies.

[0068] Additionally, the above description provides examples, and is not limiting of the scope, applicability, or configuration set forth in the claims. Changes may be made in the function and arrangement of elements discussed without departing from the spirit and scope of the disclosure. Various embodiments may omit, substitute, or add various procedures or components as appropriate. For instance, features described with respect to certain embodiments may be combined in other embodiments.

[0069] Various modifications to the disclosure will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other variations without departing from the spirit or scope of the present disclosure. Throughout the present disclosure the terms "example," "examples," or "exemplary" indicate examples or instances and do not imply or require any preference for the noted examples. Thus, the present disclosure is not to be limited to the examples and designs described herein but is to be accorded the widest scope consistent with the principles and novel features disclosed.

We claim:

1. A method for implementing an external trusted time source over a network to a conditional access system (CAS) client device, the method comprising:

transmitting an entitlement management message (EMM) to a trusted execution environment (TEE) of the CAS client device from an EMM server using a first network connection, the EMM including an epoch sequence number (ESN);

generating an updated remaining client key set (CKS) lifetime value in the TEE based on an initial lifetime duration value for the CKS, and the ESN value in the EMM;

sealing the CKS, updated ESN value in the EMM, and updated remaining CKS lifetime value as unit information; and

delivering the updated remaining CKS lifetime value and updated ESN value in the EMM from the TEE to untrusted software in the CAS client device, and

storing the updated remaining CKS lifetime value and updated ESN value.

2. The method according to claim 1, wherein the EMM is transmitted to the untrusted software before sending the EMM to the TEE.

3. The method according to claim 1, wherein the initial lifetime duration value for the CKS is delivered to the CAS client device as part of the CKS.

4. The method according to claim 1, wherein the initial lifetime duration value for the CKS is a pre-configured value that is part of a CAS client implementation.

5. The method according to claim 1, further comprising the step of initializing the remaining CKS lifetime value and ESN value when the first EMM is transmitted to the TEE after installing a CKS.

6. The method according to claim 1, wherein the TEE does not accept sealed unit information after a reboot unless it also contains an EMM related remaining CKS lifetime value and ESN value.

7. The method according to claim 1, wherein the EMM server moves to a next epoch transition over the course of a pre-defined epoch period, wherein the ESN in the EMM is incremented by M in value.

8. The method according to claim 7, further comprises updating the sealed unit information with the new incremented value for the ESN by M in value and decrementing the remaining CKS lifetime value by N in value.

9. The method according to claim 8, wherein when the remaining CKS lifetime value is at a lower bound when EMM is received by the TEE, the updated remaining CKS lifetime value in the TEE, and the ESN value in the EMM is not generated and the EMM is deleted or ignored.

10. The method according to claim 8, wherein the remaining CKS lifetime value is at a lower bound after the decrementing, the EMM is deleted or ignored and sealed unit information is sent with a remaining CKS lifetime value at the lower bound.

11. The method according to claim 7, wherein there is a time lapse between the last ESN received and the current ESN received from the EMM server so that the ESN is incremented X in value, wherein X is a multiple of M, further comprising decrementing the remaining CKS lifetime by Y, wherein the same value of the multiple of M for X, is the multiple of N for Y.

12. The method according to claim 11, wherein the remaining CKS lifetime value is at a lower bound after the decrementing, the EMM is deleted or ignored and sealed unit information is sent with a remaining CKS lifetime value at the lower bound.

13. The method according to claim 1, wherein the TEE is a first instance TEE, the method further comprising one or more instances of TEE including at least a second instance TEE, each instance of TEE comprising a different installed CKS, wherein the EMM server transmits a separate EMM with a separate ESN to each of the one or more instances of TEE, each of the one or more instances of TEE

generates an updated remaining CKS lifetime value based on the initial lifetime duration value for the CKS of each of the one or more instances of TEE, and the ESN value in the EMM for each of the one or more instances of TEE; sealing the CKS, updated ESN value in the EMM, and updated remaining CKS lifetime value as unit information in each of the one or more instances of TEE; and delivering the updated remaining CKS lifetime value and updated ESN value in the EMM from each of the one or more instances of TEE to untrusted software in the CAS client device, and storing the updated remaining CKS lifetime value and updated ESN value for each of the one or more instances of TEE.

14. The method according to claim 1, further comprising forming an attestation check message, and transmitting the attestation check message from the CAS client device to an attestation proxy server (APS) using a second network connection; and transmitting the attestation check response from the APS to the untrusted software using the second network connection, and sending the attestation check response from the untrusted software to the TEE.

15. The method according to claim 14, further comprising transmitting the attestation check message to an attestation server using a third network connection to verify authenticity, and transmitting from the attestation server a result as the verification result to the APS.

16. The method according to claim 15, wherein the attestation check message is transmitted each time there is a change in the ESN value in the sealed unit information in the TEE.

17. The method according to claim 16, wherein the verification result is negative, the failure is logged by the client device and an alarm is initiated.

18. The method according to claim 16, wherein the ESN value during the last successful verification result is persistently stored, and with each EMM that is transmitted, the EMM ESN value is compared to the sealed value of the ESN from the last successful verification result.

19. A non-transitory computer-readable recording medium in each of a client device and EMM server for implementing an external trusted time source over a network to a CAS client device, each non-transitory computer-readable recording medium storing one or more programs which when executed by a respective processor performs the method according to claim 1.

20. An apparatus for implementing an external trusted time source over a network to a conditional access system (CAS) client device, the apparatus comprising:

a non-transitory memory configured to store one or more programs, untrusted software, and a trusted execution environment (TEE);

a hardware processor configured to execute the one or more programs to perform operations of the untrusted software and the TEE; and

a network interface configured to establish communication with a network using a network connection,

wherein when the one or more programs are executed by the hardware processor:

the TEE of the CAS client device receives an entitlement management message (EMM) from an EMM server using the network connection, wherein the EMM includes an epoch sequence number (ESN),

the TEE generates an updated remaining client key set (CKS) lifetime value based on an initial lifetime duration value for the CKS, and the ESN value in the EMM,

the TEE seals the CKS, updated ESN value in the EMM, and updated remaining CKS lifetime value as unit information, and

the TEE delivers the updated remaining CKS lifetime value and ESN to untrusted software in the CAS client server, and stores the updated remaining CKS lifetime value.

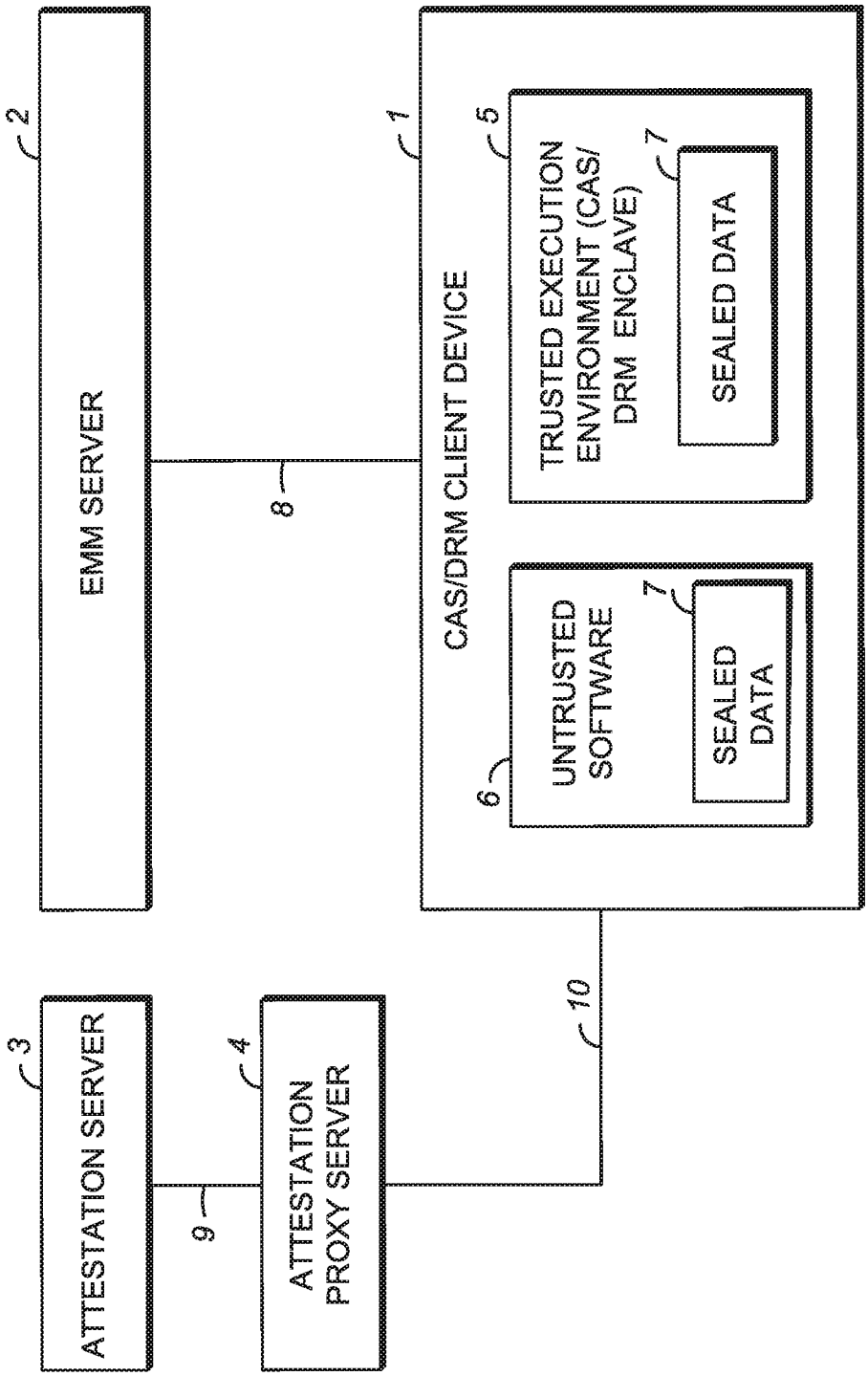
2
EMM SERVER
1
CAS/DRM CLIENT DEVICE
5
TRUSTED EXECUTION ENVIRONMENT (CAS/ DRM ENCLAVE)
7
SEALED DATA
6
UNTRUSTED SOFTWARE
7
SEALED DATA
8
3
ATTESTATION SERVER
4
ATTESTATION PROXY SERVER
9
10

