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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 November 2008 (20.11.2008)

PCT

(10) International Publication Number
WO 2008/139335 A1

(51) International Patent Classification:
H04L 9/00 (2006.01) *H04N 7/167* (2006.01)

(21) International Application Number:
PCT/IB2008/050541

(22) International Filing Date:
14 February 2008 (14.02.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
183151 13 May 2007 (13.05.2007) IL
184794 23 July 2007 (23.07.2007) IL

(71) Applicant *(for all designated States except US)*: **NDS LIMITED** [GB/GB]; 1 Heathrow Boulevard, 286 Bath Road, West Drayton Middlesex UB7 0DQ (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **TSURIA, Yossi** [IL/IL]; 14 Rabenu Polity Street, 93390 Jerusalem (IL). **SANDLER, Leonid** [IL/IL]; 117/10 Aharon Eshkoli Street, 97230 Jerusalem (IL). **BAR-ON, Gershon** [IL/IL]; Kochav Hashachar, 90641 (IL). **NACHMAN, Jacob** [IL/IL]; 3 HaTamar Street, 73127 Hashmonaim (IL). **DARSHAN, Ezra** [IL/IL]; 15B HaHavatzelet Street Nofei Aviv, 99590 Beit Shemesh (IL).

(74) Agent: **ZVIEL, David**; Director - Intellectual Property, NDS Technologies Israel Limited, 5 Shlomo Halevi Street, 97770 Jerusalem, (IL).

(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, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

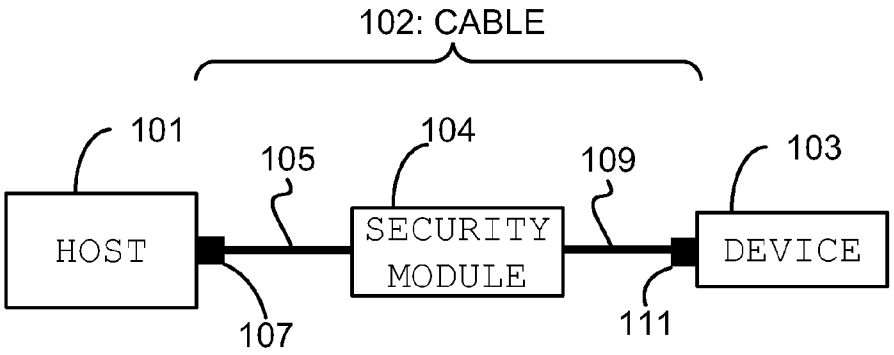
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: TRANSFERRING DIGITAL DATA

FIGURE 1



(57) Abstract: A cable (102) for transferring digital data from a host (101) to a device (103) is disclosed. The cable (102) comprises: a host connector (105/107) operable to connect the cable (102) to the host (101); a device connector (109/111) operable to connect the cable (102) to the device (103); and a data processor (104) disposed between the host connector (105/107) and the device connector (109/111), the data processor (104) comprising: a receiver operable to receive (a) encrypted digital data from the host (101), the encrypted digital data being encrypted according to a first encryption standard; and (b) first decryption information usable to decrypt the encrypted digital data; a decryptor operable to decrypt the encrypted digital data using the decryption information to form decrypted digital data; an encryptor operable to re-encrypt the decrypted digital data according to a second encryption standard to form re-encrypted digital data; and a transferrer operable to transfer the re-encrypted digital data and second decryption information usable to decrypt the re-encrypted digital data to the device (103).

WO 2008/139335 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

TRANSFERRING DIGITAL DATA

FIELD OF THE INVENTION

The present invention relates to methods and apparatus for transferring digital data from a host to a device.

BACKGROUND OF THE INVENTION

There is an increasing desire to provide digital data, and in particular multimedia content (e.g. audio/visual media content), on portable devices.

European patent application EP 1 571 556 describes a mobile terminal apparatus, which is a data processing apparatus. When downloading digital content from a server, rights data is acquired in addition to the content data that allows for the use of a first DRM system in the mobile terminal apparatus and a second DRM system in a memory card to where the digital content can be exported. When exporting the digital content to the memory card, the mobile terminal apparatus converts the rights data such that it will meet the second DRM system, and then outputs the content data and rights data as converted.

International patent application WO04/102459 describes a method, system and computer program product for transferring encrypted content and a corresponding license that are contained in a first device that uses a first Digital Rights Management (DRM) system to a second device that uses a second DRM system. One of the devices provides an Application Programming Interface (API) for importing and/or exporting the encrypted content and the corresponding license and the other device provides an application for transferring the encrypted content and the corresponding license.

European patent application EP 1 416 406 describes at least two terminal apparatuses which each uses content data in accordance with license information which is generated by a content distribution system to which it subscribes. A conversion apparatus includes a working area for storing license

information which is compatible with one of the terminal apparatuses, and a central processing section for converting the license information stored in the working area into license information which is compatible with the other terminal apparatus.

International patent application WO06/006014 describes a method, device, and system that use a transfer module that is distributed and used in a controlled manner. The transfer module has sufficient access rights to de-crypt and re-encrypt content to perform the unbinding and binding operations needed to transfer content from one terminal to another. The corresponding decryption key is transferred from the trusted party to the new device along with the transfer module.

United States Patent 5,729,204 describes a cable that allows a host device to selectively access and communicate with an associated peripheral device by establishing a data communication pathway therebetween. The cable includes one or more controllers responsive to the identifier signal designating the associated peripheral device, and establishes a communication pathway between the host device and the selected peripheral device in response to the appropriate identifier signal. The cable further includes a transceiver to transform the data signals into a transformed signal having a selected protocol compatible with at least the host device, e.g., RS-232 compatible signals.

Videoguard™ PMP, available from NDS Limited, One Heathrow Boulevard, 286 Bath Road, West Drayton, Middlesex, UB7 0DQ, UK, is a conditional access and DRM solution for portable media players (PMPs). Consumers can use a PMP to transfer content from a digital video recorder (DVR) to their PMP (via a USB 2.0 connection) or move content to their other devices (e.g. a PC).

The disclosures of all references mentioned above and throughout the present specification, as well as the disclosures of all references mentioned in those references, are hereby incorporated herein by reference.

SUMMARY OF THE INVENTION

There is provided in accordance with an embodiment of the present invention a cable for transferring digital data from a host to a device, the cable including a host connector operable to connect the cable to the host; a device connector operable to connect the cable to the device; and a data processor disposed between said host connector and said device connector, said data processor including: a receiver operable to receive (a) encrypted digital data from the host, the encrypted digital data being encrypted according to a first encryption standard; and (b) first decryption information usable to decrypt the encrypted digital data; a decryptor operable to decrypt the encrypted digital data using the decryption information to form decrypted digital data; an encryptor operable to re-encrypt the decrypted digital data according to a second encryption standard to form re-encrypted digital data; and a transferrer operable to transfer the re-encrypted digital data and second decryption information usable to decrypt the re-encrypted digital data to the device.

Preferably, the transferrer is operable to transfer the re-encrypted digital data directly to the device.

Alternatively, the transferrer is operable to transfer the re-encrypted digital data to the device via the host.

Preferably, the data processor is operable to transcode and/or transrate the digital data.

Preferably, the data processor is operable to apply a watermark to the digital data.

Preferably, the first encryption standard is DVB-CSA.

Preferably, the second encryption standard is an AES-based encryption algorithm.

Preferably, the first decryption information includes decryption keys usable to decrypt the digital data.

Preferably, the first decryption information includes control messages usable to derive decryption keys usable to decrypt the digital data.

Additionally, the cable preferably includes a smart card connector operable to connect the cable to a smart card, wherein the smart card uses the control messages to derive the encryption keys.

Preferably, the cable further includes a smart card, the smart card using the control messages to derive the encryption keys.

Preferably, the second decryption information includes decryption keys usable to decrypt the digital data.

Preferably, the second decryption information includes second control messages usable to derive decryption keys for decrypting the digital data.

Preferably, the digital data includes media content data.

There is also provided in accordance with an embodiment of the present invention a method of transferring digital data from a host to a device, wherein the host is connected to the device by a cable, the cable including a data processor, the method including the steps of: transferring digital data from the host to the data processor; processing the digital data in the data processor to form processed digital data; receiving (a) encrypted digital data from the host, wherein the encrypted digital data is encrypted according to a first encryption standard; and (b) first decryption information for decrypting the encrypted digital data; decrypting the encrypted digital data using the decryption information to form decrypted digital data; re-encrypting the decrypted digital data according to a second encryption standard to form re-encrypted digital data and transferring the processed digital data to the device.

Preferably, transferring the processed digital data includes transferring the re-encrypted digital data directly to the device.

Alternatively, transferring the processed digital data includes transferring the re-encrypted digital data to the device via the host.

Preferably, processing the digital data further includes transcoding and/or transrating the digital data.

Preferably, processing the digital data further includes applying a watermark to the digital data.

Preferably, the first encryption standard is DVB-CSA.

Preferably, the second encryption standard is an AES-based encryption algorithm.

Preferably, the first decryption information includes decryption keys usable to decrypt the digital data.

Preferably, the first decryption information includes control messages usable to derive decryption keys usable to decrypt the digital data.

Preferably, the cable further includes a smart card connector operable to connect the cable to a smart card, and wherein the smart card is operable to use the control messages to derive the encryption keys.

Preferably, the cable further includes a smart card, wherein the smart card is operable to use the control messages to derive the encryption keys.

Preferably, the second decryption information includes decryption keys usable to decrypt the digital data.

Preferably, the second decryption information includes second control messages usable to derive decryption keys for decrypting the digital data.

Preferably, the digital data includes media content data.

There is also provided in accordance with an embodiment of the present invention a cable for transferring digital data from a host to a device, the cable comprising: host connection means for connecting the cable to the host; device connection means for connecting the cable to the device; receiving means for receiving (a) encrypted digital data from the host, wherein the encrypted digital data is encrypted according to a first encryption standard; and (b) first decryption information for decrypting the encrypted digital data; decryption means for decrypting the encrypted digital data using the decryption information to form decrypted digital data; encryption means for re-encrypting the decrypted digital data according to a second encryption standard to form re-encrypted digital data; and transferral means for transferring the re-encrypted digital data and second decryption information for decrypting the re-encrypted digital data to the device.

Thus according to embodiments of the present invention, digital data can be securely transferred from a host to a device using a cable which can also process the digital data. The processing carried out on the digital data is done in the cable that connects the host to the device. The processing is carried out in

secure hardware, which is more secure than processing the digital data in software. According to preferred embodiments of the present invention, digital data encrypted according to a first encryption standard is transferred from the host to the device via the cable. The encrypted digital data is received in a data processor in the cable which decrypts the encrypted digital data, re-encrypts the digital data according to a second encryption standard and transfers the re-encrypted digital data to the device. Thus the cable can be used to transfer digital data between a host and a device that use differing encryption standards.

Related apparatus and methods are also described.

BRIEF DESCRIPTION OF THE DRAWINGS AND APPENDICES

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings wherein like reference numbers refer to like parts, and in which:

Figure 1 is a simplified pictorial illustration of a security system constructed and operative in accordance with preferred embodiments of the present invention;

Figure 2 is a simplified pictorial illustration of a security cable constructed and operative in accordance with a first embodiment of the present invention;

Figure 3 is a simplified pictorial illustration of the security module chip of the security cable of figure 2;

Figure 4 is an illustration of a method for processing digital data according to the first embodiment of the present invention;

Figure 5 is a simplified pictorial illustration of a security cable constructed and operative in accordance with a second embodiment of the present invention;

Figure 6 is a simplified pictorial illustration of the security module chip of the security cable of figure 5;

Figure 7 is an illustration of a method for processing digital data according to the second embodiment of the present invention;

Figure 8 depicts examples of devices found in typical home networking configurations as described in Appendix A;

Figure 9 depicts the distribution and use of SVP-protected content in a network spanning multiple domains of multiple users, as described in Appendix A;

Figure 10 shows the layers of SVP, as described in Appendix A;

Figure 11 illustrates the concept of an SVP acquisition point, as described in Appendix A;

Figure 12 shows an example of an SVP acquisition point, as described in Appendix A;

Figure 13 illustrates the concept of content licenses and crypto-periods, as described in Appendix A;

Figure 14 depicts a base-line ECM, as described in Appendix A;

Figure 15 shows the secure interaction of two SVP-compliant devices, as described in Appendix A;

Figure 16 shows a logical diagram of an SVP-compliant video processor found in a CE device that might receive and render content and then transfer the SVP-protected content to another SVP-compliant device, as described in Appendix A;

Figure 17 illustrates a certificate tree, as described in Appendix A;

Figure 18 illustrates a certificate revocation process, as described in Appendix A;

Figure 19 illustrates irreversible handoff from a proprietary system to an open SVP system, as described in Appendix A;

Figure 20 illustrates shared control between a proprietary system and an open SVP system, as described in Appendix A;

Figure 21 illustrates the establishment of an SAC via a challenge/response handshake protocol, as described in Appendix A;

Figure 22 illustrates the data structure of certificates, as described in Appendix A;

Figure 23 illustrates the fields of the first 320 bits of the BL-ECM structure, as described in Appendix A; and

Appendix A is a copy of the "SVP Open Content Protection System – Technical Overview" specification published by the SVP Alliance.

DETAILED DESCRIPTION OF EMBODIMENTS

Referring to figure 1, a security system comprising a host 101, device 103 and cable 102 is provided. Host 101 is connected to device 103 by the cable 102.

Embedded within the cable 102 is a security module 104, which includes software and hardware for processing digital data according to embodiments of the present invention. Security module 104 will be described in more detail below.

In addition to security module 104, the cable 102 comprises a host section 105 wherein one end of host section 105 is connected to the input of security module 104 and the other end of host section 105 is terminated by a host plug 107; the host plug 107 being used to connect the cable 102 to host 101. The cable 102 also comprises a device section 109 wherein one end of device section 109 is connected to the output of security module 104 and the other end of device section 109 is terminated by a device plug 111; the device plug 111 being used to connect the cable 102 to device 103.

According to the embodiments of the present invention that will now be described, and by way of example only:

host 101 comprises a digital video recorder (DVR) - a device that records digital video data without videotape to a hard drive based, digital storage medium. The term DVR is intended to include stand-alone set-top boxes and software for personal computers which enable video capture and playback to and from disk;

device 103 comprises a portable media player (PMP) – a portable device capable of storing and playing digital data files in one or more media formats (in embodiments of the present invention – pictures and/or video); and

the cable 102 comprises a universal serial bus (USB) cable, host plug 107 comprises a Series A or mini-A USB plug, and device plug 111 comprises Series B or mini-B USB plug. Other types of cable and/or plugs/receptacles to terminate the cable will be apparent to someone skilled in the art.

Referring to figure 2, security module 104 will now be described in more detail according to a first embodiment of the present invention. In the description that follows of this first embodiment of the present invention, security module 104 will be referred to as security module 1041. Security module 1041 comprises a USB hub 201 and a security module chip 203. USB hub 201 itself comprises an upstream port 205 and two downstream ports – downstream port 0 207 and downstream port 1 209. Upstream port 205 is connected to one end of host section 105 of the cable. Upstream port 105 is further connected to both downstream port 0 207 and downstream port 1 209. Downstream port 0 207 is connected to security module chip 203. Downstream port 1 209 is connected to one end of device section 109 of the cable. Preferably, security module chip 203 is a Secure Video Processor (SVP) compliant chip (i.e. it complies with Appendix A - the "SVP Open Content Protection System – Technical Overview" specification published by the SVP Alliance, the content of which is hereby incorporated herein by reference).

Referring to figure 3, security module chip 203 will now be described in more detail. Security module chip comprises USB port 301, application processor 303, secure processor 305 and DRM function 307. USB port 301 enables security module chip 203 to interface with downstream port 0 207 of USB hub 201. USB port 301 is connected to application processor 303. In this first embodiment, application processor 303 preferably comprises a reduced instruction set computer (RISC) microprocessor such as the ARM9 (available from ARM Limited, Cherry Hinton, Cambridge, United Kingdom) or ARC™600 (available from ARC International, Elstree, England). Application processor 303 manages the input digital data stream flowing into security module chip 203; manages the output digital data stream streaming out of security module chip 203; transfers the input and output streams between ports and memory (not shown);

prevents overflow and/or underflow of the input and output streams; filters and manages data management packets (e.g. extracts Entitlement Control Messages (ECMs) and Entitlement Management Messages (EMMs) from the input digital data stream); provides an interface to secure processor 305 for the digital data streams; and synchronises between the digital data streams and the secure processor 305 (e.g. sends ECMs to secure processor 305 at the correct time (i.e. just before the processing of the ECM by secure processor 305 is carried out) and sends EMMs to secure processor 305). Other operations carried out by application processor 303 will be apparent to someone skilled in the art.

Application processor 303 is connected to secure processor 305. In this first embodiment, secure processor 305 preferably also comprises an RISC microprocessor such as the ARM9 or ARC™600 as mentioned previously. Secure processor 305 performs various security functions such as encryption key negotiation with host 101 and secure local storage (e.g. of data resulting from the processing of EMMs) in, for example, an Electrically Erasable Programmable Read-Only Memory (EEPROM) (not shown).

Secure processor 305 is connected to DRM function 307, which is a cryptographic engine that is operable to decrypt and re-encrypt data, as will be described in more detail below. For example, DRM function 307 is operable to encrypt and re-encrypt data according to the Advanced Encryption Standard (AES) cipher algorithm in Cipher Block Chaining (CBC) Mode or Electronic Code Book (ECB) mode; the Data Encryption Standard (DES) and Triple DES cipher algorithms; and is operable to decrypt data that has been encrypted according to the Digital Video Broadcasting (DVB) Common Scrambling Algorithm (CSA) cipher algorithm.

Referring to figure 4, a method of securely transferring digital data from the host 101 to the device 103 using the cable according to this first embodiment of the present invention will now be described. In a first step 401, host 101 sends a control message to security module chip 203 in security module 1041 instructing security module chip 203 to perform certain processing operations, including (but not limited to): removal of encryption from digital data that is to be transferred under a global key and/or under a global encryption

algorithm (e.g. Digital Video Broadcasting – Common Scrambling Algorithm (DVB-CSA)); and application of encryption under a locally generated key and/or local encryption algorithm (e.g. Advanced Encryption Standard (AES)).

Then in step 403, host 101 sends the digital data to be transferred to device 103, together with associated information to security module chip 203 in security module 1041. In this first embodiment, the control words used to remove the global encryption are signalled in entitlement control messages (ECM) that secure processor 305 is operable to process in order to extract the control words that are to be used to decrypt the digital data. The associated information can either be transferred as part of the digital data stream or alternatively as a separate information stream. The digital data and associated information is received in security module 1041 at upstream port 205 of USB hub 201. USB hub 201 then outputs the digital data and associated information from downstream port 0 207 to security module chip 203.

Security module chip 203 receives the digital data and associated information at USB port 301 and passes it to application processor 303 for handling. Application processor knows from the earlier control message how to handle the digital data and associated information and passes the digital data and associated information to secure processor 305 for processing. In step 305, secure processor 305 (in conjunction with DRM function 307) performs the operations that it was instructed to perform, including: removal of global encryption from the received digital data (e.g. using encryption keys derived from the ECMs sent by host 101); and application of local encryption to the received, now unencrypted digital data (e.g. using AES). Preferably, the local keys used to encrypt the digital data are protected by packaging them as SVP base line ECMs (BL-ECM). BL-ECMs are standard (i.e. non-proprietary) ECMs that contain the local control words for decrypting the digital data.

Then, in step 407, secure processor 203 sends the digital data (that has had local encryption applied to it) and associated information (e.g. the associated BL-ECMs) back to host 101 via application processor 303, USB port 301, and downstream port 0 207 and upstream port 205 of USB hub 201. The BL-ECMs are transferred to host 101 over an SVP secure authentication channel

(SAC) that host 101 instructs security module 104 to establish. An SAC is a virtual communications channel established for the reliable private transfer of data and the process for establishing an SAC is described in Section 7, Appendix B of the "SVP Open Content Protection System – Technical Overview" specification published by the SVP Alliance and mentioned previously.

Upon receiving the digital data and associated information from security module 1041, host 101 sends the digital data and associated information to device 103 via security module 1041 (step 409). The digital data and associated information is received in security module 1041 at upstream port 205 of USB hub 201. USB hub 201 then outputs the digital data and associated information from downstream port 1 209 to device 103. The associated information is transferred to device 103 over an SVP SAC.

Upon receiving the digital data and associated information, device 103 processes the content (e.g. removes the local encryption using keys derived from the received BL-ECMs, decodes the digital data, renders the content for display, etc.) (step 411)

Thus, according to the above described first embodiment of the present invention, digital data can be securely transferred from host 101 to device 103 via the cable. This method is particularly useful for hosts that only have a limited number of output ports (e.g. a single USB port). In this first embodiment, it will be appreciated that security module 1041 does not contain any USB host controllers or accompanying USB host controller software. Less processing power is therefore required of security module 1041. However, it will also be appreciated that host 101 transfers digital data three times over its USB port: to security module 1041, back from security module 1041 and to device 103.

Referring to figure 5, security module 104 will now be described in more detail according to a second embodiment of the present invention. In the description that follows of this second embodiment of the present invention, security module 104 will be referred to as security module 1042. Security module 1042 comprises a security module chip 501. Security module chip 501 comprises a USB device module503 and a USB host module 505. USB device module 503 is

connected to one end of host section 105 of the cable. USB host module 505 is connected to one of end device section 109 of the cable.

With reference to figure 6, security module chip 501 further comprises application processor 601 (which is equivalent to application processor 303 of figure 3). Application processor 601 is connected to secure processor 603 (which is equivalent to secure processor 305 of figure 3). Secure processor 605 is connected to DRM function 605 (which is equivalent to DRM function 307 of figure 3). USB device module 503 and USB host module 505 are both connected to application processor 601.

Referring to figure 7, a method of securely transferring digital data from the host 101 to the device 103 using the cable according to this second embodiment of the present invention will now be described. In a first step 701, host 101 sends a control message to security module chip 501 in security module 1042 instructing security module chip 501 to perform certain operations, including (but not limited to): removal of encryption from digital data that is to be transferred under a global key and/or under a global encryption algorithm (e.g. Digital Video Broadcasting – Common Scrambling Algorithm (DVB-CSA)); and application of encryption under a locally generated key and/or local encryption algorithm (e.g. Advanced Encryption Standard (AES)).

Then in step 703, host 101 sends the digital data to be transferred to device 103, together with associated information to security module chip 501 in security module 1042. In a similar way to that described above in relation to the first embodiment, in this second embodiment, the control words used to remove the global encryption are signalled in entitlement control messages (ECM) that secure processor 603 is operable to process in order to extract the control words that are to be used to decrypt the digital data. The associated information can either be transferred as part of the digital data stream or alternatively as a separate information stream. The digital data and associated information is received in security module 1042 at USB device module503 which passes the digital data and associated information to application processor 601. Application processor knows from the earlier control message how to handle the digital data and associated

information and passes the digital data and associated information to secure processor 603 for processing.

In step 705, secure processor 603 (in conjunction with DRM function 605) performs the operations that it was instructed to perform, including: removal of global encryption from the received digital data (e.g. using encryption keys derived from the ECMs sent by host 101); and application of local encryption to the received, now unencrypted digital data (e.g. using AES). Preferably, the local keys used to encrypt the digital data are protected by packaging them as SVP base line ECMs (BL-ECM).

Then, in step 707, secure processor 403 sends the digital data (that has had local encryption applied to it) and associated information (e.g. the associated BL-ECMs) to device 103 via application processor 601 and USB host module 505. The associated information is transferred to device 103 over an SVP SAC that host 101 instructs security module chip 501 to establish.

Upon receiving the digital data and associated information, device 103 processes the content (e.g. removes the local encryption using keys derived from the received BL-ECMs, decodes the digital data, renders the content for display, etc.) (step 709)

Thus, according to the above described second embodiment of the present invention, digital data can be securely transferred from host 101 to device 103 via the cable. This method is again particularly useful for hosts that only have a limited number of output ports (e.g. a single USB port). In this second embodiment, it will be appreciated that host 101 transfers digital data over its USB port only once: to security module 1042. This is more efficient and represents less load on host 101 compared with the above described first embodiment where, it will be remembered, host 101 transfers digital data over its USB port three times. However, it will also be appreciated that the inclusion of USB host module 505 in security module chip 501 increases the level of processing power required from security module chip 501 since managing a USB host module takes more power than managing a USB device module (of which USB hub 201 is an example). Inclusion of a USB host module 505 in security module chip 501 may also

increase the cost of security module chip 501 and increase the complexity of the software running in security module chip 501.

It will be apparent from the foregoing description that many modifications or variations may be made to the above described embodiments without departing from the invention. Such modifications and variations include:

In the above described embodiments, it was assumed that the encoding of the digital data was suitable for both host 101 and device 103 (e.g. Moving Pictures Expert Group-2 (MPEG-2) or MPEG-4). In alternative embodiments, device 103 may not have the capability to decode and render digital data in the format from which it is output by host 101. In such alternative embodiments, security module chip 203/501 is configured to transcode the digital data it receives from host 101 before sending it to device 103. Transcoding is the direct digital-to-digital conversion from one codec to another. It involves decoding/decompressing the original data to a raw intermediate format (i.e. PCM for audio or YUV for video), in a way that mimics standard playback of the content, and then re-encoding the raw intermediate formatted data into the target format.

Security module chip 203/501 is operable to decode the digital data received from host 101 and re-encode it in an encoding format that device 103 is able to decode and render for display. For example, device 103 may not have the capability to decode and render digital data in the MPEG-2 format from which it is output by host 101. In such a case, security module chip 203/501 is configured to transcode the digital data it receives from host 101 from MPEG-2 format to MPEG-4 format before sending it to device 103. Preferably, the message sent from host 101 in steps 401/701 as described above instructs security module chip 203/501 to transcoded the digital data.

Transcoding can also refer to the encoding of files to a lower or higher bit rate without changing the video formats of the files, a process that is also known as transrating.

In alternative embodiments, security module chip 203/501 is also configured to apply a watermark to the digital data received from host 101 before transferring it to device 103. The watermark is unique to the security module chip

203/501, may or may not be visible in the rendered digital data, does not affect normal viewing of the digital data but can be extracted from the digital data stream. Thus digital data can be traced back to individual security module chips (i.e. back to individual cables) and therefore if hacked digital data is discovered, the originator of such hacked digital data can be identified.

In some embodiments, the digital data that is to be transferred from host 101 to device 103 may be 'in-the-clear', i.e. unencrypted. In such embodiments, security chip module 203/501 may be configured just to transcode and/or transrate the content and/or apply a watermark to the digital data.

In the above described embodiments, the digital data that is to be transferred from host 101 to device 103 is encrypted under a global key and/or under a global encryption algorithm. In some embodiments, such global encryption could be part of a Digital Rights Management (DRM) scheme and the host 101 would then transfer DRM license data rather than ECMs as described above. The DRM license data contains the requisite data for extracting the encryption keys. In the above described embodiments, security module chip 203/501 was operable to derive encryption keys from ECMs sent by host 101 in order to remove the global encryption from the received digital data. In alternative embodiments, a smart card in host 101 is operable to process the ECMs in order to derive the decryption keys from the ECMs. In such an embodiment, security module chip 203/501 is operable to establish a secure communications channel with the smart card in host 101 (e.g. an SVP SAC), send the ECMs to the smart card for processing by the smart card and receive the decryption keys from the smart card.

In another embodiment, security module 104 further comprises a smart card (e.g. a subscriber identity module (SIM) card) that is operable to process the ECMs received from host 101 in order to derive the keys to descramble the received, globally encrypted digital data.

In yet another embodiment, security module chip 203/501 further comprises a smart card port enabling a removable smart card to be connected to security module 104 (e.g. plugged into security module 104). The smart card port preferably complies with ISO 7816 – an international standard related to electronic

identification cards, especially smart cards, managed jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

The above described embodiments where security module 104 includes a smart card or can be connected to a smart card that is not a smart card in the host 101 is particularly useful in situations where host 101 is only operable to receive and decrypt one broadcast stream but a user wishes to receive two broadcast streams simultaneously (e.g. to view one and to record one). Host 101 can be configured to process one of the broadcast streams and the other broadcast stream can be offloaded and transferred to device 103 (with security module 104 carrying out the processing of the offloaded broadcast stream).

In the above described embodiments, device 103 comprises a portable media player (PMP). In alternative embodiments, device 103 comprises an external storage device (e.g. a USB mass storage device) configured to store the digital data.

Although the above described embodiments related to the transfer of media content data, it will be apparent to someone skilled in the art that the methods of transferring digital data using the cable are equally applicable to any form of digital data which is to be transferred between two devices.

It is appreciated that various features of the invention which are, for clarity, described in the contexts of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable subcombination.

It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the invention is defined only by the claims which follow:

APPENDIX A

SVP Open Content Protection System

Technical Overview

1 Introduction

The SVP specification describes how to protect digital video content by adding security enhancements to a standard video processor making it a Secure Video Processor. Developed for use on home networks and portable devices, SVP enables flexible and fair content consumption by consumers while protecting against indiscriminate content proliferation. SVP extends the rights and business reach of content owners, and operators by securely protecting content on any SVP-compliant device. Under SVP, digital content is protected end-to-end such that clear content resides only inside the secure SVP-compliant media chip. The superior security offered by SVP-compliant devices enables high quality content storage and consumption and thus increases the utility of such devices to consumers. Moreover, SVP's interoperability with other approved content protection systems provides for a seamless, friendly consumer experience while maintaining adequate content protection.

Figure 8 depicts the types of devices that can be found in typical home networking configurations.

SVP capability consists of content protection functionality that adds but a small incremental cost to standard video processing chips. A standard video processor with this additional functionality is known as a *Secure* Video Processor or SVP-compliant chip. The SVP solution is not based on any global secret that can jeopardize the entire solution; each SVP is personalized so that a hack of a single SVP chip is just that. In contrast to other content protection systems that protect individual links, or are software-based, SVP protects the content end-to-end within secure silicon container.

SVP is:

- The key to secure end-to-end control of content in the home network
- A hardware-based specification that protects digital content throughout the entire content-use chain; the protection matches and often exceeds that of premium content in pay-TV systems
- Economical, requiring a relatively small number of gates added to a standard video processing chip
- Interoperable with other approved content protection (CP) systems

SVP works by:

- Separating content protection from business model management offered by conditional access or digital rights management systems
- Keeping the content, its keys, and license persistently protected until rendering
- Defining rights in a standard tamper-resistant license
- Issuing each device a unique Device Certificate
- Allowing network operators to entitle each device with multiple Network-Operator Certificates
- Accepting content from multiple, compliant acquisition points and exporting content to other, approved CP systems.

As a hardware-based solution, SVP enhances security while making security easy and economical to standardize. An SVP-compliant chip can be embedded in any digital device, including set-top boxes, digital TVs, PVRs, and other portable devices. There is no need for significant customization for different types or models.

1.1 SVP Licensing

SVP is licensed in a fair, reasonable, and non-discriminatory manner through the SVP Licensing Authority (SVPLA). The SVPLA is a limited corporation, wholly owned by NDS Ltd., that licenses all intellectual property rights and technology required to implement an SVP-compliant product or system. The goal of the SVPLA is to establish a standard that will promote a level playing field for all parties interested in SVP compliance. For example, any eligible party can become a licensee and build an SVP-compliant chip or CE device based on the license signed. Similarly, any CA or DRM provider can build its own SVP headend or create its own network certificates. Licensees may also build private extensions.

The SVPLA works in close coordination with the SVP Alliance, an independent, not-for-profit corporation that oversees the SVPLA. Leading players in the digital entertainment industry, SVP Alliance members include content owners and distributors, network operators, consumer electronics manufacturers, IC manufacturers, IT and telecommunication companies, and conditional access and digital rights management companies. Membership in the SVP Alliance provides opportunities to influence the future direction of the technology and to participate in trade events, conferences, press briefings, and promotional events related to SVP technology.

2 How an SVP System Works

In general, an SVP-compliant home network receives content from external sources (as shown in Figure 9), imposes SVP protection on that content, and handles the content according to a defined set of rules. These rules are derived from specification contained in the content's specific content license and the SVP Device Certificate.

An SVP-compliant network gives SVP protection to all content. In general, content received in the clear (free-to-air) is scrambled with SVP's native scrambling algorithm before being stored or sent between devices on an SVP-compliant network.

Figure 9 depicts the distribution and use of SVP-protected content in a network spanning multiple domains[1] of multiple users, over large distances, where proximity control[2] may be implemented.

An acquisition[3] point generates the initial SVP Content License based on usage rights and restrictions received with the content (e.g., rights and restrictions received from a CA/DRM system or from Broadcast Flag markings). Thereafter, content protection occurs in the SVP-compliant chip, which, as shown, can be embedded in any digital device, including set-top boxes, TVs, DVRs, PDAs, and other portable devices. Devices are characterized by their basic content functionality—storing, rendering, and so forth.

2.1 The Different Roles of Content Protection and CA/DRM

CA/DRM is responsible for enforcement and secure monetization of the business model associated with content. For example, purchase of a pay per view event is handled by CA/DRM systems. In the SVP paradigm, content protection is applied in the post-monetization content control phase. Specifically, content protection relates to the enforcement of such content usage rights as copying/moving,

[1] Concerning domains, see Section 2.6.

[2] Concerning proximity control, see Section 2.7.

[3] Concerning acquisition, see Section 2.2.

distribution, temporal access, consumption, and export of content control.

An approved CA/DRM technology can introduce content to the SVP by mapping its CA/DRM rights to SVP-defined rights by means of the SVP acquisition (as explained in section 2.2). Interaction is enabled between the two systems such that the CA/DRM system controls all monetization of content and passes the rules to the SVP system.

Figure 10 shows the layers of SVP and illustrates how SVP content protection operates in a separate layer from that of the CA/DRM.

2.2 Acquisition

Acquisition is the process of creating the initial SVP Content License for a specific piece of content. Acquisition is often performed by a mapping of external CP rules to an SVP-compliant Content License, and this done by an SVP-compliant acquisition point. For example, in pay-TV environments,[4] content is usually sent scrambled and accompanied by a CA license encapsulated in entitlement control messages (ECMs).[5] ECMs have an additional function—descrambling keys are also derived from ECMs. ECMs are delivered to users in parallel with associated content.

In a typical DVB system, ECMs are changed frequently—perhaps every ten seconds—throughout a live event.[6] Each period covered by one ECM is called a *crypto-period*, and each new ECM means a new scrambling key for the crypt-period that it covers. A new ECM can also reflect a change in content usage rules.

The external content rules received in ECMs together with the Device Certificate determine the content usage rights (how the content may be used). When content arrives at an SVP-compliant system, its content rules must be mapped to an SVP-compliant Content License,[7]

---

[4] Even free-to-air content may be accompanied by content control criteria that may be required by regulators or Operators (such as "Broadcast Flag" or similar.)

[5] DVB terminology is used here for the sake of convenience. However, the SVP standard is compatible with DSS and other standards as well.

[6] So, for example, an hour-long event would be associated with approximately 360 ECMs.

[7] For information on the Content License, see "Content License—CSLs and BL-ECMs" later in this section.

which will then accompany the content wherever it remains under SVP protection.

As shown in Figure 11, the component that performs acquisition is known as an *acquisition point*. An SVP-compliant acquisition point meets the SVP specification requirement for mapping external Content Licenses to SVP-compliant Content Licenses and forwarding the newly-created SVP licenses to an SVP-compliant chip. The devices that house them are therefore known as *acquisition devices*. Typical acquisition devices are smart cards and cable cards. An acquisition point can be embedded within an acquisition device provided that the device meets the SVP compliance and robustness rules for acquisition points.

Figure 12 shows an example of an SVP acquisition point. The broadcast CA acquisition point receives external content rules from a CA system. These content rules are sent to the acquisition point in parallel with a content stream that is routed to an SVP-compliant chip. The acquisition point outputs an SVP-compliant Content License and forwards the Content License to the chip that is receiving the content. Based on the Content License and the Device Certificate,[8] SVP decides on the permitted use of the content.

Every acquisition point must have an Acquisition Point Certificate that affirms the acquisition point as being SVP-compliant.

As can be seen, SVP is designed to work with a wide range of CA/DRM systems.[9] When content arrives at an SVP-compliant STB under CA/DRM control, the acquisition device transfers control of the content to the SVP-compliant network by means of the acquisition process described.[10] *This transfer of control enables the content to be made available to the network in accordance with content usage rules set by the delivery CA system.*

The network operator can also use the acquisition device to perform tasks such as setting up its authorized domains[11], issuing and renewing certificates,[12] passing certificate revocation lists[13], and so

---

[8] Concerning Device Certificates, see Section 2.3.

[9] See also Section 5.

[10] As explained earlier, in acquisition, the acquisition point maps external Content Licenses to SVP-compliant Content Licenses.

[11] Concerning domains, see Section 2.6.

[12] Concerning certificates, see Section 2.3.

[13] Concerning certificate revocation lists, see Section 4.9.

forth. In such scenarios, the acquisition device acts as the CA headend's proxy on the home network.

The above is similarly applicable to any DRM system and any content delivery mechanism such as broadcast or unicast.