FIG. 1

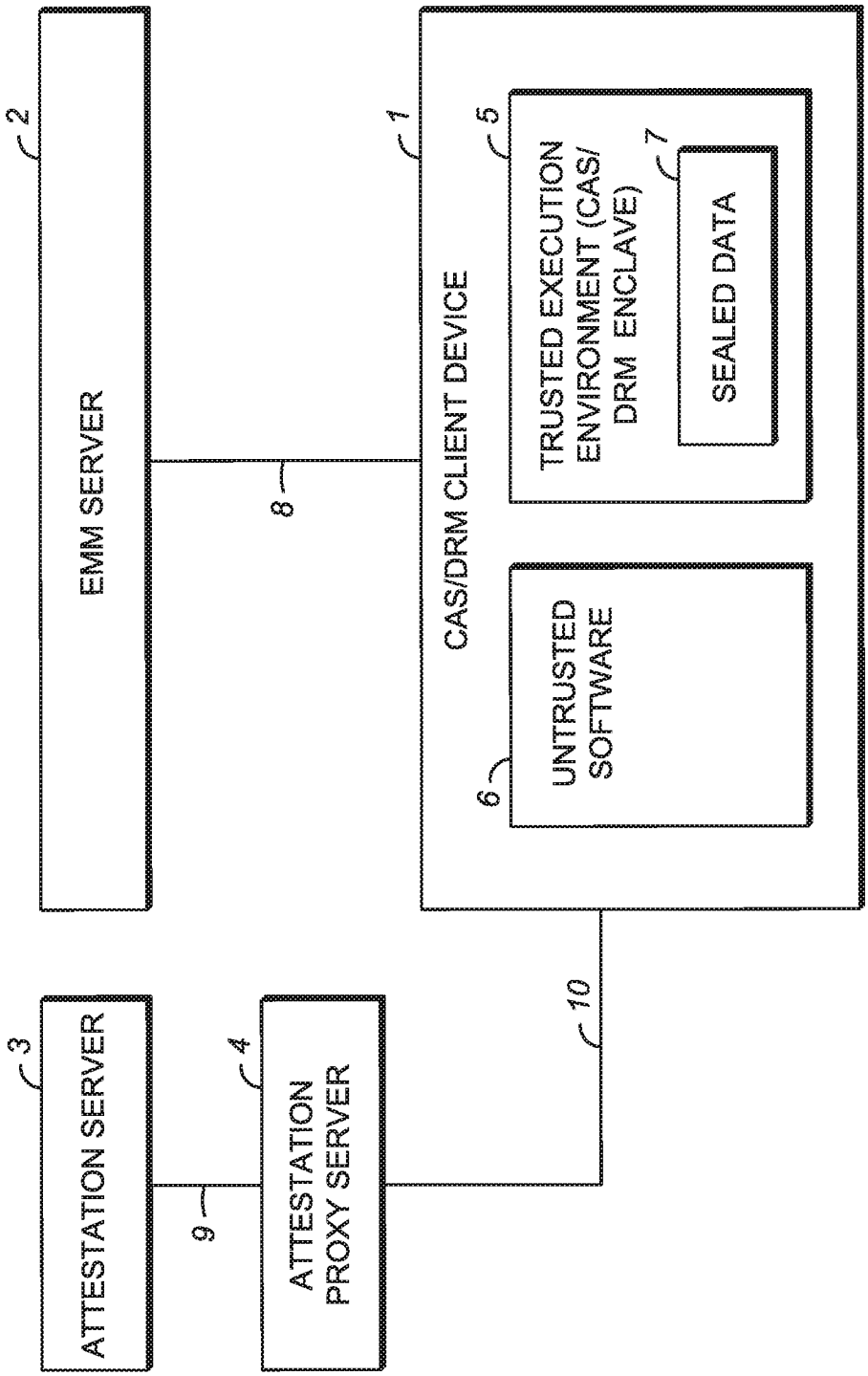
EMM SERVER
2
CAS/DRM CLIENT DEVICE
1
TRUSTED EXECUTION ENVIRONMENT (CAS/ DRM ENCLAVE)
5
SEALED DATA
7
UNTRUSTED SOFTWARE
6
8
ATTESTATION SERVER
3
ATTESTATION PROXY SERVER
4
9
10

FIG. 2

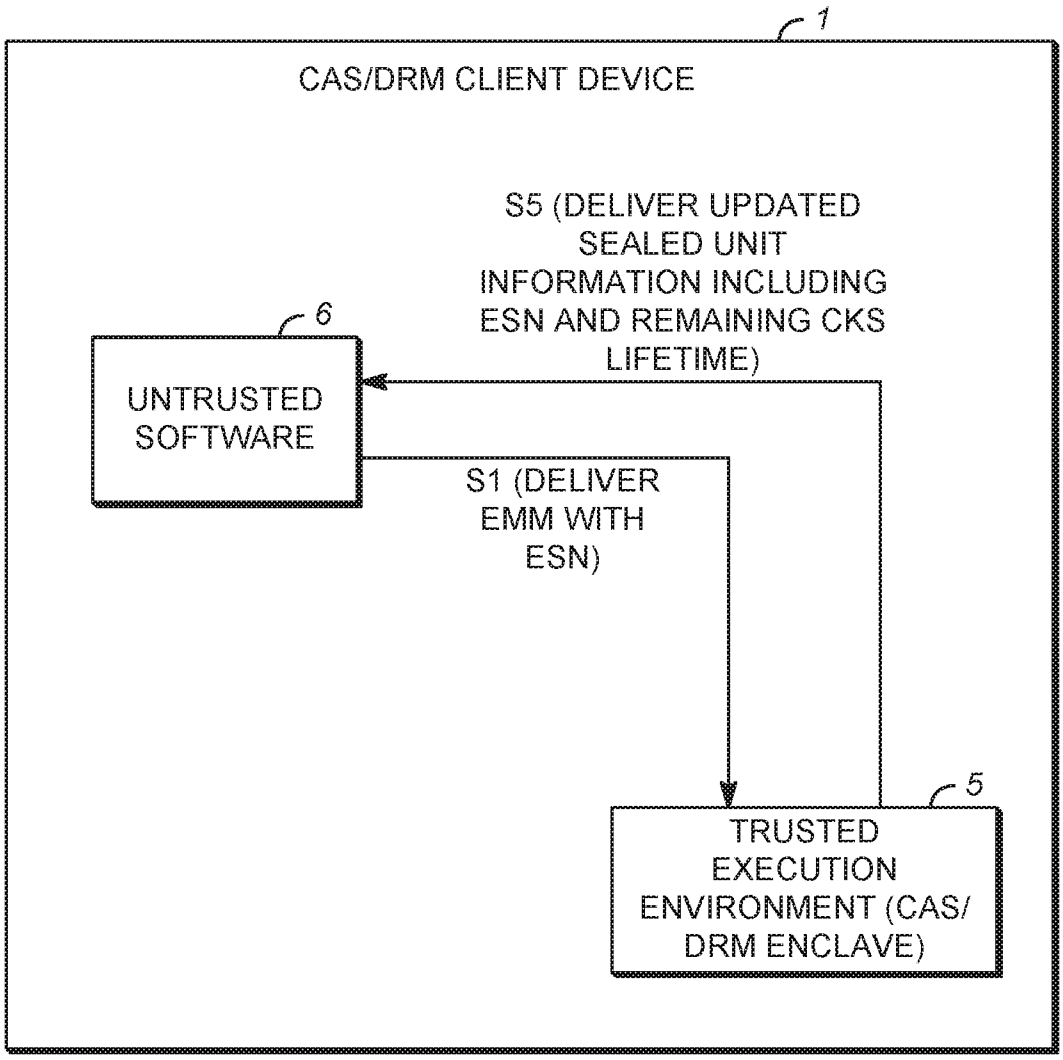
1
CAS/DRM CLIENT DEVICE
S5 (DELIVER UPDATED SEALED UNIT INFORMATION INCLUDING ESN AND REMAINING CKS LIFETIME)
6
UNTRUSTED SOFTWARE
S1 (DELIVER EMM WITH ESN)
5
TRUSTED EXECUTION ENVIRONMENT (CAS/DRM ENCLAVE)