Two Content Scrambling Algorithms

SVP works with two scrambling/descrambling algorithms: the native scrambling algorithm (NSA) and the *external scrambling algorithm* (ESA). For interoperability, NSA is SVP's AES-based[14] scrambling algorithm. This algorithm is common across all devices that contain SVP-compliant chips. ESA is the scrambling algorithm used by the external content delivery—CA or DRM—system (e.g., DVB CSA, DES, 3-DES).

Content License—CSLs and BL-ECMs

An SVP-compliant Content License contains usage rights, and security information, such as content keys, needed for descrambling.

The content is time-divided into equal-duration content *crypto-periods*. The content is also segmented into several variable-duration *content segments*. A content segment consists of several contiguous crypto-periods. Typically, a film or other event will have at least one content segment and many crypto-periods. (See Figure 13).

A Content License has two subcomponents. Both subcomponents are derived from ECMs.[15]

- ***Base line ECMs*** **(BL-ECMs)**
  Contain information relating to a crypto-period such as the crypto-period's content keys.
- ***Content segment licenses*** **(CSLs)**
  Contain the segment's content usage-rights and enforcement requirements, such as copy and temporal control, parental rating, and scrambling policy. In an SVP-compliant home network, an SVP-compliant *acquisition device* produces the initial Content License on the basis of rights received in ECMs sent with the content.

Note: Content protected by the Broadcast Flag uses a somewhat different licensing mechanism, in which the CSL is stored in the device handling the content.[16]

---

[14] Patent pending.

[15] ECMs are explained at the beginning of Section 2.2

Secure Handling of the Content License

The Content License is sent from one device to another protected by the inter-device secure authenticated channel (SAC).[17]

Keys in BL-ECMs

A BL-ECM has room for two control words (i.e., descrambling keys): the ESA control word required to descramble the external—original—scrambling and the NSA control word necessary to descramble the local native scrambling. It may, however, contain only the NSA control word if the content was delivered without external scrambling to the SVP-compliant network. See Figure 14.

2.3 Device Certificates

Every SVP-compliant device must have a Device Certificate. A Device Certificate is a data structure that gives the identity and attributes of an SVP device. Each certificate is linked to a unique secret that resides in a single chip. Each SVP-compliant device must contain an SVP-compliant chip.

The device's attributes include rules that govern how the device can handle content. For example, the certificate associated with a television will specify that the device is a television and that, as such, it is restricted to receiving and rendering content—no SVP protected output is allowed. On the other hand, a PVR certificate may specify that storing, copying/moving, rendering, and distributing protected content be permitted.[18] The SVP specification also supports revocation of Device Certificates.

The following list shows some of the information contained in the certificate (for more information on certificates, see Section 4 and Section 8):

- Identifier
- Type of device, e.g., render only
- Descrambling algorithms supported
- Video formats supported
- Public key

---

[16] Full explanation of how SVP supports the Broadcast flag is beyond the scope of this document.

[17] Concerning the secure authenticated channel, see Section 2.5.

[18] See the functionality permitted to different devices as described in Figure 9.

The device holds a private key paired with the certificate's public key. This private key is securely stored under the protection of the SVP chip's unique secret.

2.3.1 How Content Licenses and Certificates Work Together

As explained, a Content License determines how a *particular* piece of content may be handled (rendered, copied, moved, stored, etc.). A Device Certificate, on the other hand, determines how a *specific device* can handle content in general.[19] If a Content License and Device Certificate have different values, the stricter value applies.

For example, imagine a TV with storage capability. Imagine also that the device's certificate identifies the device as a TV but not as a storage device. TV's are permitted to receive content and render it, but they are not permitted to store content. In this case even if the Content License permits storage, the device will not be able to make use of its storage capability, because its certificate does not permit storage.

2.4 Basic Content Handling Options

The SVP specification requires that descrambling and decompression all be performed within one SVP-compliant chip. This requirement ensures that clear compressed digital content is never accessible outside the silicon and that all content remains scrambled until rendering. As explained in the previous section, content usage rules (the Content License) and device rules (the Device Certificate) determine how particular content may be used.

The SVP specification sets forth a number of basic options for content handling. From these, it is possible to build a very wide range of business models. The basic options for content handling are the following:

- **Acquire**
  Convert associated external (i.e., non-SVP) content rights and control to SVP rights and control; create the initial SVP Content License for the content.
- **Render**
  Transform protected content into human-consumable form.
- **Copy/Move**
  Within or outside a consumer's domain. In *move*, the original copy is destroyed or rendered inaccessible. The stored content is generally under the control of a single SVP; it is also locally

[19] For the basic content handling options, see Section 2.4.

scrambled (as defense against the McCormac hack). Local scrambling is performed with SVP's own AES-mode native scrambling algorithm (NSA). Stored broadcast-scrambled content may be super-scrambled.

- **Temporary Store**
  Temporarily stored content is usable for a limited time, for example, 90 minutes. Temporary store provides a sliding window for buffered viewing—live pause and instant replay—of *copy never* content.
- **Distribute (transfer)**
  Output SVP-protected content and its license.
- **Export**
  The term export refers to content to which SVP protection no longer applies. Content can be exported to analog, clear digital, or to another approved content protection system.

The Content License determines whether content is passed between devices with only its original (ESA) scrambling, with only local (NSA) scrambling, or super-scrambled (NSA on top of ESA).

2.5 Secure Authenticated Channel

A secure authenticated channel (SAC) must be created between the sending device and the receiving device before content may be transferred. The SAC is not for the content itself, but rather for secure transmission of control messages (including Content License, Content Revocation List (CRL), and time) related to the content.

As mentioned in Section 2.3, each SVP-compliant chip holds a Device Certificate—a data structure that uniquely identifies that particular chip and the properties of the device in which it resides. Acquisition points, be they hardware components or tamper resistant software (TRS), require Acquisition Point Certificates.

Before two CE devices (or an Acquisition Device and a CE device) can send content to each other, they must establish a SAC. The first step in the process of establishing a SAC is the exchange of certificates.[20] Because each certificate contains a public key, each device receives the other's public key by means of the exchange and uses that public key to authenticate the certificate that contains it. Once the signed public keys have been exchanged and the two devices have been authenticated, the devices negotiate a symmetric session key used to encrypt and sign further communication (session keys can be changed

[20] For information on certificates, see also Section 4; for a detailed account on how a SAC is established, see Section 7.

at regular intervals). The channel established is then used to convey control messages.

Two SVP-compliant devices can also establish a SAC executed by the TRS SVP Manager software. This SAC is used for transmission of data related to domains,[21] proximity controls,[22] and extensions[23] to SVP core security functions.

Figure 15 shows the secure interaction of two SVP-compliant devices. Content is sent protected (i.e., scrambled) between devices. The Content License is sent over the hardware SAC that originates inside the SVP-compliant chip.

2.6 Domains

Domain is a construct designed to enable fair-use of content while limiting the sharing of content among devices.

For example, imagine that a content owner sells permanent access rights for a film to a home network owner and typical subscriber named Jim Trenton. The operator is happy to have Jim and his immediate family view and copy the film on any device in Jim's home. The operator is also willing to let Jim and family view the film on any portable device they own and take the film wherever they go.

On the other hand, the content owner is not willing to let the Trentons share the film with persons outside the immediate family: The operator would not want Jim's friends, Chuck and Phoebe Wilson, to bring a portable device to Jim's home, connect the device to Jim's home network, and copy the movie in usable form to their device. Nor would the content owner want Jim's son to send the film to his pals via the Internet.

A domain is a consumer household that contains a potentially-limited number of media devices owned, rented, or operated by a user or household, devices among which content can be exchanged and used according to specified usage-rights. Each domain is assumed to have a unique DomainID and a secret DomainKey.

SVP enables definition of two types of domains:

- **Externally managed (vertical)**
  The domain's characteristics are managed by a *gateway* connected to an external network. An example of a home network gateway

[21] Concerning domains, see Section 2.6.

[22] Concerning proximity controls, see Section 2.7.

[23] Concerning proprietary extensions, see Section 3.4.

on an externally managed domain would be a set-top box with a network operator's DRM or CA system. In pay-TV, for example, the operator's domain may be managed by the CA smart card and its secure non-volatile memory (NVM). Operators impose domain restrictions on specified content by means of Content Licenses. The operator's domain relates only to the operator's own content.

- **Autonomous (horizontal)**
  The domain is managed by one of the horizontal devices[24] in the domain that has secure storage. To enable future changes and regulatory rules to be implemented, the SVP standard allows autonomous domains to be implemented in TRS software

SVP domain control enables content owners and operators to enforce various distribution models and be confident that indiscriminate proliferation will be prevented.

2.7 Proximity

Proximity is a construct designed to limit distribution and consumption of content over long distances. Use of proximity controls can curtail indiscriminant, unauthorized redistribution of content over the Internet. Domain is not a geographical concept. A subscriber with a vacation home might own devices that are members of the same domain yet separated from each other by many hundreds of miles. On the other hand, in various instances, the content is to be consumed within a specified location. For such situations, the SVP specification provides *proximity control*.

Proximity control is imposed by means of effective measurement of distance—e.g., by means of round trip time (RTT) time between the content sourcing device and a target device.

At present, SVP allows proximity control to be implemented within the SVP TRS SVP manager. In the future, it will be incorporated into the core security functions performed by the SVP chip hardware SAC.

2.8 Handling Content

The following sections give generic scenarios for handling live and recorded content. As explained in this chapter, all content handling scenarios presume the following:

- A SAC has been established between any two devices passing control data

[24] A horizontal device is a CE device that has no linkage to a particular content distributor/network operator.

- Control data is passed only over a SAC.
- Content remains scrambled or super-scrambled until rendering

2.8.1 How an SVP System Handles Live Content

2.8.1.1 Acquisition and Media Device

In an acquisition and media device, when the SVP-compliant chip descrambles a live broadcast, it will receive control words (keys) directly from the acquisition point. On receiving the broadcast's first ECM, the acquisition point produces a CSL and verifies that the user is permitted to view the broadcast. If viewing is permitted, the acquisition point begins producing control words and sending them to the SVP-compliant chip, which demultiplexes, descrambles, and renders the content.

Like any two SVP-compliant devices, the acquisition point and the SVP-compliant chip must establish a SAC. Thus, the acquisition point and SVP-compliant chip authenticate each other, and control words are encrypted uniquely for the SVP to which they are sent. No other video processor will be able to use these control words to descramble the content. Control words are sent in BL-ECMs as part of the content license (CL).

In this case, the BL-ECMs contain only the ESA control word—the "external" control word used by the network operator to scramble the content.

2.8.1.2 Media Device

If live content is sent over a home network to a thin client (that is assumed not to have an acquisition point), the sending device (e.g., home network server) establishes a SAC with the receiving device and forwards the content license—CSLs and BL-ECMs—to the receiving SVP-compliant video processor. Content sent over the home network can be sent in its original scrambling or can be super-scrambled.[25] If the content is super-scrambled, the BL-ECMs also contain the NSA control words required to remove the super-scrambling.

In a typical home network, the home network server can transfer SVP-protected content to other devices on the home network or to its internal storage. Typically, the home network server is an Acquisition and Media Device containing an acquisition point, and this acquisition

[25] Depending on provisions of the CSL.

point in the server produces a CSL and BL-ECMs. The BL-ECMs contain ESA control words only.

The server's SVP-compliant chip performs the following tasks:

- Forwards the CSL to the client via the SAC
- Rescrambles or Super scrambles the content and forwards it to the client via the home network
- Places the control words in the BL-ECMs, modifies the content rights in the CSL, and forwards the CL to the client via the SAC

The Media Device acts as a client, and its SVP-compliant chip performs the following tasks:

- By means of the CSL, verifies that the content may be viewed on the client's associated device (e.g., analog TV)
- Descrambles the content
- Decompresses and decodes the content and sends it to the analog TV

2.8.2 How an SVP System Handles Stored Content

In an SVP-compliant system, content will typically be super-scrambled before being stored.

2.8.2.1 Content with Permanent Full Access Rights at Storage Time

For regular content that a subscriber is entitled to store and use at will within the home network, the content will be recorded together with its content license. At playout, the CL will be forwarded over a SAC to whatever device displays or stores the content.

2.8.2.2 Content without Access Rights at Storage Time

If the subscriber is not entitled to the content at storage time, (for example, the content was pushed to the subscriber, and must be purchased before viewing), BL-ECMs stored with the content contains only the native (local) control words. At playback, once the subscriber has gained entitlement to view the content, an acquisition point adds the ESA control words to the BL-ECMs before they are sent on the destination device for processing

Note: The playback scenario is possible only for devices connected to the Acquisition Point themselves or able via proxy to acquire the ESA control word. Portable devices can gain additional entitlement only when they are attached to the network where an acquisition point is available.

3 The SVP-Compliant Chip

3.1 Main Chip Components

The SVP specification requires that demultiplexing, descrambling, and decompression all be performed within one SVP-compliant video processor. Figure 16 shows a logical diagram of an SVP-compliant video processor found in a CE device that might receive and render content and then transfer the SVP-protected content to another SVP-compliant device. The two main components are the core security functions component (in gray), and the content processing component (in blue). The chip's interface with applications in the CE device is maintained by the SVP manager, a software component. The SVP manager is also the locus of any extended SVP functionality. The SVP Manager can be provided by the licensed device manufacturer or the licensed CA/DRM vendor.

3.2 Devices That Require SVP Protection

In an end-to-end SVP system, any consumer device with any of the following characteristics must have an embedded SVP-compliant chip:

- Has access to clear compressed digital content or to content keys.
- Controls content usage rights
- Controls keys for secure authenticated channel

3.3 Functionality

SVP functionality falls into two categories:

- **Standard:** defines the standard functionality of all SVP-compliant chips with built-in room for future extensions
- **Extended:** the SVP specification allows private extensions

3.3.1 Standard Functionality Requirements

An SVP-compliant device receives content and the content's associated SVP-compliant Content License (CSL and BL-ECMs). The SVP-compliant chip verifies that the Content License allows rendering on the device and then demultiplexes, descrambles, and decompresses the content; displaying it on the device. The SVP can also send the

scrambled, compressed content for storage on the host device and pass the content on to another SVP-compliant device.[26]

The following subsections give high-level requirements for SVP-compliant chips and acquisition points.

3.3.1.1 SVP-Compliant Chip

The following is a list of high-level requirements for SVP-compliant chips.

Processing in Hardware by One Chip

1. All processing of content from the scrambled compressed format to the descrambled decompressed format and all license processing shall be performed in secure hardware within a single chip.

Content Handling

2. An SVP-compliant chip may receive compressed video/audio/interactive data in one of the following possible scrambling states:
   a. In the clear
   b. Scrambled by a CA/DRM-originated algorithm (DVB-CSA, DES, etc.)
   c. Scrambled by the SVP AES-based native scrambling algorithm (NSA) stream cipher
   d. Super-scrambled—both 'b.' and 'c.' above, in order
3. An SVP-compliant chip shall be able to scramble any content with its NSA (128-bit control words).
4. An SVP-compliant chip shall be able to descramble content scrambled with the NSA (in accordance with provisions contained in the content's license and conditions specified in the device's certificate).

Content Licenses

5. An SVP-compliant chip shall receive, potentially modify, and transmit SVP-compliant Content Licenses.
6. A Content License shall consist of a Content Segment License (CSL)—pertaining to a particular content segment—and any number of Base Line ECMs (BL-ECMs) holding the actual control words required for descrambling.

---

[26] Both these functions can be performed only in accordance with the Content License and Device Certificate.

Certificates, Public Identity, Unique Secret

7. An SVP-compliant chip shall be associated with a public certificate that uniquely identifies that SVP-compliant chip and the properties of the device in which it resides (e.g., TV, PVR, acquisition device-smart card).
8. An SVP-compliant chip shall be serialized by securely embedding in it secret data required for secure storage and a unique public ID. The secret data shall be sufficiently large to withstand brute force attacks, and it shall never be exposed outside the SVP.
9. An SVP-compliant chip shall support RSA public keys. An SVP's private key may be securely stored outside the SVP.
10. An SVP-compliant chip shall support one or more Network-Operator Certificates.[27]

Secure Authenticated Channel

11. Before exchanging content, two SVP-devices shall mutually authenticate each other—using their respective certificates—and establish a secure, authenticated channel as follows:
    a. Establish that the other SVP-compliant device has a valid certificate
    b. Establish that the other SVP-compliant device is the owner of the certificate presented
    c. Negotiate with the other SVP-compliant device a session key for secure exchange of control data such as Content Licenses, time reference, domain information, and so forth.
12. When sending content to another SVP-compliant device, the SVP-compliant chip sending the content shall send control data over the SAC (i.e., CSLs and BL-ECMs, etc. shall be uniquely encrypted for the receiving device).

Time Keeping

13. An SVP-compliant chip shall keep relative time from power on until power off.
14. An SVP-compliant chip shall securely receive—via SAC—an absolute time reference and compute time by adding the relative time to the last-received absolute time.
15. An SVP-compliant chip shall maintain its time information securely and shall update it securely during SAC setup.

---

[27] A Network-Operator Certificate consists of attributes and permissions relevant to content provided by a specific network operator (see Section 4.3).

Export to Other Content Protection System

16. When giving control to another content protection system, SVP shall transfer analog or compressed digital content, as permitted by the certificate and content license.

Support for Domains

17. An SVP-compliant chip shall be linked to a specific authorized domain; the maximum number of devices within the domain can be limited by certificate.

3.3.1.2 Acquisition Point

The following is a list of high level requirements for SVP-compliant acquisition points.

1. An SVP-compliant acquisition point shall receive non-SVP content control criteria and map them to SVP-compliant data structures (CSLs and BL-ECMs).
2. An SVP-compliant acquisition point shall send CSLs and BL-ECMs only over a SAC.
3. An SVP-compliant acquisition point shall also meet the following functionality requirements listed above for SVP-compliant chips: 7., 8., 9., 11., 13., 14., 15., and 17.

3.4 Extended SVP Functionality

The SVP specification allows for private (proprietary) extensions that add functionality or security to the basic SVP specification. Extended SVP devices are interoperable with standard SVP devices, except when specifically forbidden by the extended SVP device's certificate or by a particular content's CSL.

SVP Licensees may create their own extensions. For example, the SVP specification does not require a chip to have non-volatile memory, but non-volatile memory may be included as a proprietary implementation.

4 Certificates

Every SVP-compliant media device and acquisition device contains at least one certificate. The concept of certificates was introduced in Section 2.3 as part of the general overview of the SVP system. The present chapter provides additional information on certificates.

The SVP specification recognizes the following kinds of certificates:

- Acquisition Point Certificates
- Device Certificates
- Network-Operator Certificates

The SVPLA Root Certificate Authority (see Section 4.5) will be responsible for certificate allocation.

4.1 Acquisition Point Certificates

An Acquisition Point Certificate grants an acquisition device the right to map external Content Licenses to SVP-compliant Content Licenses and the ability to establish a secure authenticated channel with an SVP-compliant chip. The certificate prohibits a pure acquisition device from processing content.

4.2 Device Certificates

A Device Certificate contains the identity and attributes of an SVP-compliant device. The certificate includes a public key.[28] The device holds a private key paired with the public key. This private key is held in a secure, secret storage area.

4.2.1 Types of Devices

Devices are divided into three broad categories.

- Acquisition devices
- Media Devices
- Acquisition and Media Devices

[28] Section 2.3 gives a partial list of information held in Device Certificates. Section 8 shows the complete format of Device Certificates.

These device types are characterized as follows:

Acquisition Device

An acquisition device is an SVP-compliant device that contains an acquisition point in accordance with the SVP device specification.[29] A pure acquisition device does not implement any content processing function. It does, however, implement the core security functions present in an SVP-compliant IC. For example, an acquisition device must be able to establish a secure authenticated channel with a media device.

A smart card is an example of a removable acquisition device. An embedded chip in a media device and a virtual smart card in a media device are examples of bound acquisition devices.

All acquisition devices require an Acquisition Point Certificate, and the acquisition point within the acquisition devices must be certified as being SVP-compliant. The device itself need only undergo self-certification.

Media Device

A media device is an SVP-compliant device that can receive content and enable content consumption, storage, redistribution, and export, or a combination of these functions in accordance with the SVP device specification. STBs, thin-client STBs, and a Portable PVRs are examples of Media Devices. Media Devices are self-certified.

Acquisition-and-Media Device

An *acquisition and media device* is an SVP-compliant device with the combined functionality of a bound acquisition device and a media device. Examples of such devices are Broadcast Flag-compliant free-to-air set-top boxes (STBs), DTT-ready digital televisions, TV sets, or STBs with DRM or CA embedded in software or hardware. The acquisition and media device requires an Acquisition Point Certificate and the acquisition point within the device must be certified as being SVP-compliant. The device itself need only undergo self-certification.

4.2.2 The Device Certificate

The Device Certificate grants a media device or an acquisition-and-media device the right to perform any or all of the following:

[29] For information on acquisition and acquisition points, see Section2.2.

- [R] Receive SVP-protected content and Render content to human-consumable form.
- [S] Store SVP-protected content "internally" under exclusive control of the receiving device.
- [X] Export, relinquish SVP protection of content, as in content exported as analog or clear digital, or content handed off to another trusted content protection system.
- [T] Transfer, end-to-end transfer of SVP-protected compressed digital content to SVP-compliant devices.

The Device Certificate is usually issued at time of manufacture. Under exceptional circumstances, it may be securely downloaded to an SVP-compliant device in the field.

4.3 Network-Operator Certificates

A Network-Operator Certificate is an additional certificate issued and signed solely by a network operator or a CA/DRM provider on behalf of the network operator. A Network-Operator Certificate consists of attributes and permissions relevant only to the network operator's content.

Under its SVP license, the issuing network operator—or its agent, the CA/DRM provider—can control the Network-Operator Certificate. The Network-Operator Certificate can limit the number of devices attached to a home network and regulate home networks in other ways. If necessary, a network operator enables a Network-Operator Certificate, thereby placing the network's content on *specific* subscriber devices under the network operator's control. In this way, the Network-Operator Certificate extends the network's existing conditional access or digital rights management rules to specific types of devices.

4.4 Certificate Hierarchy

Each certificate actually belongs to an ordered sequence of certificates, called a *certificate chain*. In the certificate chain, each element of the sequence is digitally signed (using RSA) by its parent certificate (i.e., the preceding certificate in the chain). The first element of the sequence has as its parent (and is signed by) one of four defined system-wide SVP *roots*. Certificates can be issued to devices during production or downloaded to devices already in the field.[30]

[30] See Section 4.2.2.

Figure 17 represents the certificate tree. The certificate tree is hierarchical, beginning with the SVPLA Root Certificate Authority. Each child inherits properties from its parent.

4.5 Root Certificate Authority

A certificate is required for each device that contains an SVP-compliant chip or acquisition point.[31] The Root Certificate Authority division of the SVPLA determines legal and commercial rules and procedures for obtaining SVP certificates. The Root Certificate Authority also securely issues certificates to SVP licensees and manages all SVP certification and revocation procedures.

The Root Certificate Authority will also be responsible for providing consumer device manufacturers and network service operators the option to manage their own certificate authorities or obtain certificates directly from the SVPLA Certificate Authority. Each recognized certificate authority established by a device manufacturer or network operator becomes part of the chain of trust.

When network operators issue their own Network-Operator Certificates, the operator's conditional access or DRM system is extended and used by the operator to perform actions such as setting up explicitly authorized domains, renewing network-specific certificates, and passing on SVP certificate revocation lists.

4.6 The Licensing and Certification Chain

4.6.1 Device Certificate

The first stage in producing an SVP-compliant device is producing SVP-compliant chips. Chipset manufacturers require an SVP License to receive the complete SVP specification. The license agreement includes provisions for compliance and robustness as well as for testing procedures.

In the next stage, the CE manufacturer—also a licensee—applies for and purchases a certificate for each device. For example, a digital STB manufacturer producing one million SVP-compliant STBs must purchase one million Device Certificates.

[31] Whether the acquisition point is implemented in hardware or software.

4.6.2 Inheritance and Certificate Trees

Each device in the hierarchical certificate tree shown in Figure 17 inherits properties from its parent. For example, if the restrictions of the PVR offshoot of the "CE Manufacturer 1" branch of the tree state that the PVR may store scrambled content only, all PVR devices below it will have the same restriction. Similarly, if the TV offshoot of the "CE Manufacturer 1" branch is restricted to rendering content, all televisions below it will share the same restrictions. Each SVP-compliant chip has one or more certificate chains that belong to it.

4.7 Chain of Trust

As explained, when two SVP-compliant devices communicate, they establish a secure authenticated channel.[32] As a precursor to a secure authenticated channel setup, two SVP devices exchange certificates, and each device verifies the other device's certificate.

Verification is obtained through a procedure in which the signature of each certificate is checked against a public key of its *ancestor* until a common ancestor is reached. This hierarchical arrangement of certificates is known as a *chain of trust*. Such a procedure requires a few seconds maximum, but it does not need to be carried out repeatedly, since each device keeps a copy of the other's certificate in memory.

For example, suppose two vertical devices certified by the network service operator shown on the left side of Figure 17 exchange certificates, the verification procedure will continue until the network service operator, the *common ancestor* is reached.

In contrast, suppose two horizontal devices, manufactured by CE Manufacturer 1 and CE Manufacturer 2 respectively exchange certificates. The certificate procedure will continue until the Root Certificate Authority is reached.

4.8 Secure Authenticated Channel

SVP specifies that all control data (CSLs and BL-ECMs, etc.) be passed only over secure authenticated channels (SACs). The concept of SACs was introduced in Section 2.5 as part of a general overview of the SVP system. This chapter explains how SACs are established.

[32] For details of secure authenticated channel setup, see Section 7.

4.8.1 Certificate Exchange

As explained in Section 4.7, certificate exchange is a prerequisite for establishment of a SAC.[33] The SVP-compliant device's application level is responsible for initiating the communication and delivering the SVP's own and its ancestors' certificates to another SVP-compliant device. Each SVP-compliant chip must receive the other SVP-compliant chip's complete chain of ancestors up to the root.

At the conclusion of certificate exchange, each device has validated the other side's certificate and can therefore trust the other side's device properties and use the other side's RSA public key.

4.8.2 Certificate Validation Sequence

For each certificate, there is only one device that can successfully pass the authentication process, because each certificate is linked to a unique secret that resides in a single chip.

The SVP software in the SVP-compliant device identifies the certificate chain from the root to a device. The SVP-compliant chip validates the chain of trust by checking a certificate's signature using the public key of the higher level. "Inheritance rules" are applied at the same time to the certificate's device properties fields.

4.9 Certificate Revocation

Within the bounds of strict guidelines, the SVPLA may revoke a certificate associated with a specific device.

Figure 18 shows the certificate revocation process. In this process, the SVPLA distributes a certificate revocation list (CRL) to operators. The operators subsequently distribute the CRL to all their devices, thus revoking the devices on the list. When a device with an acquisition point receives the CRL, it checks whether any of the devices in its domain are on the list. If the CSL associated with any content item indicates that a revoked device may not render the content, the content will not be passed to any revoked device in the acquisition point's domain. Certificate revocation will be subject to the input of all interested parties.[34]

[33] For detailed information on how a SAC is established, see Section 7

[34] The steps required for revocation are beyond the scope of the present document.

5 Network Operator Scenarios

5.1 Interaction between SVP and CA/DRM Systems

A pay-TV content stream is typically protected by a DRM or conditional access system. Since pay-TV consumers may want to transfer such content to their non-proprietary open SVP-compliant systems, the conditional access system can provide a time-limited and otherwise-limited license for content consumption in the SVP-compliant system. The connective bridge between the proprietary and SVP systems on the same or different devices will enable content interoperability according to the following content control models:

- **Irreversible handoff**
- **Shared control**
  As in:
  - Rental
  - Tethered consumption
    Horizontal SVP device is connected to CA/DRM vertical device to enable playback
- **Control retained by proprietary system**
  Content binning , or delayed CA/DRM resolution

The following sections explain these models.

5.1.1 Irreversible Handoff

Figure 19 represents irreversible handoff from a proprietary system to an open SVP system.

In this model, the external system delivers content and its associated license to the SVP system. After content delivery, the SVP system has complete control of content usage states.

5.1.2 Shared Control

This section explains the following shared control models:

- **Rental**
  For example, CA/DRM can update rental window; SVP controls playback
- **Tethered consumption**
  Playback is controlled by SVP while connected to the CA/DRM

Rental

Figure 20 shows shared control between a proprietary and SVP system.

Rental is an instance of the shared control model. In rental, the SVP system has complete control of usage rights enforcement for a limited duration. Playback of content under the SVP system within the rental period requires no connection to the proprietary system, whereas extension of the rental period (if desired) is the responsibility of the CA/DRM system.

Tethered Consumption

Tethered consumption is another instance of the shared control model. In tethered consumption, the content resides on the SVP-compliant device, but a connection is required between the SVP-compliant and proprietary devices. During playback, the SVP-compliant device, a horizontal device, receives the Content License and control words from the proprietary device. This small amount of data requires a very low throughput link between the SVP and proprietary devices.

6 Glossary

Term	Explanation
Acquisition	Process of receiving external content usage rules and outputting SVP-compliant data structures that express those rules.
Acquisition point	A functional entity that creates the initial SVP Content License through the receipt of content rights from an external non-SVP source and the mapping of those rights to SVP rights and enforcement rules embodied in the SVP Content License.
Acquisition device	A licensed device that functions as an acquisition point in accordance with the SVP Device Specification. The acquisition device is not required to implement any content processing function; it does, however, implement the initial SVP content control created upon content arrival or introduction, by mapping the external content control to an SVP-compliant Content License. The acquisition device also implements core security functions present in the licensed IC, e.g., establishing a secure acquisition point with a media device. A smart card is an example of a removable acquisition device. An embedded chip in a media device and a virtual smart card in a Media Device are examples of bound acquisition devices.
Baseline entitlement control message (BL-ECM)	SVP-compliant data structure that contains encrypted control words necessary to decrypt content. Each BL-ECM is linked to a specific CSL. Note: In contrast to ECMs, which are proprietary by nature, BL-ECMs are basically standard—hence *baseline*.
BL-ECM	See *baseline entitlement control message*.
Broadcaster	General term used to refer to a TV operator, cable MSO, or satellite broadcaster.
CE device	Consumer electronics device.
Certificate or Device Certificate	A protected and signed data package that uniquely identifies a licensed device and states the device type and its restrictions. The certificate includes the device's RSA public keys required for secure authenticated channel setup following certificate exchange between two licensed devices.

Term	Explanation
Content License	SVP-compliant data structure that contains the SVP rules that prescribe authorized use of associated content (e.g., copy permissions, distribution rules, etc.) and contains data that control authorized access to the content. Each SVP-protected content item has its own cryptographically bound Content License.
Content Segment License (CSL)	A subcomponent of a Content License. A Content Segment License includes the usage rules associated with scrambled content. A single piece of content may contain several segments and a CSL for each different segment. A CSL is associated with a segment of content and any number of BL-ECMs.
Control words (CWs)	Digital keys used to scramble/descramble content.
CP	Content protection
Digital content	Digital representation of audiovisual works, including audio, video, text, and/or graphics, and associated metadata (e.g., subtitles, descriptions, interactive data).
Domain	A set of media devices owned, rented, or operated by a user or household.
ECM	See *entitlement control packet*.
Entitlement control packet	DVB standard term for a broadcast packet that contains access criteria.
External scrambling algorithm	Scrambling/descrambling algorithm used by external system (for example, CA) to protect content delivered to the SVP system.
Horizontal device	A CE device having no linkage to a particular content distributor. Such a device may interconnect to a home domain without any connection to an external pay-TV network.
McCormac hack	CW distribution hack, originally proposed by John McCormac. A "McCormac Server" extracts broadcast CWs, and distributes them to "McCormac Clients," who receive the scrambled broadcast and use the CWs received to descramble content.
Native scrambling algorithm (NSA)	Scrambling/descrambling algorithm for protection of content within the SVP system.
Network-Operator Certificate	An SVP-compliant signing certificate issued by, or on behalf of, the SVPLA to the network operator for signing network operator device certificates.

Term	Explanation
Rivest, Shamir, Adelman public key (RSA)	Cryptographic algorithm A de-facto standard used as the basis for asymmetric signing and encryption in the SVP system.
Root Certificate Authority	The administrative body appointed by the Licensor and responsible for administering Certificate Revocation Lists and Certificates, whose private key is used to sign the root certificate, and whose public modulus is securely available to all SVP chips in a manner that is secured against modification.
Scramble	Encryption of content.
Secure authenticated channel (SAC)	A virtual communications channel established between entities for reliable private transfer of data.
SVP Manager	Software responsible for the interface to the licensed IC and that may perform content protection functions that are not mandated by SVP compliance to be implemented in the licensed IC, such as those related to domain, geographic, and proximity Controls.
TRS	Tamper resistant software
Vertical device	A CE device specified or subsidized by a content distributor or network operator who has a cashier relationship with customers. The content distributor or network operator may specify interrelationships between devices.

7 Secure Channel Setup

A SAC is established via a challenge/response handshake protocol as represented in Figure 21. The outcome of this protocol is a 128-bit symmetric session key used to encrypt further communication between the two SVPs. This is the meaning of *secure channel*—all communication between two devices is encrypted and can be decrypted only by those two devices. The SVP specification requires a secure *authenticated* channel, meaning that before two devices can establish a secure channel, they must authenticate each other as valid SVP certificate holders. As part of this process, each device's certificate properties are made known to the other side, and other control data (not included in the certificate) is exchanged securely.

The symmetric key is valid for a limited period of time (a *session*), so it is referred to as a *session key*. If further communications are required after a session has ended, the SVP software must initiate a handshake again to obtain a new session key.

A handshake between two devices consists of two stages. At the first stage, each side generates a 128-bit random number, encrypts it with the other side's public key, and sends it to the other side. Each side decrypts the other side's random number using its own secret key and then hashes the two random numbers to generate the shared key[35].

The second stage uses that key to pass additional data (time, domain, revocation data, etc.) between the devices. The shared key becomes a valid session key only after successful execution of the second stage.

Each stage consists of commands at both sides (see Fig.21). At the conclusion of the first stage both devices have a shared key, but it can be used only to protect the second stage's information exchange. The shared key becomes a valid session key following a successful second stage.

Each device records the time in which the first protocol step occurs and allows a reasonable interval from that time to the last protocol step. This procedure protects the handshake from replay attacks. A

[35] The hash order is determined by data delivered in the Challenge data structure's clear envelope.

dedicated 24-bit timer within each SVP-compliant chip counts time from reset to enable this time comparison.

8 Certificate Structure and RSA Modulus

8.1 Certificate Structure

Figure 22 and Table 1 below describe the data structure of certificates. Field descriptions are given immediately below. The 112-byte sequence of all standard and proprietary fields is referred to in this document as *Body*.

Table 1: Certificate Fields

Field	2K	1K	Signed
Protection (CBC-MAC)	16	16	
Standard Body Fields	96	96	Y
Available for Proprietary Extension Body Fields	16	16	Y
Compressed Modulus	128	64	Y
Reserved	-	64	Y
Total	**256**	**256**	

Protection Field

Protection field is CBC-MAC for exported or symmetric certificates; hash for asymmetric original certificates.

The CBC-MAC field is the signature of the certificate.

Compressed Modulus

This field contains the RSA modulus or public key of the certified device. The modulus may be either a 1K or a 2K key. However, to save space in the certificate (and therefore in the SVP), the field contains a compressed version of the modulus. When the certificate is loaded, the modulus is expanded.

8.2 RSA Modulus

Each certificate has an associated (explicit) compressed RSA modulus of either 512 bits or 1024 bits, and an (implicit) expanded (full) RSA

modulus of twice the number of bits, the expanded RSA modulus being a function of the certificate's 64-bit *CertificateID* field and its compressed RSA modulus.

Outside of an SVP, a certificate and its associated compressed RSA modulus are always represented by a 2048-bit value, called the *recovered certificate*. When this 2048-bit value is raised to the power 65537 (i.e., $2^{16} + 1$) and the result reduced modulo the expanded RSA modulus of the parent certificate, the bit assignments in Table 2 apply to the 2048-bit result (bit 0 is the LSB):

Table 2: RSA Modulus Bits

Bit Position	Occupied by...
2047–1920	Validating 128-bit hash of bit positions 1919–0
1919–1152	768-bit certificate structure
1151–1024 and 511–0 (the latter only if the compressed RSA modulus is 512 bits)	Available for proprietary (non-standard) extensions
1023–0 if it is 1024 bits, or 1023–512 if it is 512 bits	The compressed RSA modulus occupies bit positions

9 Content License Structure

9.1 Content Segment License

The CSL structure may be any length (i.e., number of bits) that is a multiple of 32 and that is between 576 and 1856 bits, inclusive. The fields of the first 576 bits of the CSL structure are shown in the following table:

Table 3: CSL Fields

Field Name		Size (bits)	Comments
CSL ID		64	Encrypted
SF		8	Any value specified in the standard.
Sfextension		8	
Version		8	
Extended CCI	CCI	2	Copied directly from CSL to content handling component of SVP
	NextGeneration	1	
	Movable	1	
	NextGenerationMovable	1	
	Domain Limitations (MAD, CAD, RAD)	3	
Originator ID		96	
Content ID		48	
Domain ID		48	
ScramblingPolicy		8	
ESAselect		4	Index to bitmap SelfCertificate ESA descramblers; used to select among supported ESA functions
TransferType		2	

Field Name		Size (bits)	Comments
MacrovisionRequired		1	Copied directly from CSL to content handling component of SVP
BroadcastFlag		1	Copied directly from CSL to content handling component of SVP
ParentalRating		16	
RequiredIssuerMask		32	
RequiredIssuer		32	
Required regular security qualities	RequiredSelfTQ	4	
	RequiredDomainImplementationQuality	4	
	RequiredRealTimeClockQuality	4	
	RequiredUnassignedRegularQualities	5*4=20	
Required special security qualities	RequiredFingerprintQuality	4	
	RequiredUnassignedSpecialQualities	5*4=20	
StartTime		32	
FinishTime		32	
PermittedOutputTypes		24	Bitmap of CODECs whose use is permitted
RequiredSecurityFunctions		8	Bitmap of security functions that must be supported for rendering
CRLcheckRequiredInGracePeriod		1	
CRLcheckRequiredAfterGracePeriod		1	
DomainKeyProhibited		1	
Certificate1KProhibited		1	
PassThroughProhibited		1	
SFonlyForCopyMove		1	
SFonlyForRendering		1	
MatchingIssuerRequiredForRendering		1	
RequiredTQ		4	
NSAscrambled		1	

Field Name	Size (bits)	Comments
ESAscrambled	1	
ESAkeyValid	1	
TQunlimited	1	
ExpirationCheckRequiredForCopyMove	1	
ExpirationCheckRequiredForRendering	1	
Reserved	14	
Standard Part Total	576	
Reserved	Variable	

The remaining bits, if any, are available for potential future CSL extensions.