FIG. 3

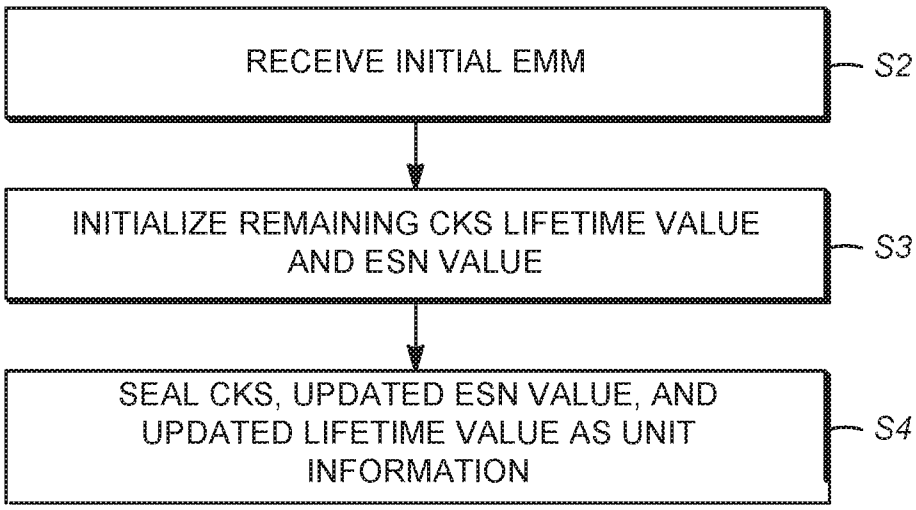
RECEIVE INITIAL EMM
S2
INITIALIZE REMAINING CKS LIFETIME VALUE AND ESN VALUE
S3
SEAL CKS, UPDATED ESN VALUE, AND UPDATED LIFETIME VALUE AS UNIT INFORMATION
S4

FIG. 4

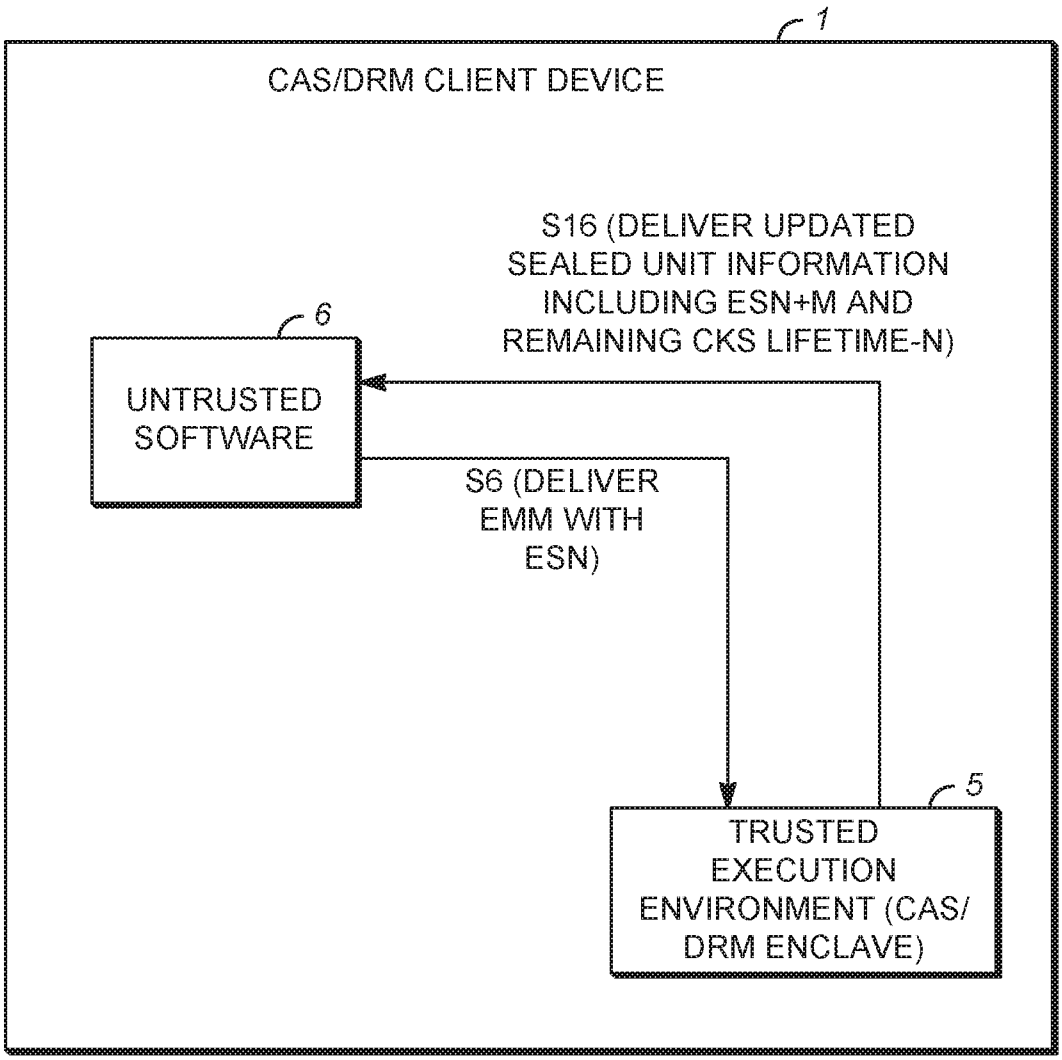
1
CAS/DRM CLIENT DEVICE
S16 (DELIVER UPDATED SEALED UNIT INFORMATION INCLUDING ESN+M AND REMAINING CKS LIFETIME-N)
6
UNTRUSTED SOFTWARE
S6 (DELIVER EMM WITH ESN)
5
TRUSTED EXECUTION ENVIRONMENT (CAS/ DRM ENCLAVE)

FIG. 5

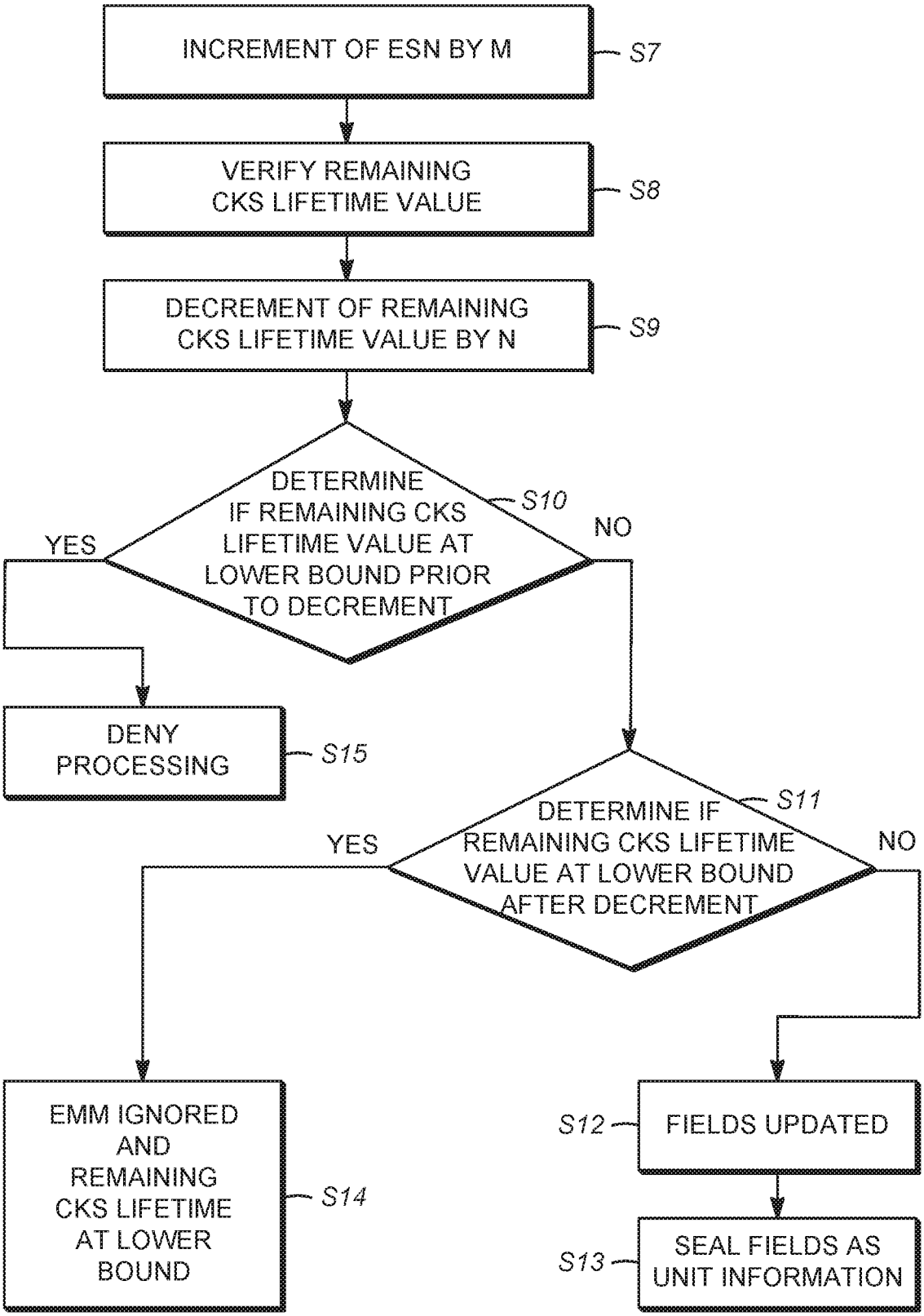
INCREMENT OF ESN BY M
S7
VERIFY REMAINING CKS LIFETIME VALUE
S8
DECREMENT OF REMAINING CKS LIFETIME VALUE BY N
S9
DETERMINE IF REMAINING CKS LIFETIME VALUE AT LOWER BOUND PRIOR TO DECREMENT
S10
YES
NO
DENY PROCESSING
S15
DETERMINE IF REMAINING CKS LIFETIME VALUE AT LOWER BOUND AFTER DECREMENT
S11
YES
NO
EMM IGNORED AND REMAINING CKS LIFETIME AT LOWER BOUND
S14
S12
FIELDS UPDATED
S13
SEAL FIELDS AS UNIT INFORMATION

FIG. 6

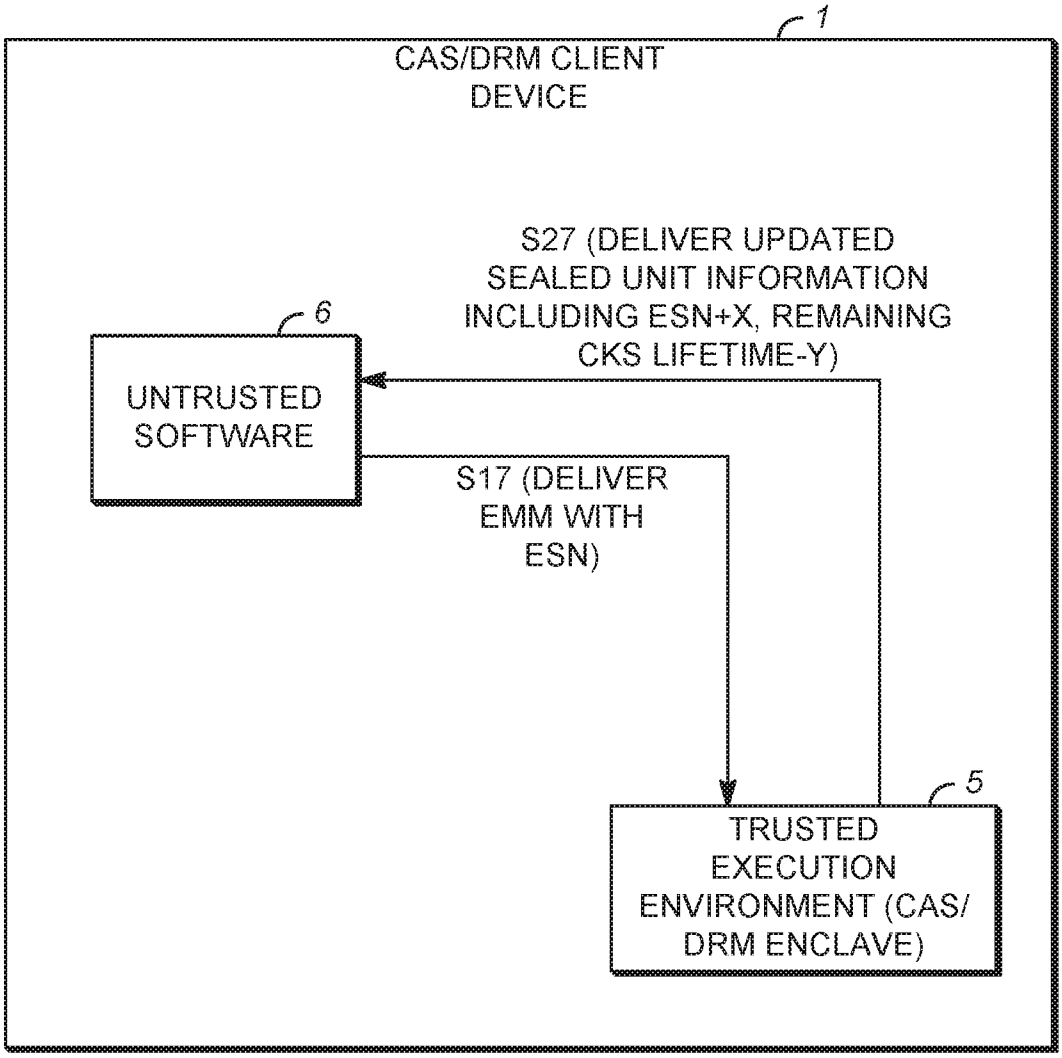
1
CAS/DRM CLIENT DEVICE
S27 (DELIVER UPDATED SEALED UNIT INFORMATION INCLUDING ESN+X, REMAINING CKS LIFETIME-Y)
6
UNTRUSTED SOFTWARE
S17 (DELIVER EMM WITH ESN)
5
TRUSTED EXECUTION ENVIRONMENT (CAS/ DRM ENCLAVE)