9.1.1 Constant Values

Table 4 defines the "fixed" constants used by the standard SVP system.

Table 4: SVP Standard Constant Values

Constant Name	Value	Comment
GeneralConstant (C)	TBD	First 16 bytes of TBD Universal constant
Public Exponent	$2^{16}+1$ (10001_{16})	
StandardSF	0	
CBC IV	TBD	
IV_HW_SIGNATURE	TBD	
IV_CRL	TBD	
IV_CERTIFICATE	TBD	
IV_SESSION_KEY	TBD	
ESA Codes	See Table 5	

Table 5: Content ESA Codes

Hex Code	ESA Name	ESA Reference	Comment
TBD	DVB		
TBD	DES		
FF	Reserved for Expansion		

9.1.2 Transfer Types

Content transfer type (Table 6) is requested and allowed/prohibited within the context of handling licenses.

Table 6: Transfer Types

CSL Transfer Type Encoding	Meaning	Description
00	For Rendering	Content is sent to the SVP for rendering only
01	Reserved	In NSK implementation, identical to "For Render" (look at MSB only)
10	For Copy	Content stored in an SVP's storage device is sent to another SVP, for storing the data on the latter's storage. After the transfer, both storage devices hold the content.
11	For Move	Same as "Copy" above, except that content is deleted from the source device's storage following receipt of content by the target device. Note that in NSK, deletion of moved content is a software task.

9.2 BL-ECM

The BL-ECM structure may be any length (i.e., number of bits) that is a multiple of 32 and that is between 256 and 1856 bits, inclusive. The fields of the first 320 bits of the BL-ECM structure are shown in Figure 23 and Table 7 below.

Table 7: Core BL-ECM Structure

Field	Length (bytes)	Encrypted	Signed	Notes
CBC-MAC	16			Signature field
EncryptedBlockEnd	1		Y	See Note 1
CryptoPeriod	1		Y	
TimeOffset	2		Y	
Reserved	4		Y	
NSA CW	16	See Note 2	Y	
ESA CW	8-16	Y	Y	

Field	Length (bytes)	Encrypted	Signed	Notes
Reserved Encrypted	Variable	Y	Y	by NSK—see Note 3
Reserved Clear	Variable		Y	by NSK—See Note 4
Total (excluding clear envelope)	**Min. 48 bytes**			**Must be divisible by 4**

Notes:

1. ***EncryptedBlockEnd***
   Gives the offset of the first non-encrypted byte, beginning at the end of the CBC-MAC. Must be divisible by 4.
2. **In *Output BL-ECM*:**
   Encrypted part always starts from offset 8, and XOR pad starts from offset 0.

   In *Input BL-ECM*:
   If (***CSL.SF = NDS_SF***) AND (***SelfCertificate.SF = NDS_SF***) AND (***CSL.NSAkeyOmitted*** = 1): NSA CW is clear—encrypted part starts from offset 24, and XOR pad starts from offset 16.
   Otherwise: NSA CW is encrypted, starting at offset 8, and XOR pad starts from offset 0.

   This is done to enable more efficient Smart card – SVP communications: by allowing the card to drop the (unused) NSA key and its re-insertion by the SVP Manager for input to NSK.
3. ***ReservedEncrypted***
   Covered by ***EncryptedBlockEnd***. NSK decrypts and then ignores this field.
4. ***ReservedClear***
   Included in signature check.

   The remaining bits, if any, are available for potential future BL-ECM extensions.

What is claimed is:

CLAIMS

1. A cable for transferring digital data from a host to a device, said cable comprising:

a host connector operable to connect said cable to said host;

a device connector operable to connect said cable to said device; and

a data processor disposed between said host connector and said device connector, said data processor comprising:

a receiver operable to receive (a) encrypted digital data from said host, wherein said encrypted digital data is encrypted according to a first encryption standard; and (b) first decryption information usable to decrypt said encrypted digital data;

a decryptor operable to decrypt said encrypted digital data using said decryption information to form decrypted digital data;

an encryptor operable to re-encrypt said decrypted digital data according to a second encryption standard to form re-encrypted digital data; and

a transferrer operable to transfer said re-encrypted digital data and second decryption information usable to decrypt said re-encrypted digital data to said device.

2. A cable according to claim 1, wherein said transferrer is operable to transfer said re-encrypted digital data directly to said device.

3. A cable according to claim 1, wherein said transferrer is operable to transfer said re-encrypted digital data to said device via said host.

4. A cable according to any of claims 1 to 3, wherein said data processor is operable to transcode and/or transrate said digital data.

5. A cable according to any preceding claim, wherein said data processor is operable to apply a watermark to said digital data.

6. A cable according to any of claims 1 to 5, wherein said first encryption standard comprises DVB-CSA.

7. A cable according to any of claims 1 to 6, wherein said second encryption standard comprises an AES-based encryption algorithm.

8. A cable according to any of claims 1 to 7, wherein said first decryption information comprises decryption keys usable to decrypt said digital data.

9. A cable according to any of claims 1 to 7, wherein said first decryption information comprises control messages usable to derive decryption keys usable to decrypt said digital data.

10. A cable according to claim 9, further comprising a smart card connector operable to connect said cable to a smart card, wherein said smart card uses said control messages to derive said encryption keys.

11. A cable according to claim 9, further comprising a smart card, wherein said smart card uses said control messages to derive said encryption keys.

12. A cable according to any of claims 1 to 11, wherein said second decryption information comprises decryption keys usable to decrypt said digital data.

13. A cable according to any of claims 1 to 11, wherein said second decryption information comprises second control messages usable to derive decryption keys for decrypting said digital data.

14. A cable according to any preceding claim, wherein said digital data comprises media content data.

15. A method of transferring digital data from a host to a device, wherein said host is connected to said device by a cable, said cable comprising a data processor, said method comprising:

transferring digital data from said host to said data processor;

receiving (a) encrypted digital data from said host, wherein said encrypted digital data is encrypted according to a first encryption standard; and (b) first decryption information for decrypting said encrypted digital data;

decrypting said encrypted digital data using said decryption information to form decrypted digital data;

re-encrypting said decrypted digital data according to a second encryption standard to form re-encrypted digital data and

transferring said processed digital data to said device.

16. A method according to claim 15, wherein transferring said processed digital data comprises transferring said re-encrypted digital data directly to said device.

17. A method according to claim 15, wherein transferring said processed digital data comprises transferring said re-encrypted digital data to said device via said host.

18. A method according to any of claims 15 to 17, wherein processing said digital data further comprises transcoding and/or transrating said digital data.

19. A method according to any of claims 15 to 18, wherein processing said digital data further comprises applying a watermark to said digital data.

20. A method according to any of claims 16 to 19, wherein said first encryption standard comprises DVB-CSA.

21. A method according to any of claims 16 to 20, wherein said second encryption standard comprises an AES-based encryption algorithm.

22. A method according to any of claims 16 to 21, wherein said first decryption information comprises decryption keys usable to decrypt said digital data.

23. A method according to any of claims 16 to 21, wherein said first decryption information comprises control messages usable to derive decryption keys usable to decrypt said digital data.

24. A method according to claim 23, wherein said cable further comprises a smart card connector operable to connect said cable to a smart card, and wherein said smart card is operable to use said control messages to derive said encryption keys.

25. A method according to claim 23, wherein said cable further comprises a smart card, wherein said smart card is operable to use said control messages to derive said encryption keys.

26. A method according to any of claims 15 to 25, wherein said second decryption information comprises decryption keys usable to decrypt said digital data.

27. A method according to any of claims 15 to 25, wherein said second decryption information comprises second control messages usable to derive decryption keys for decrypting said digital data.

28. A method according to any of claims 15 to 27, wherein said digital data comprises media content data.

29. A cable for transferring digital data from a host to a device, said cable comprising:

host connection means for connecting said cable to said host;

device connection means for connecting said cable to said device;

receiving means for receiving (a) encrypted digital data from said host, wherein said encrypted digital data is encrypted according to a first encryption standard; and (b) first decryption information for decrypting said encrypted digital data;

decryption means for decrypting said encrypted digital data using said decryption information to form decrypted digital data;

encryption means for re-encrypting said decrypted digital data according to a second encryption standard to form re-encrypted digital data; and

transferral means for transferring said re-encrypted digital data and second decryption information for decrypting said re-encrypted digital data to said device.