FIG. 7

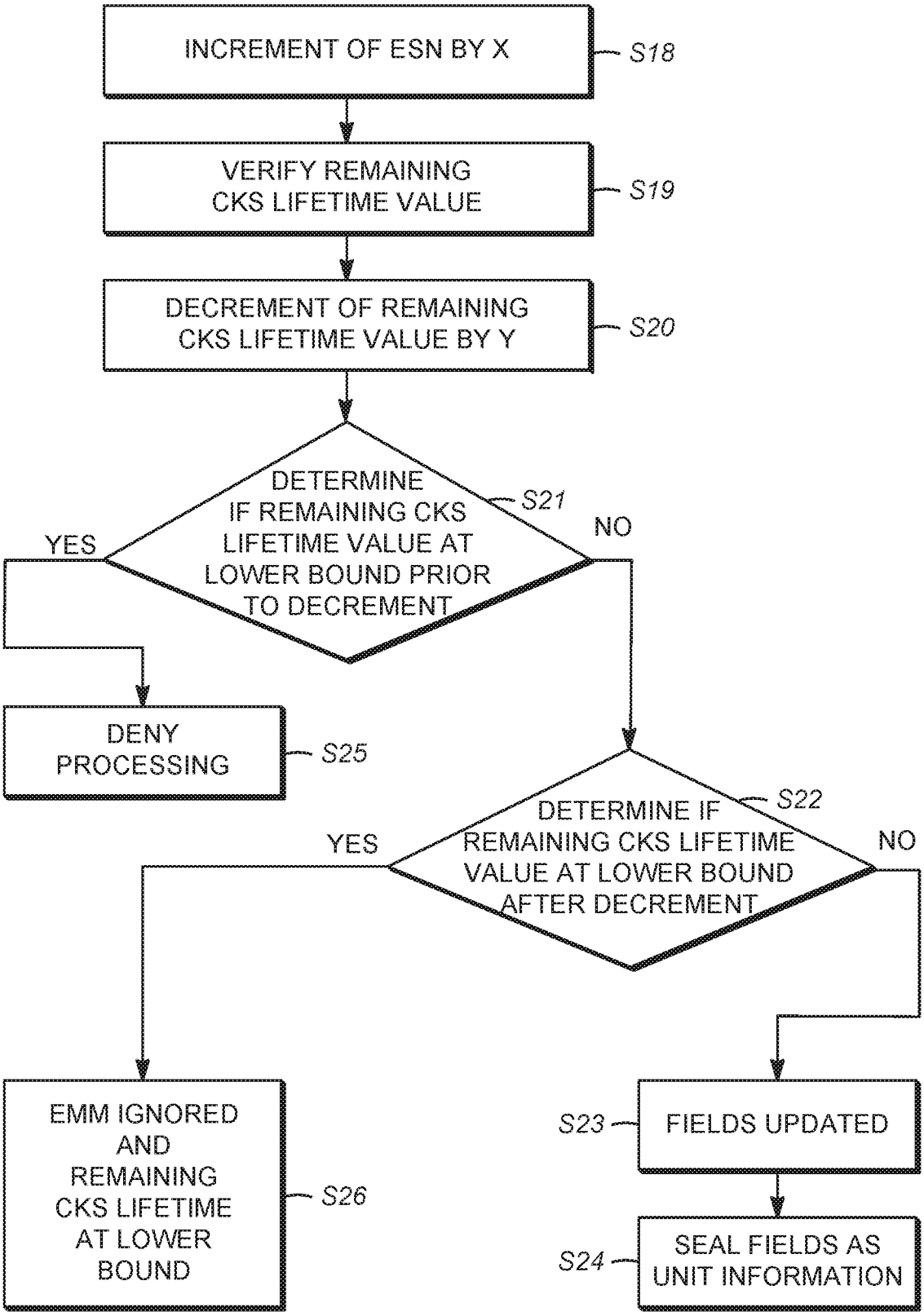
INCREMENT OF ESN BY X
S18
VERIFY REMAINING CKS LIFETIME VALUE
S19
DECREMENT OF REMAINING CKS LIFETIME VALUE BY Y
S20
DETERMINE IF REMAINING CKS LIFETIME VALUE AT LOWER BOUND PRIOR TO DECREMENT
S21
YES
NO
DENY PROCESSING
S25
DETERMINE IF REMAINING CKS LIFETIME VALUE AT LOWER BOUND AFTER DECREMENT
S22
YES
NO
EMM IGNORED AND REMAINING CKS LIFETIME AT LOWER BOUND
S26
S23
FIELDS UPDATED
S24
SEAL FIELDS AS UNIT INFORMATION

FIG. 8

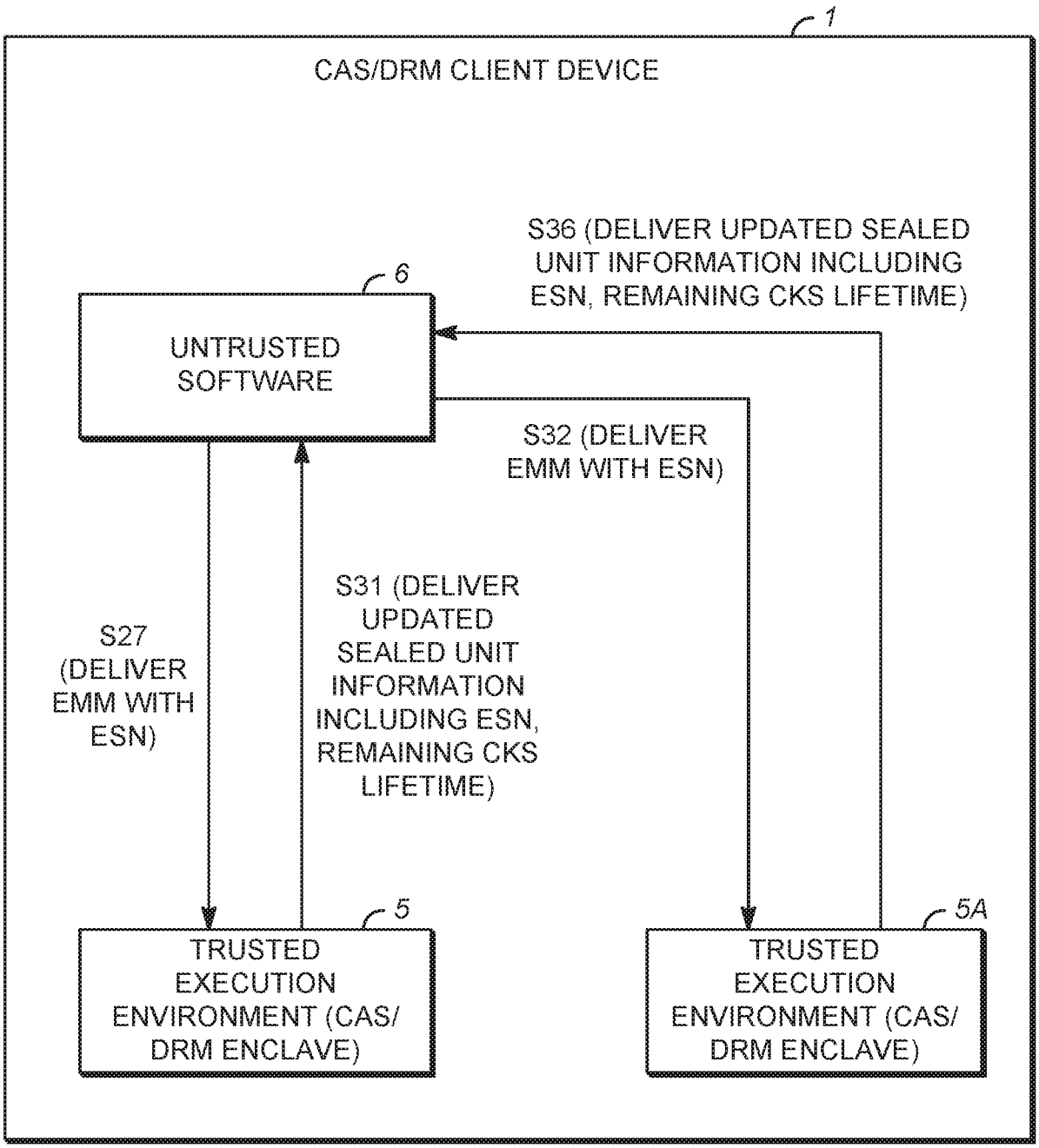
1
CAS/DRM CLIENT DEVICE
S36 (DELIVER UPDATED SEALED UNIT INFORMATION INCLUDING ESN, REMAINING CKS LIFETIME)
6
UNTRUSTED SOFTWARE
S32 (DELIVER EMM WITH ESN)
S31 (DELIVER UPDATED SEALED UNIT INFORMATION INCLUDING ESN, REMAINING CKS LIFETIME)
S27 (DELIVER EMM WITH ESN)
5
TRUSTED EXECUTION ENVIRONMENT (CAS/ DRM ENCLAVE)
5A
TRUSTED EXECUTION ENVIRONMENT (CAS/ DRM ENCLAVE)

FIG. 9

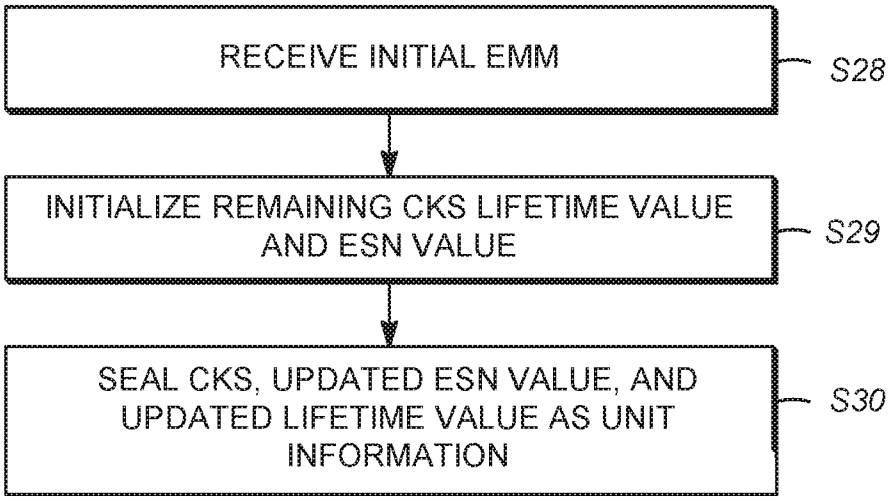

FIG. 10A

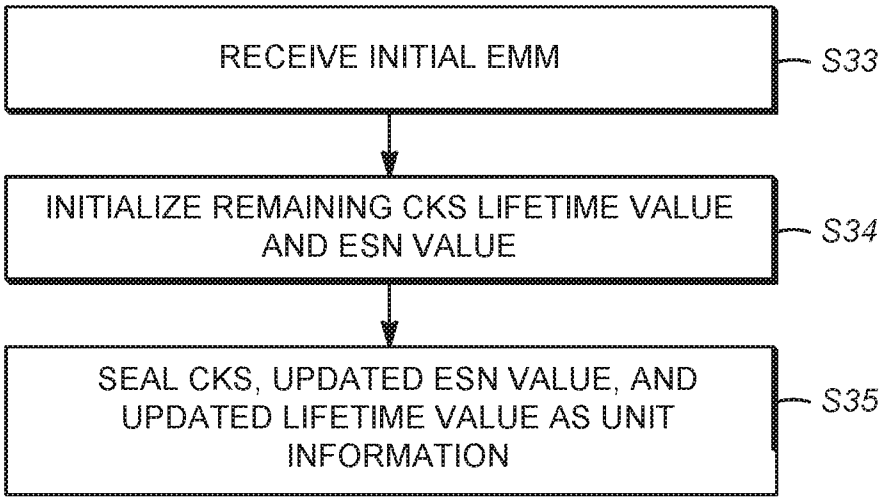

FIG. 10B

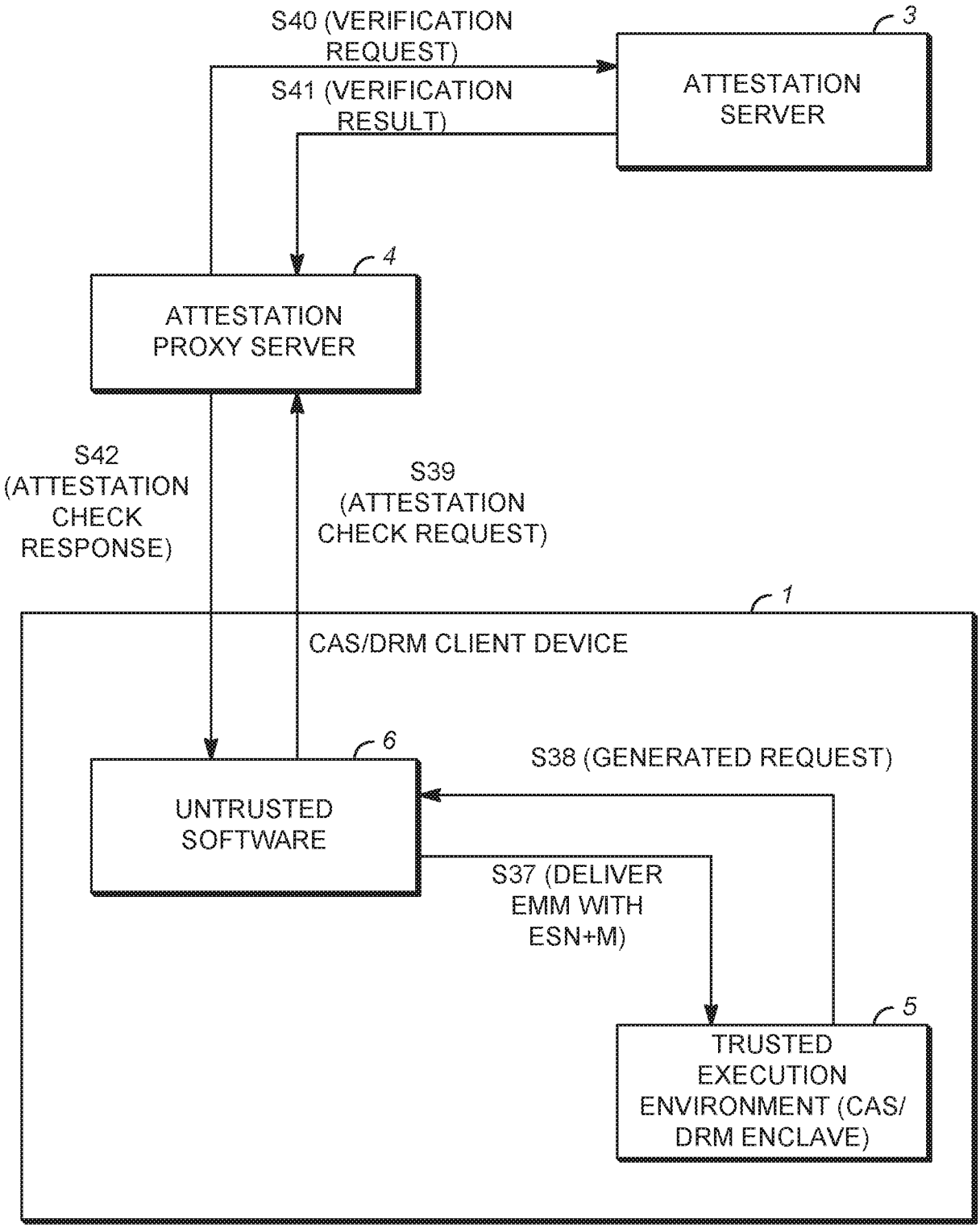
S40 (VERIFICATION REQUEST)
S41 (VERIFICATION RESULT)
3
ATTESTATION SERVER
4
ATTESTATION PROXY SERVER
S42 (ATTESTATION CHECK RESPONSE)
S39 (ATTESTATION CHECK REQUEST)
1
CAS/DRM CLIENT DEVICE
6
UNTRUSTED SOFTWARE
S38 (GENERATED REQUEST)
S37 (DELIVER EMM WITH ESN+M)
5
TRUSTED EXECUTION ENVIRONMENT (CAS/ DRM ENCLAVE)