FIGURE 1

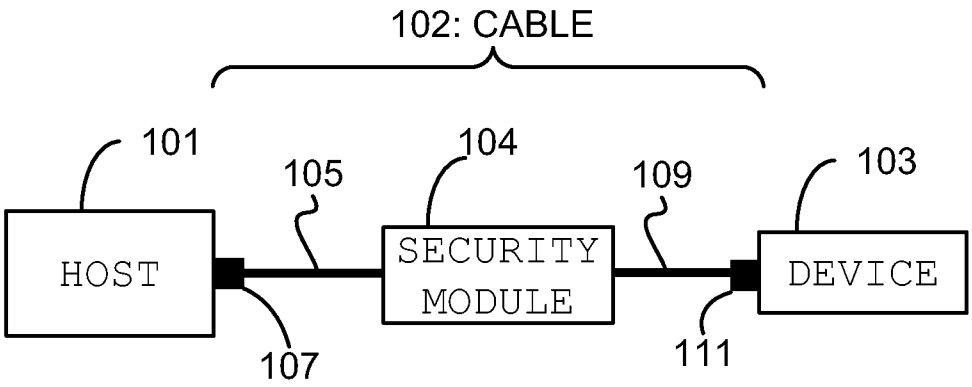


FIGURE 2

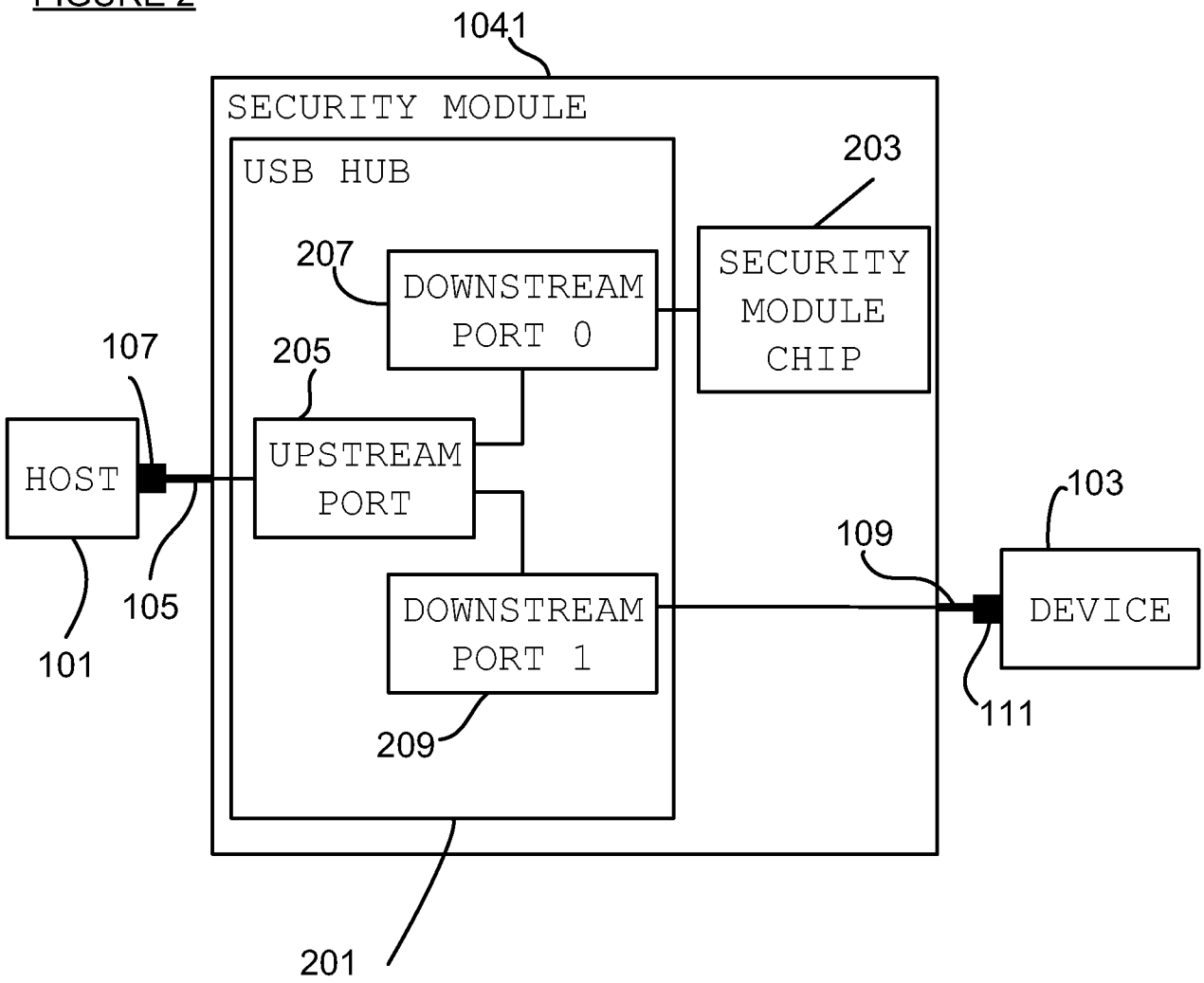


FIGURE 3

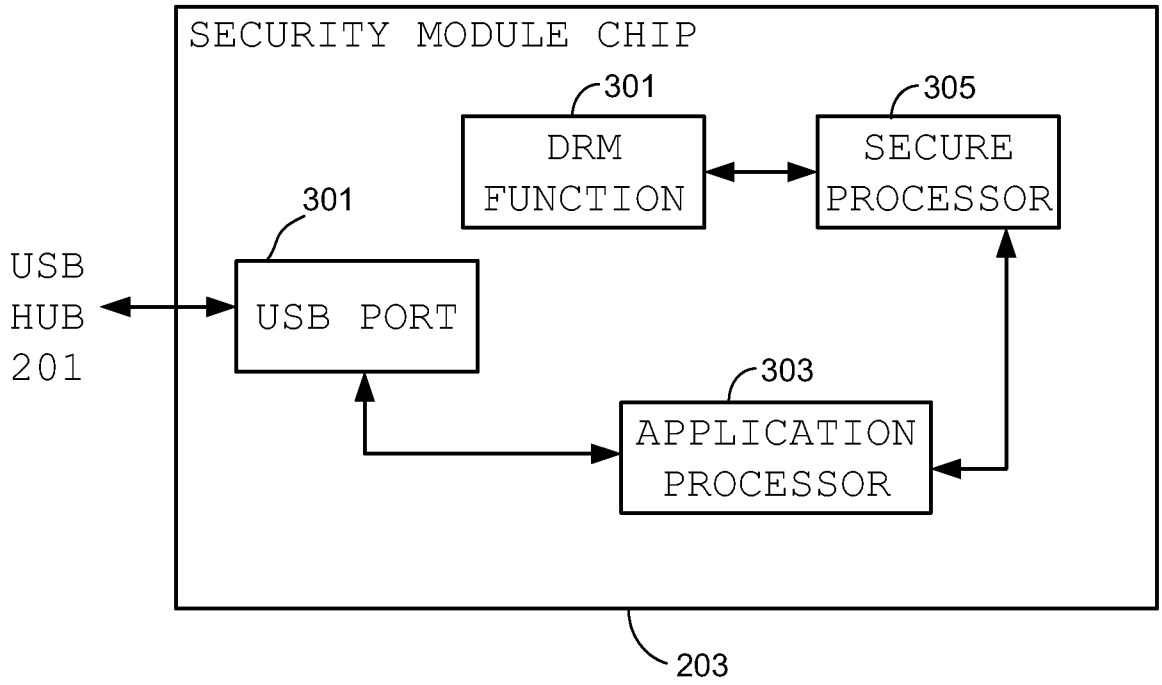

SECURITY MODULE CHIP
301
DRM FUNCTION
305
SECURE PROCESSOR
301
USB HUB 201
USB PORT
303
APPLICATION PROCESSOR
203

FIGURE 4

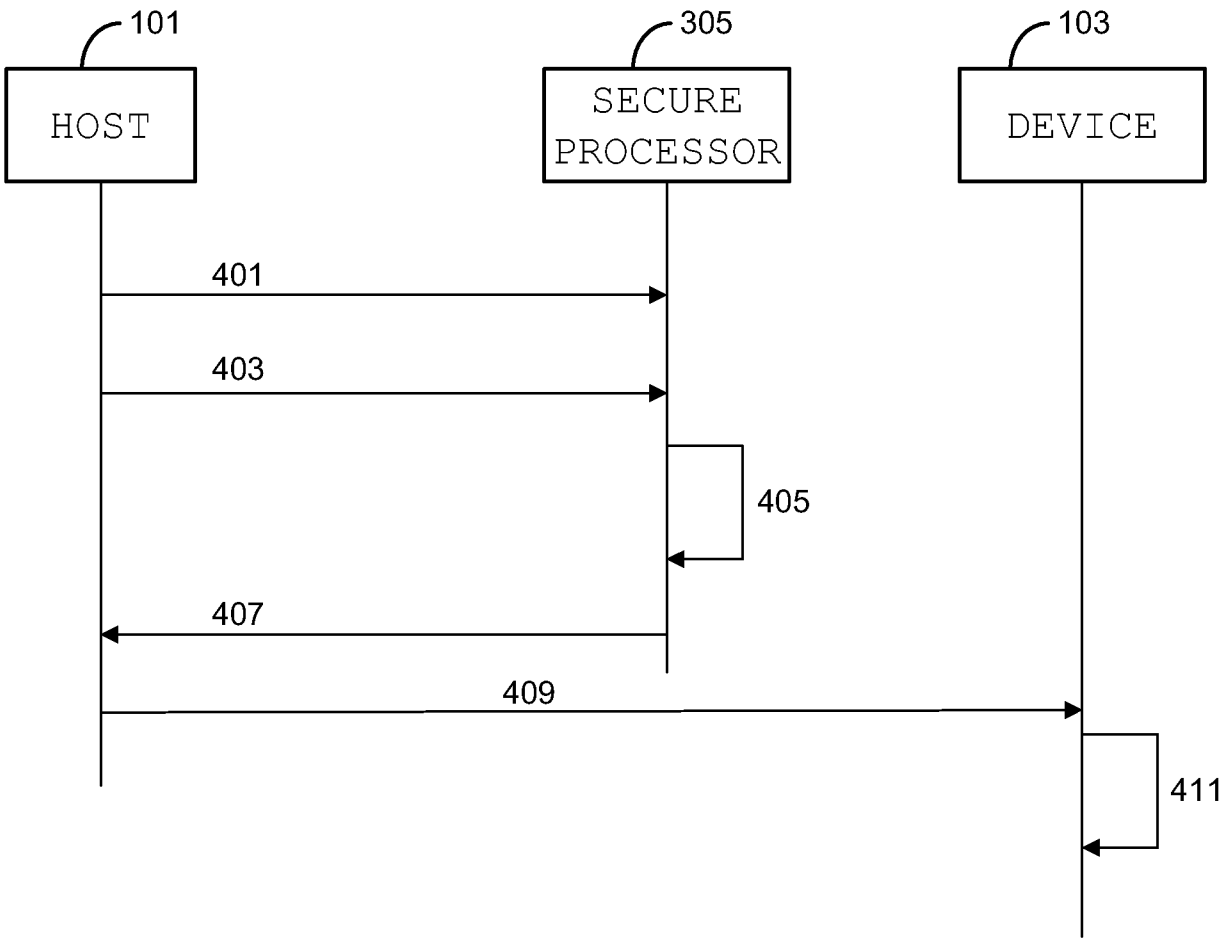


FIGURE 5

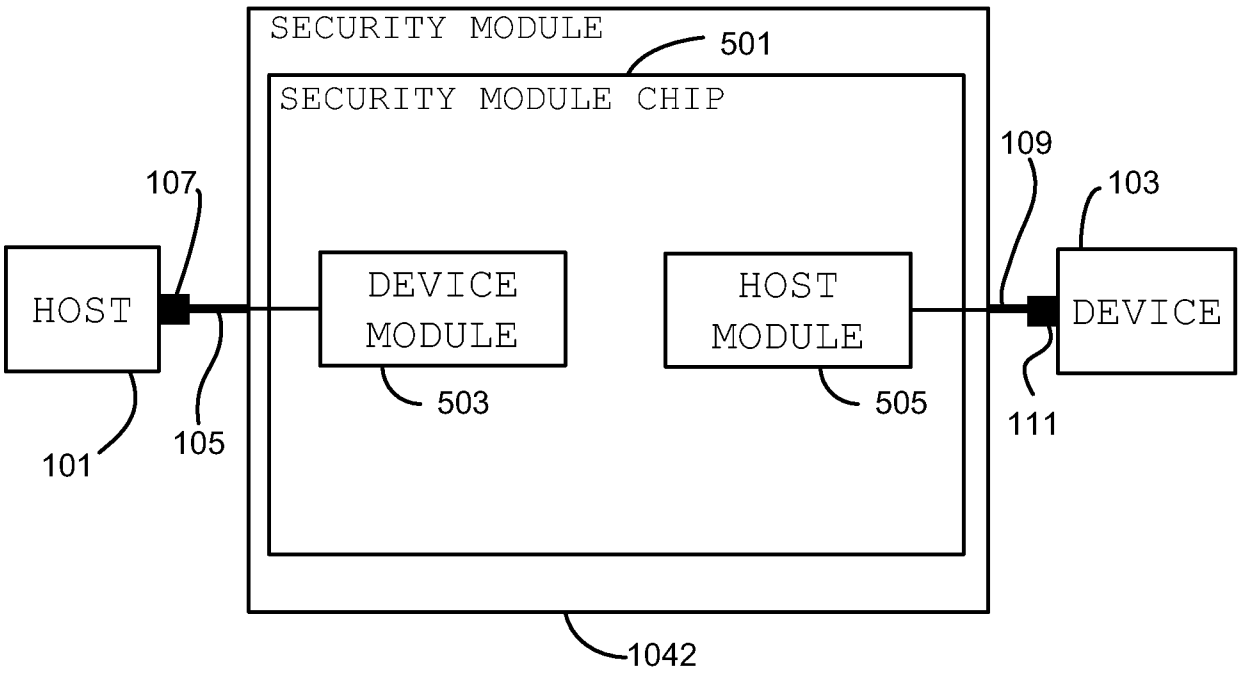


FIGURE 6

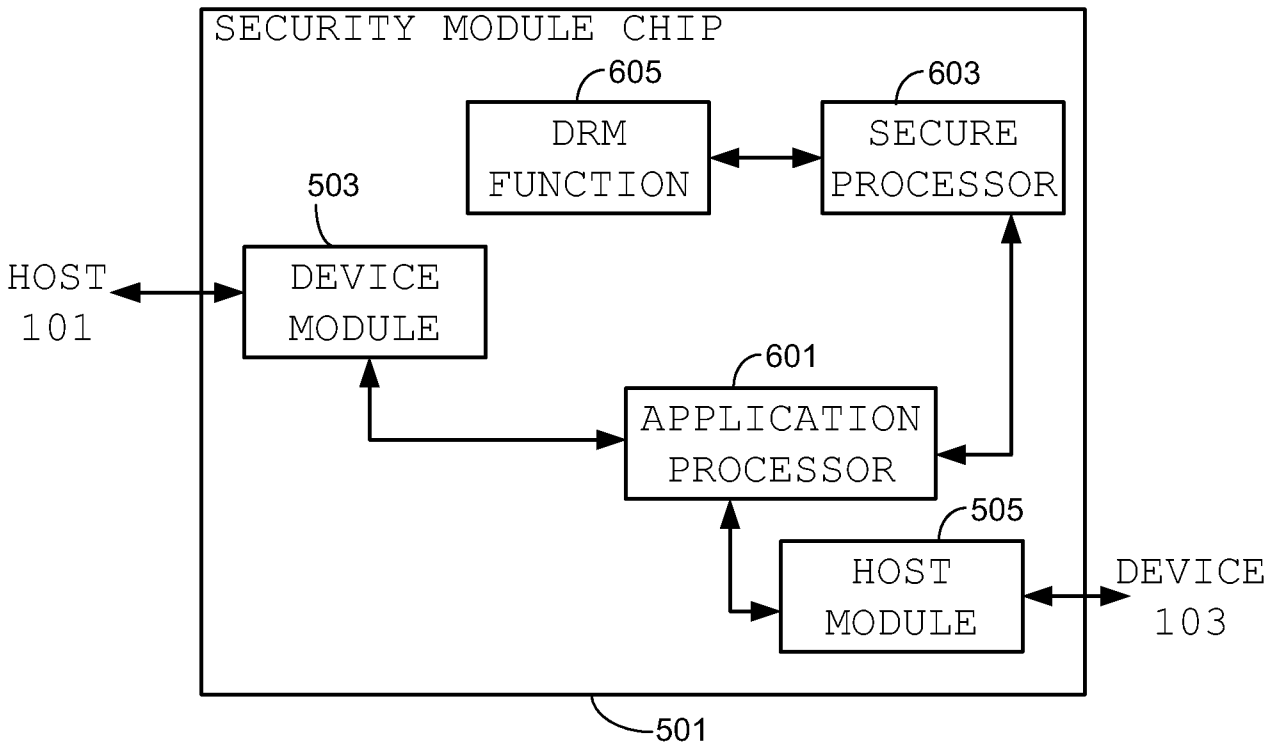


FIGURE 7

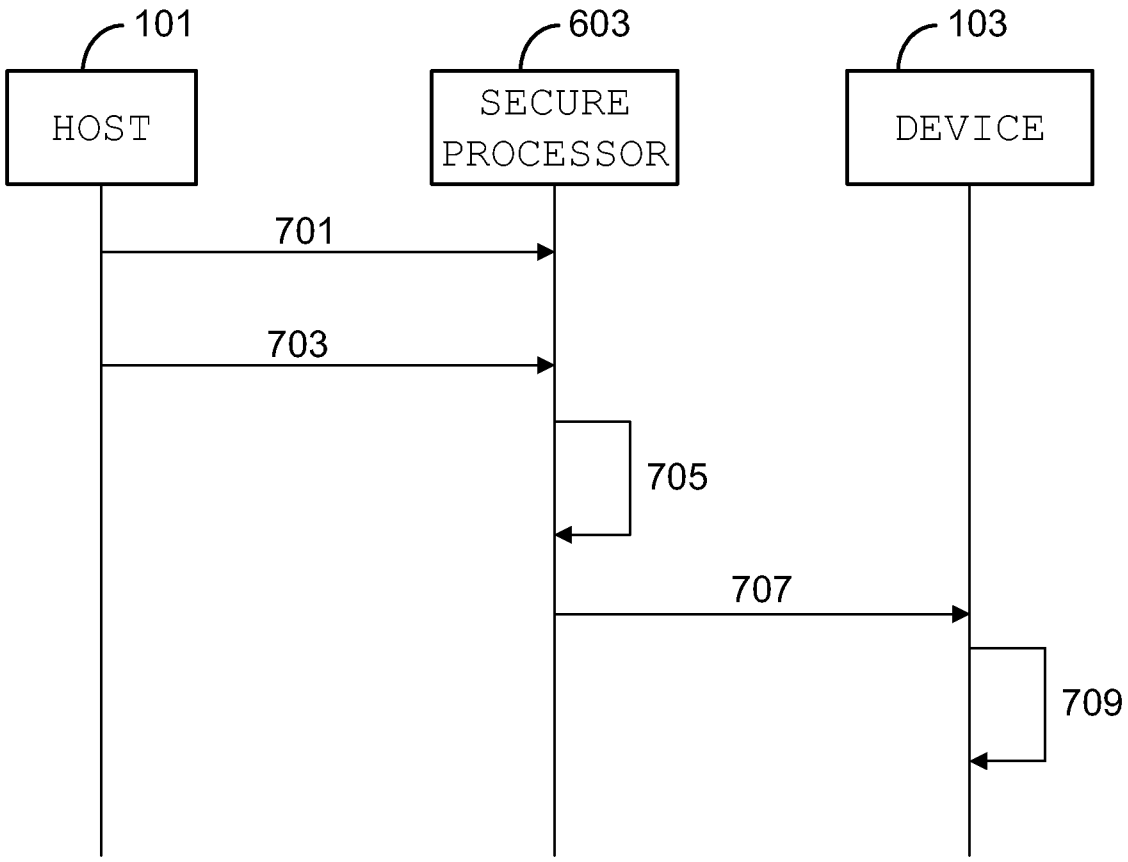


FIGURE 8

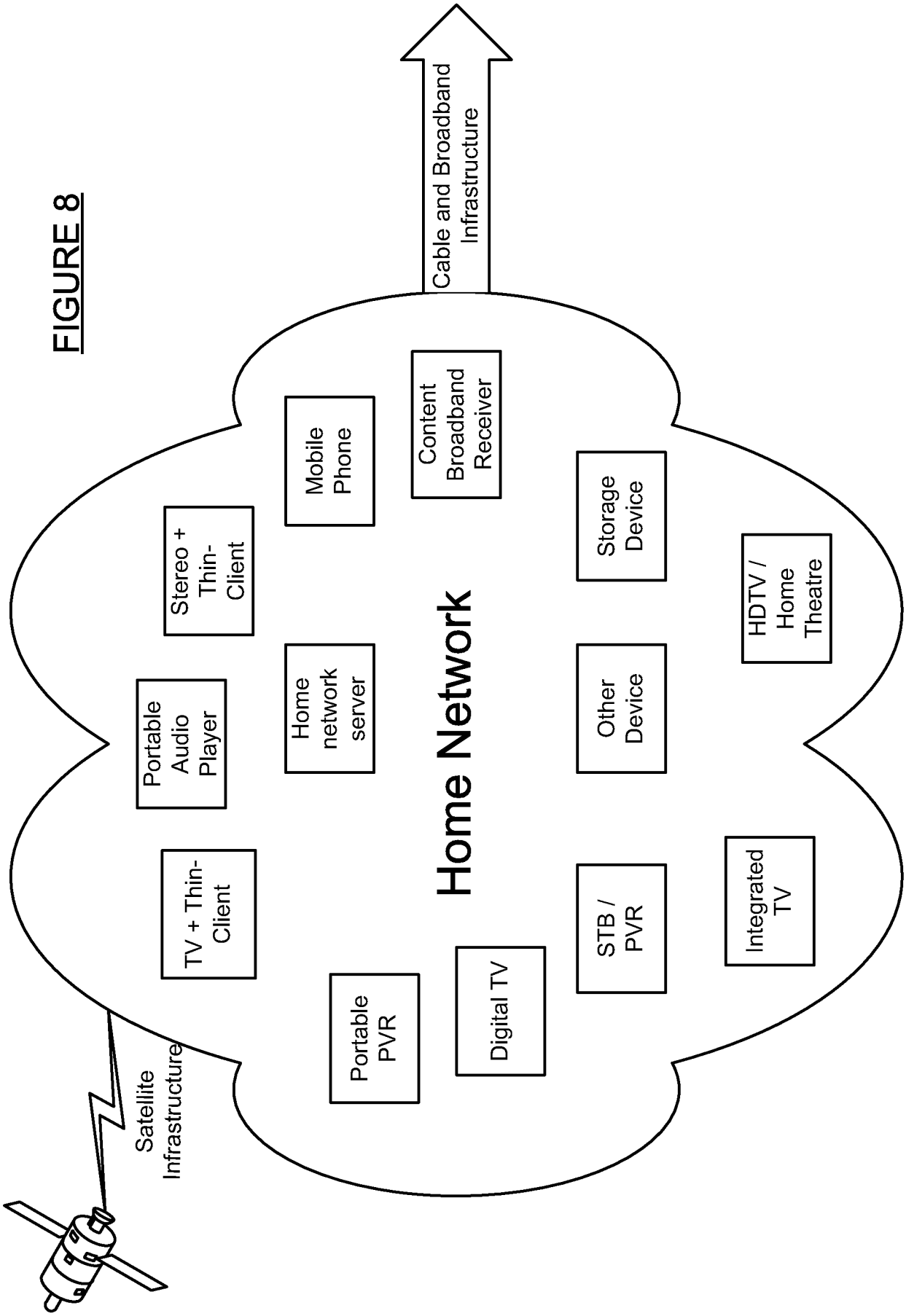

Cable and Broadband Infrastructure
Content Broadband Receiver
Mobile Phone
Stereo + Thin-Client
Storage Device
HDTV / Home Theatre
Portable Audio Player
Home network server
Other Device
TV + Thin-Client
Home Network
Portable PVR
Digital TV
STB / PVR
Integrated TV
Satellite Infrastructure

FIGURE 9

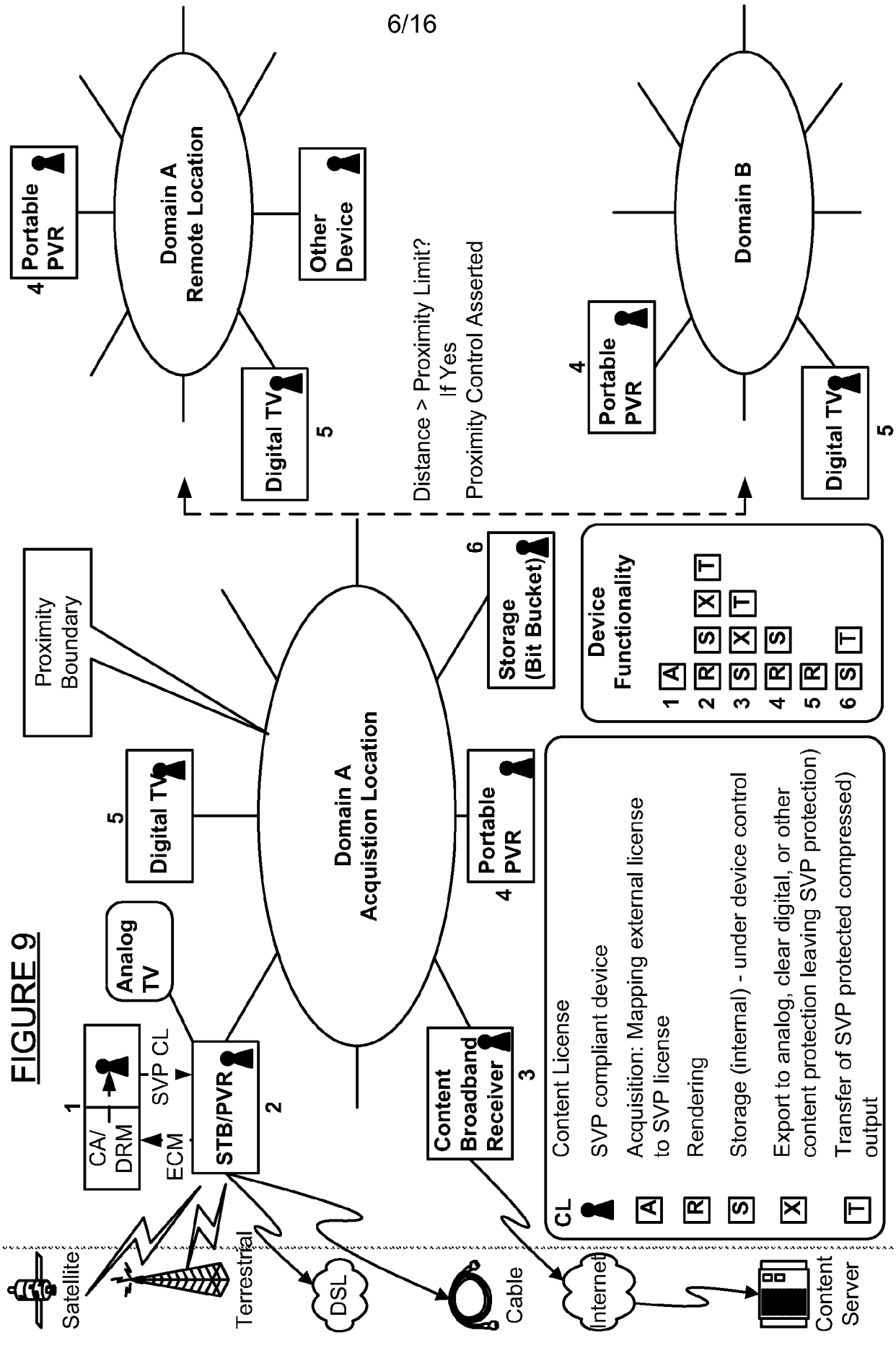

Satellite
Terrestrial
DSL
Cable
Internet
Content Server
CA/ DRM
1
ECM
SVP CL
STB/PVR
2
Analog TV
Digital TV
5
Proximity Boundary
Domain A Acquistion Location
Content Broadband Receiver
3
Portable PVR
4
Storage (Bit Bucket)
6
Distance > Proximity Limit?
If Yes
Proximity Control Asserted
Domain A Remote Location
Portable PVR
4
Other Device
Digital TV
5
Domain B
Portable PVR
4
Digital TV
5
Device Functionality
1 A
2 R S X T
3 S X T
4 R S
5 R
6 S T
CL Content License
SVP compliant device
A Acquisition: Mapping external license to SVP license
R Rendering
S Storage (internal) - under device control
X Export to analog, clear digital, or other content protection leaving SVP protection)
T Transfer of SVP protected compressed) output