FIG. 11

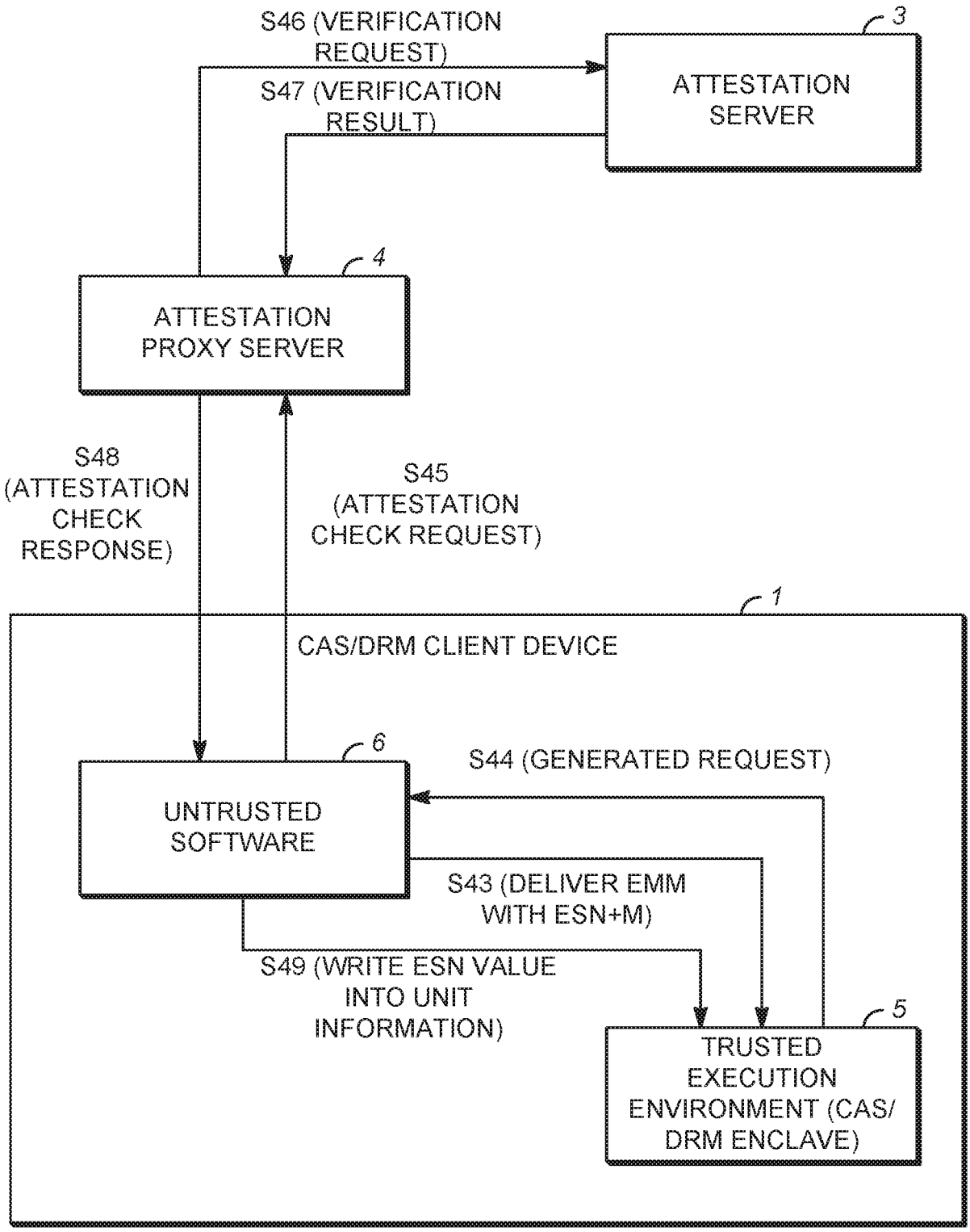
S46 (VERIFICATION REQUEST)
S47 (VERIFICATION RESULT)
3
ATTESTATION SERVER
4
ATTESTATION PROXY SERVER
S48 (ATTESTATION CHECK RESPONSE)
S45 (ATTESTATION CHECK REQUEST)
1
CAS/DRM CLIENT DEVICE
6
S44 (GENERATED REQUEST)
UNTRUSTED SOFTWARE
S43 (DELIVER EMM WITH ESN+M)
S49 (WRITE ESN VALUE INTO UNIT INFORMATION)
5
TRUSTED EXECUTION ENVIRONMENT (CAS/ DRM ENCLAVE)

FIG. 12

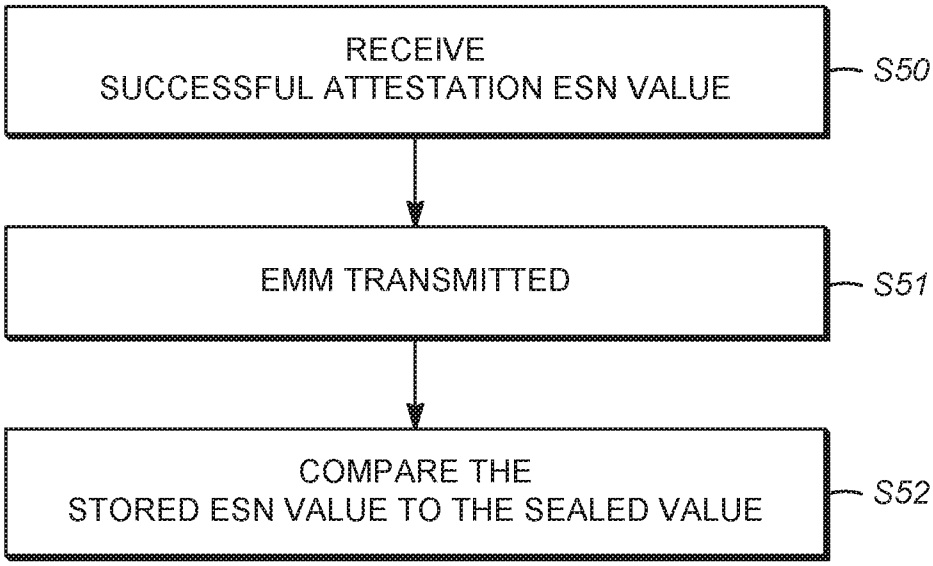
RECEIVE
SUCCESSFUL ATTESTATION ESN VALUE
S50
EMM TRANSMITTED
S51
COMPARE THE
STORED ESN VALUE TO THE SEALED VALUE
S52

FIG. 13

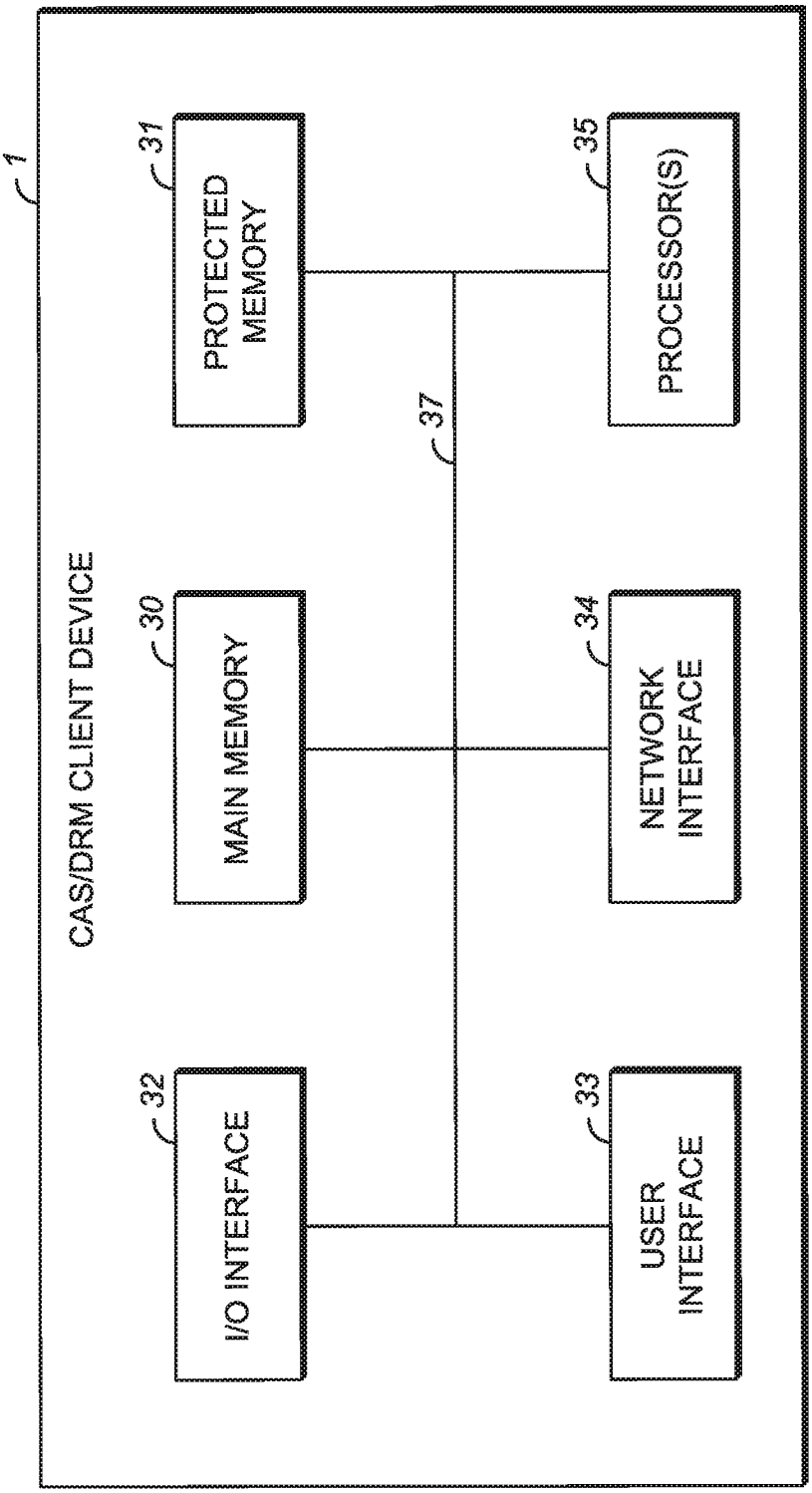
1
CAS/DRM CLIENT DEVICE
31
PROTECTED MEMORY
35
PROCESSOR(S)
37
30
MAIN MEMORY
34
NETWORK INTERFACE
32
I/O INTERFACE
33
USER INTERFACE