FIGURE 10

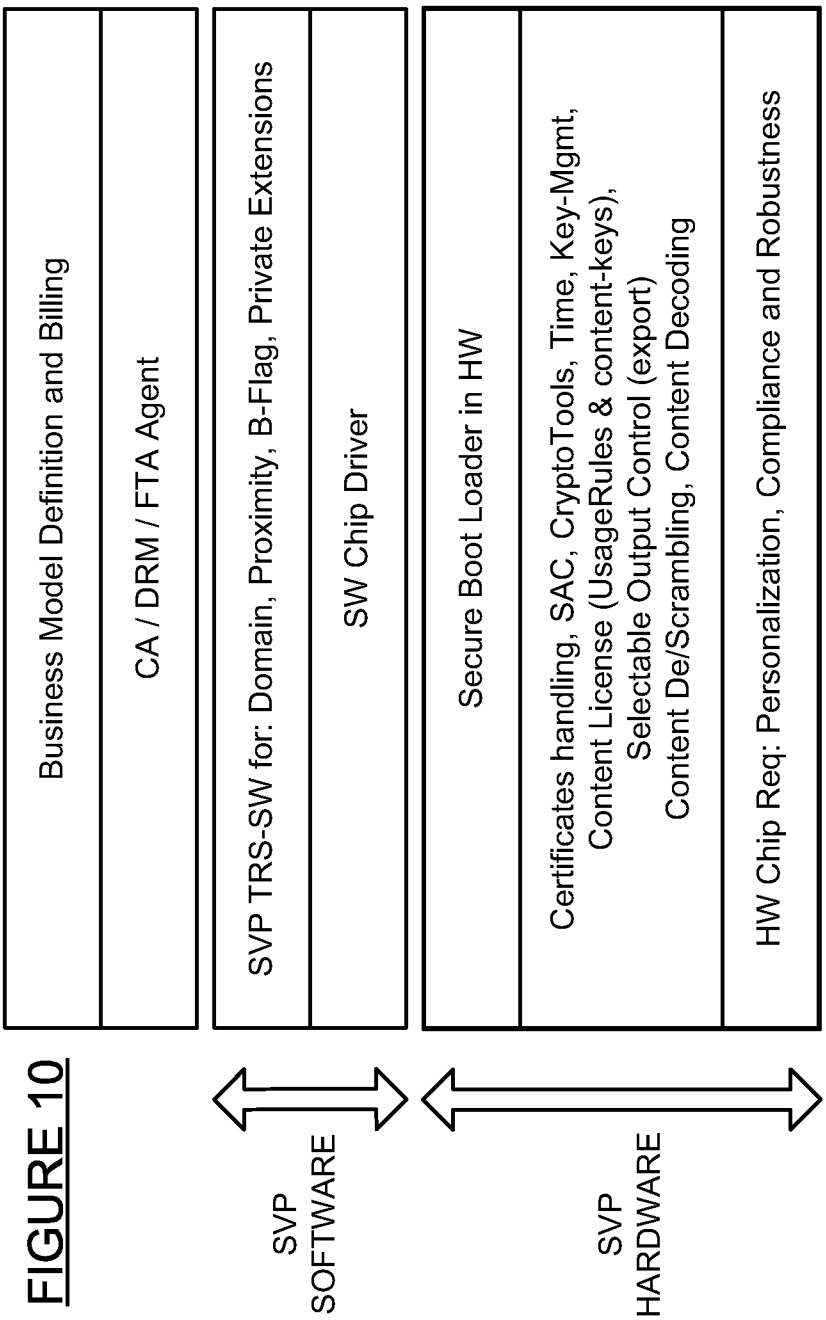
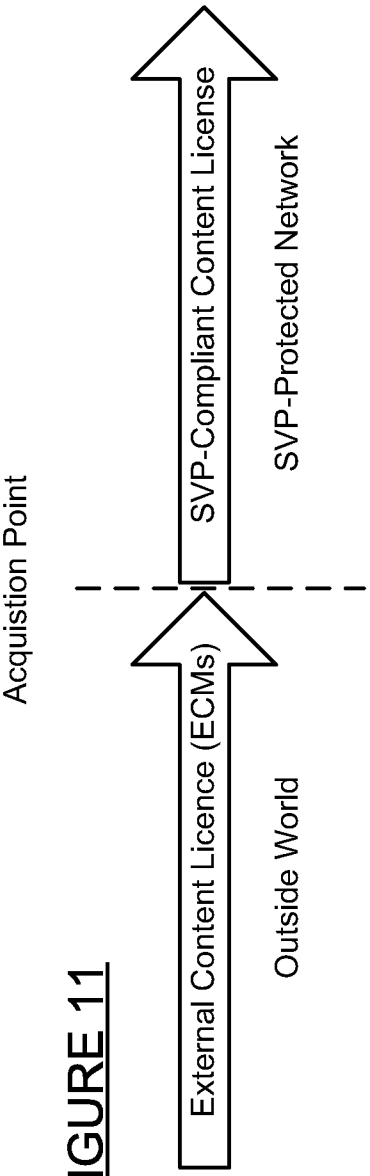


FIGURE 11



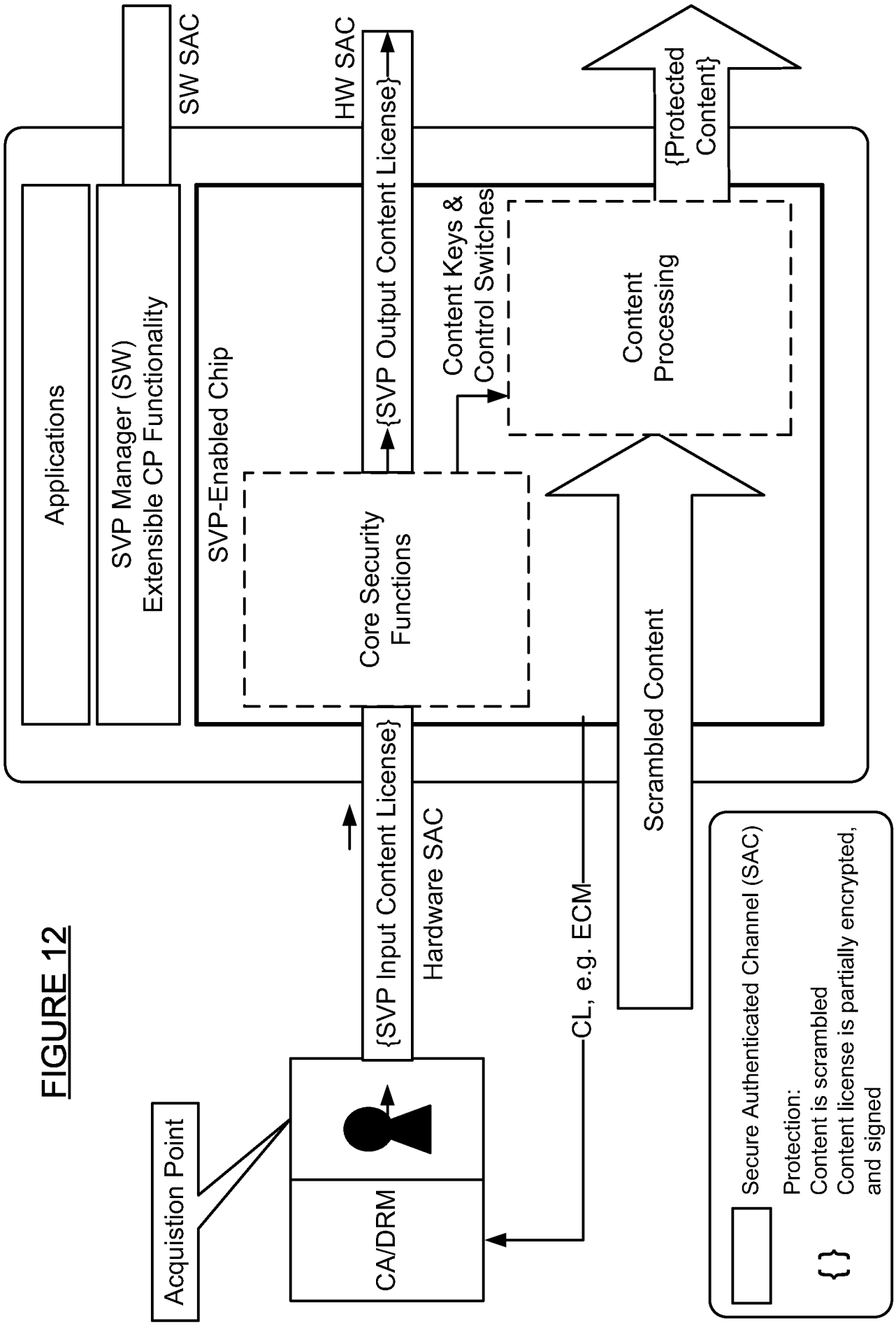

SW SAC
HW SAC
{SVP Output Content License}
{Protected Content}
Applications
SVP Manager (SW)
Extensible CP Functionality
SVP-Enabled Chip
Content Keys & Control Switches
Content Processing
Core Security Functions
{SVP Input Content License}
Hardware SAC
Scrambled Content
CL, e.g. ECM
Acquistion Point
CA/DRM
Secure Authenticated Channel (SAC)
Protection:
Content is scrambled
Content license is partially encrypted, and signed
{ }

FIGURE 12

FIGURE 13

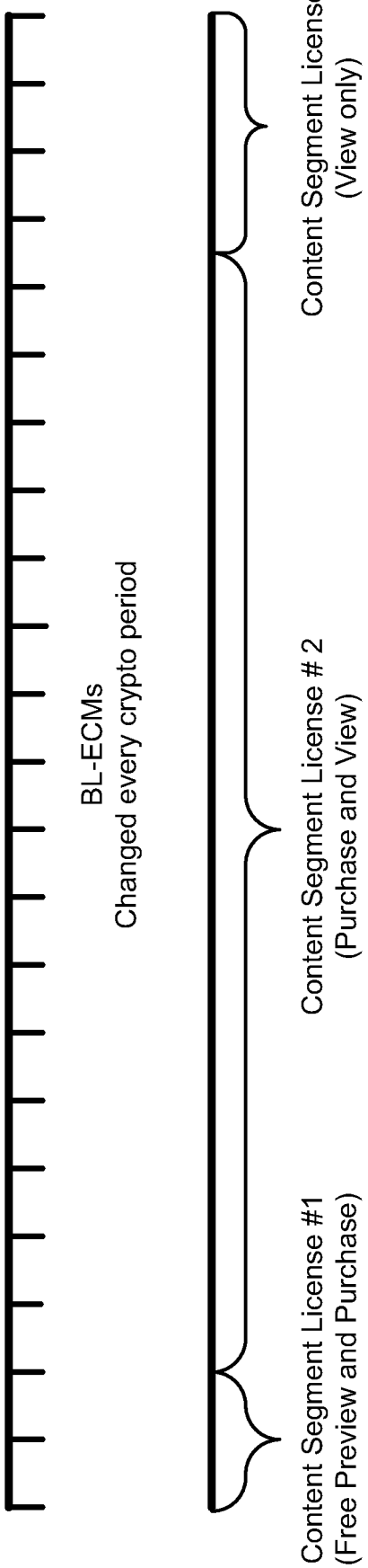


FIGURE 14

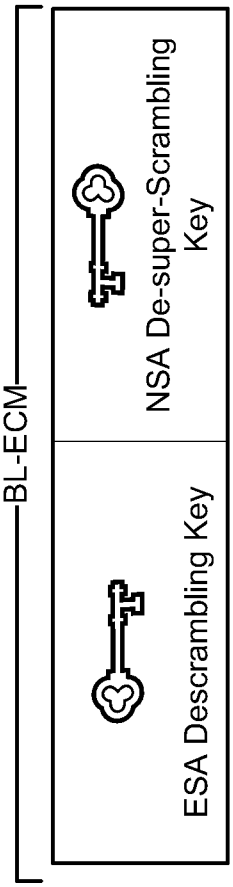
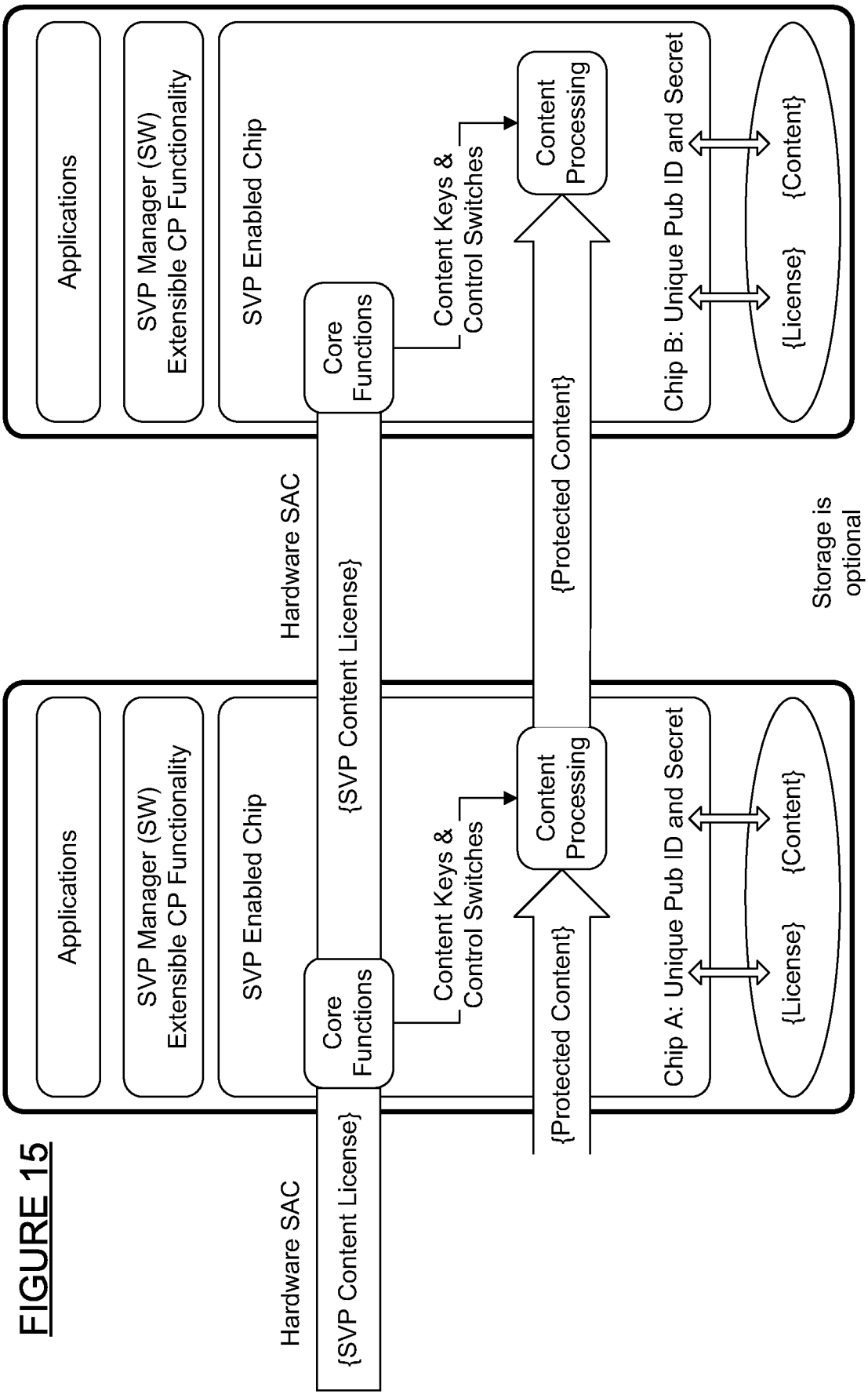


FIGURE 15


Applications
SVP Manager (SW)
Extensible CP Functionality
SVP Enabled Chip
Core Functions
Content Keys & Control Switches
Content Processing
Chip A: Unique Pub ID and Secret
{License}
{Content}
{SVP Content License}
{Protected Content}
Hardware SAC
Applications
SVP Manager (SW)
Extensible CP Functionality
SVP Enabled Chip
Core Functions
Content Keys & Control Switches
Content Processing
Chip B: Unique Pub ID and Secret
{License}
{Content}
{SVP Content License}
{Protected Content}
Hardware SAC
Storage is optional