FIG. 14

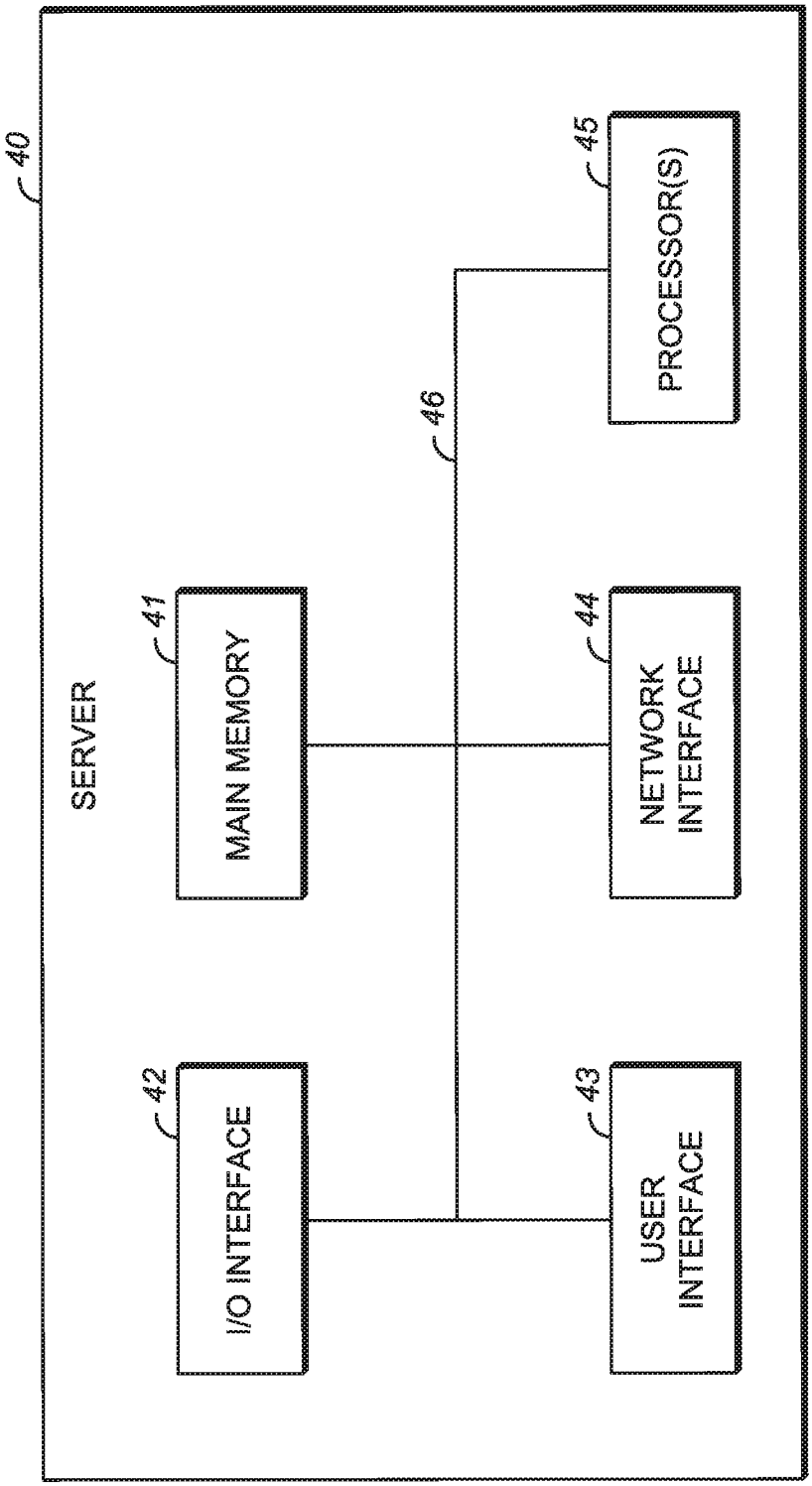
40
SERVER
41
MAIN MEMORY
42
I/O INTERFACE
43
USER INTERFACE
44
NETWORK INTERFACE
45
PROCESSOR(S)
46

FIG. 15

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2020/017476

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04N21/266 H04N21/418 H04N21/4367 H04N21/4623 H04N21/6543
H04N21/658 H04N21/43 G06F21/12 G06F21/72
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)
H04N 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.
A	US 2018/367829 A1 (SHENG ZHIFAN [CN] ET AL) 20 December 2018 (2018-12-20) figures 1-3 paragraph [0007] - paragraph [0016] paragraph [0052] - paragraph [0073] paragraph [0095] - paragraph [0100] -----	1-20
A	US 2018/189464 A1 (NARENDRA TRIVEDI ALPA T [US] ET AL) 5 July 2018 (2018-07-05) figures 1-4 paragraph [0013] - paragraph [0036] paragraph [0041] - paragraph [0044] -----	1-20
A	US 2014/095918 A1 (STAAHL PER [SE] ET AL) 3 April 2014 (2014-04-03) figures 2, 4-6 paragraph [0001] - paragraph [0007] paragraph [0032] - paragraph [0051] -----	1-20

-/--

[X] Further documents are listed in the continuation of Box C.

[X] 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
7 May 2020	15/05/2020

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Berthelé, P

1

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	TARATE NACHIKET: "Using ARM TrustZone to Implement Downloadable CAS Framework and Secure Media Pipeline in IPTV Client Devices", 2018 IEEE INTERNATIONAL SYMPOSIUM ON BROADBAND MULTIMEDIA SYSTEMS AND BROADCASTING (BMSB), IEEE, 6 June 2018 (2018-06-06), pages 1-11, XP033386061, DOI: 10.1109/BMSB.2018.8436855 [retrieved on 2018-08-14] page 1 - page 4	1-20

A	US 2014/033323 A1 (MORONEY PAUL [US] ET AL) 30 January 2014 (2014-01-30) figures 3, 5 paragraph [0016] - paragraph [0017] paragraph [0028] - paragraph [0031] paragraph [0037] paragraph [0050] - paragraph [0053]	1-20

A	CN 108 200 453 A (ACAD OF BROADCASTING SCIENCE SAPPRFT ET AL.) 22 June 2018 (2018-06-22) the whole document	1-20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2020/017476

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2018367829 A1	20-12-2018	CN 106851351 A	13-06-2017
		US 2018367829 A1	20-12-2018
		WO 2017092687 A1	08-06-2017
US 2018189464 A1	05-07-2018	NONE	
US 2014095918 A1	03-04-2014	CN 104620253 A	13-05-2015
		EP 2901362 A1	05-08-2015
		US 2014095918 A1	03-04-2014
		WO 2014048744 A1	03-04-2014
US 2014033323 A1	30-01-2014	US 2014033323 A1	30-01-2014
		WO 2014018895 A1	30-01-2014
CN 108200453 A	22-06-2018	NONE	