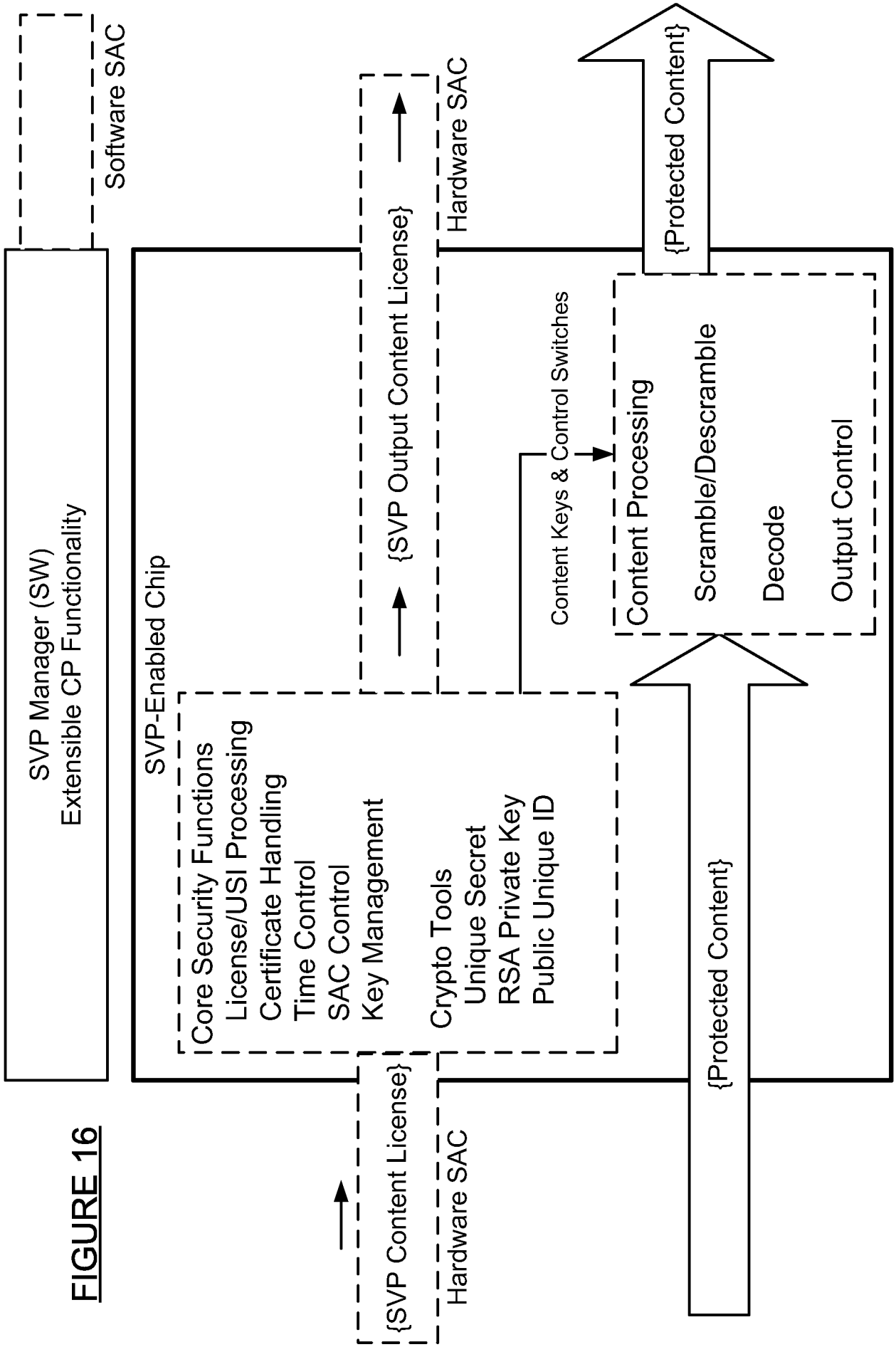

SVP Manager (SW)
Extensible CP Functionality
Software SAC
SVP-Enabled Chip
Core Security Functions
License/USI Processing
Certificate Handling
Time Control
SAC Control
Key Management
Crypto Tools
Unique Secret
RSA Private Key
Public Unique ID
{SVP Output Content License}
Hardware SAC
{SVP Content License}
Hardware SAC
Content Keys & Control Switches
Content Processing
Scramble/Descramble
Decode
Output Control
{Protected Content}
{Protected Content}

FIGURE 16

FIGURE 17

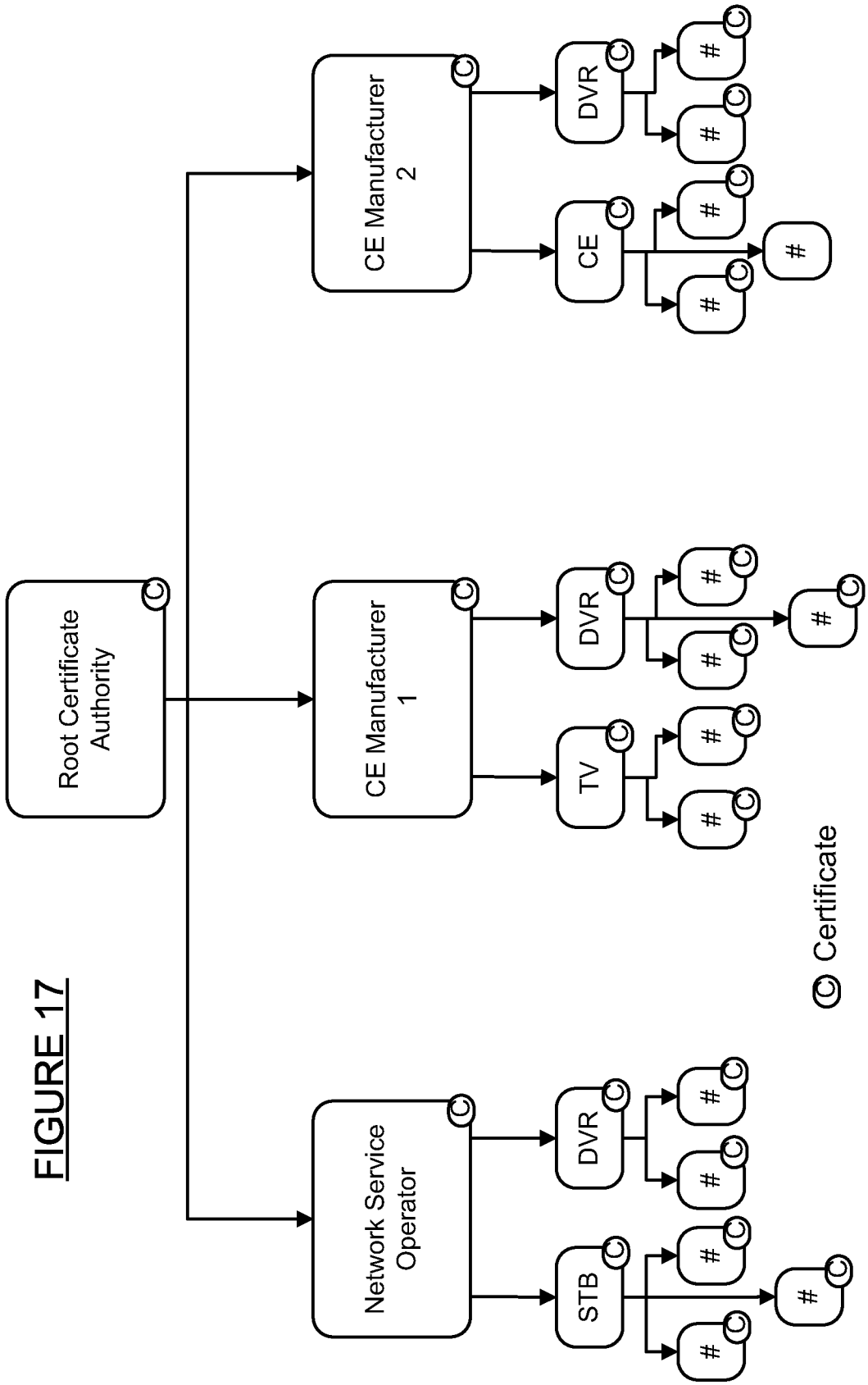
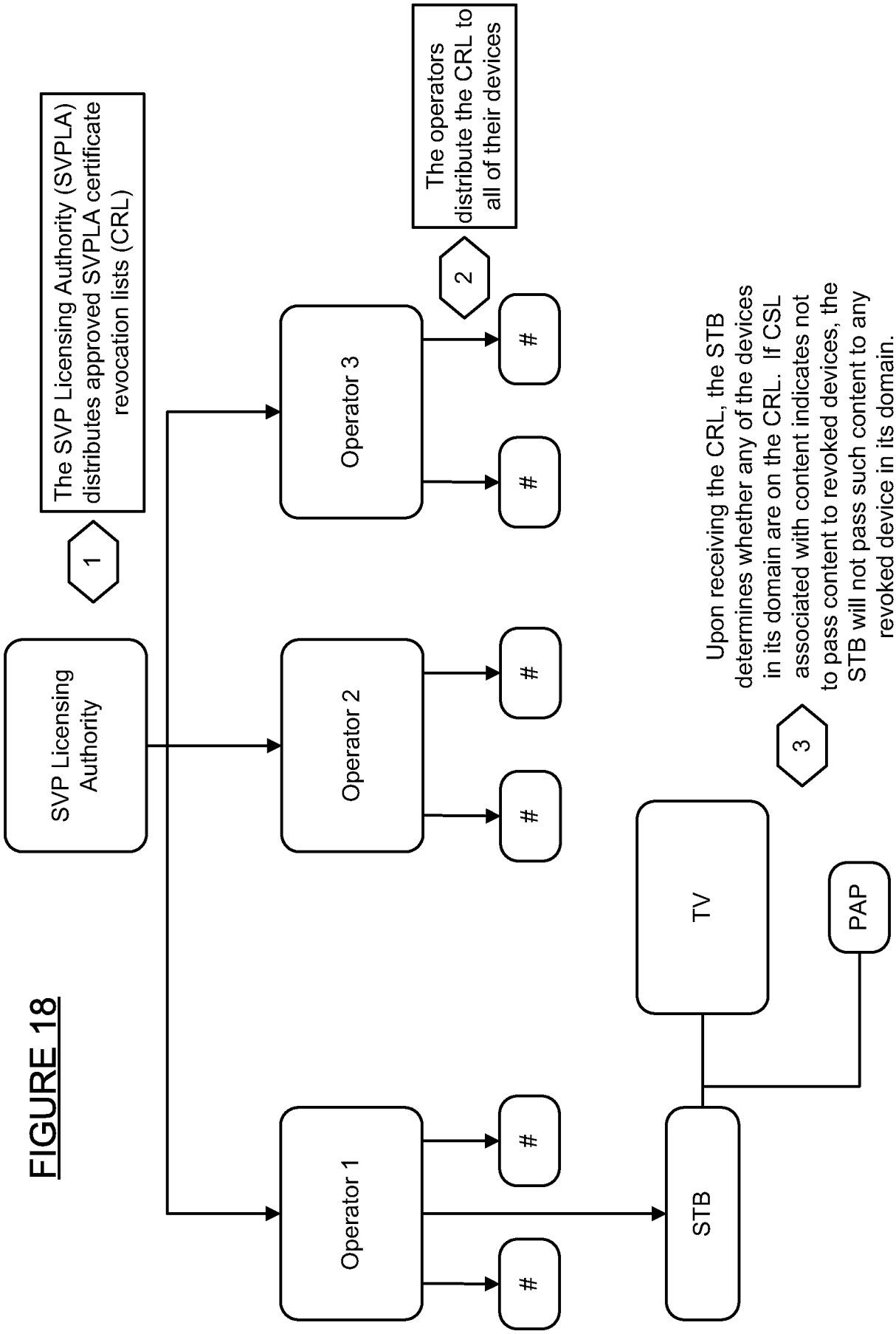

Root Certificate Authority
CE Manufacturer 1
CE Manufacturer 2
Network Service Operator
TV
DVR
CE
STB
#
© Certificate

FIGURE 18


SVP Licensing Authority
1
The SVP Licensing Authority (SVPLA) distributes approved SVPLA certificate revocation lists (CRL)
Operator 1
Operator 2
Operator 3
#
#
#
#
#
#
2
The operators distribute the CRL to all of their devices
STB
TV
PAP
3
Upon receiving the CRL, the STB determines whether any of the devices in its domain are on the CRL. If CSL associated with content indicates not to pass content to revoked devices, the STB will not pass such content to any revoked device in its domain.

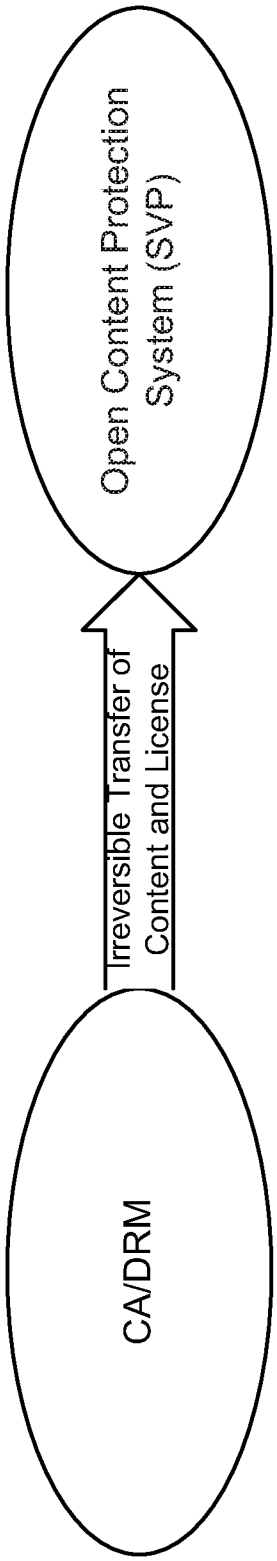


FIGURE 19

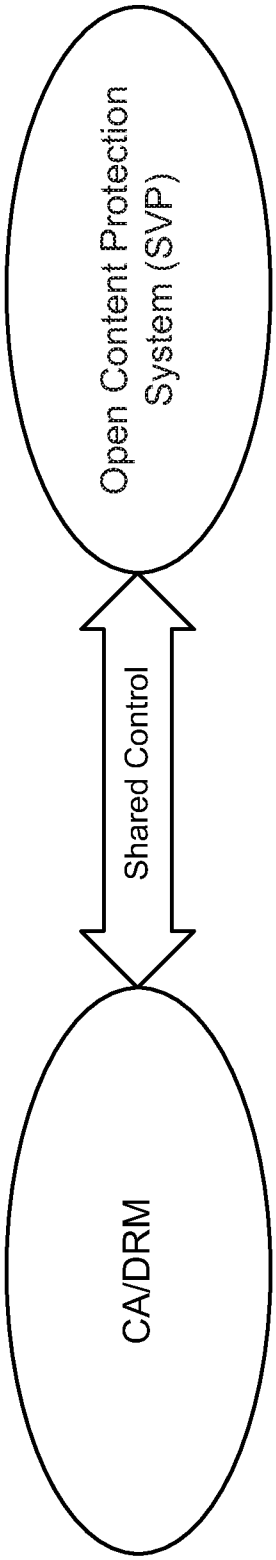


FIGURE 20

FIGURE 21

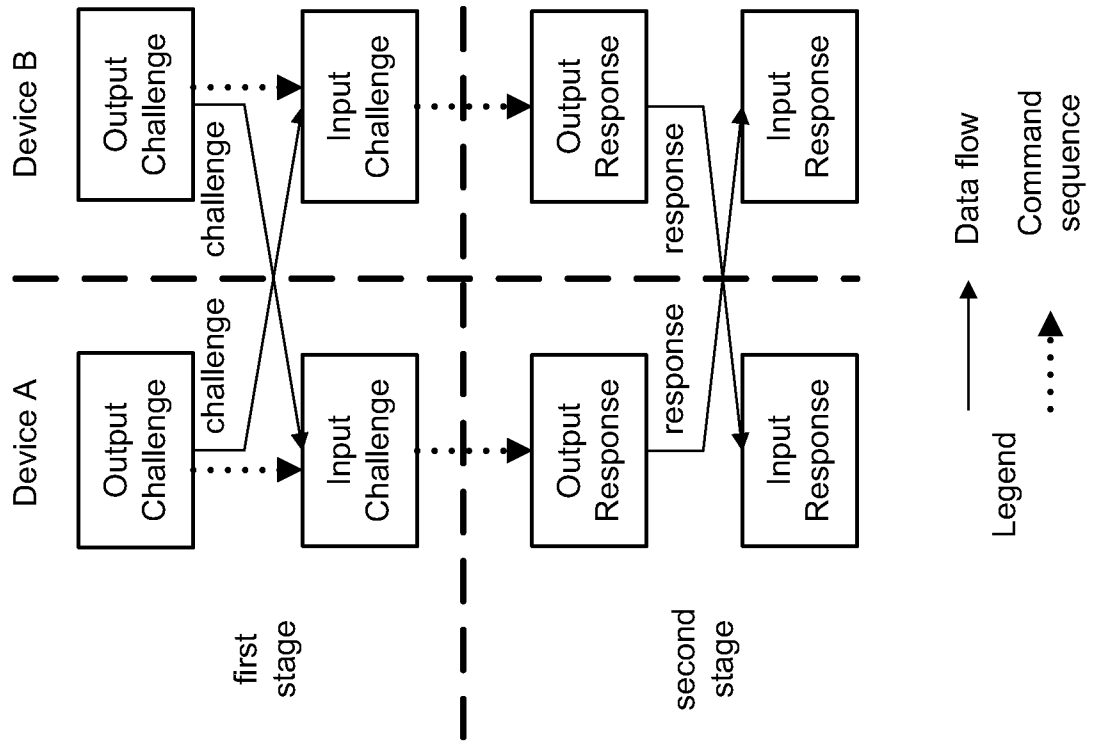


FIGURE 22

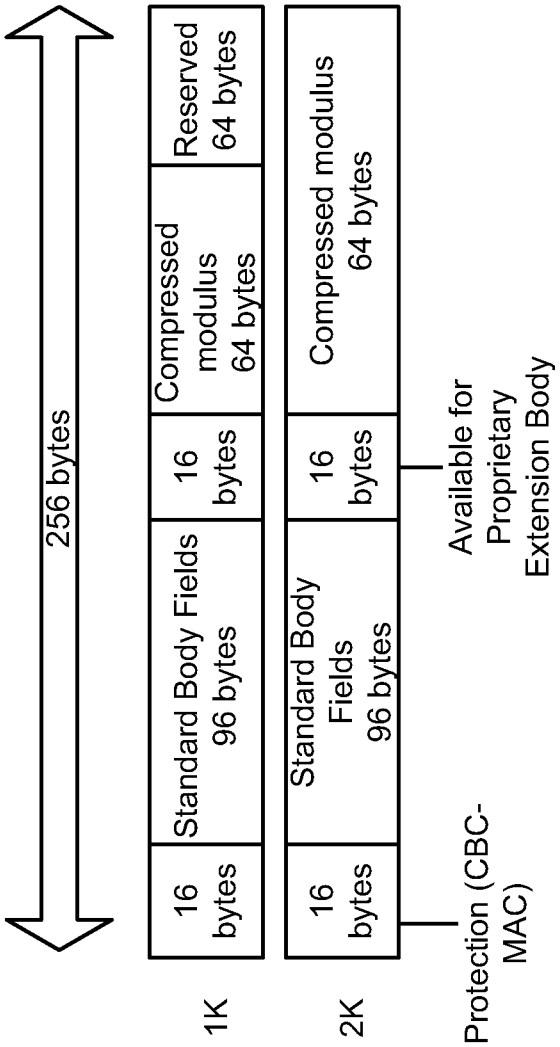
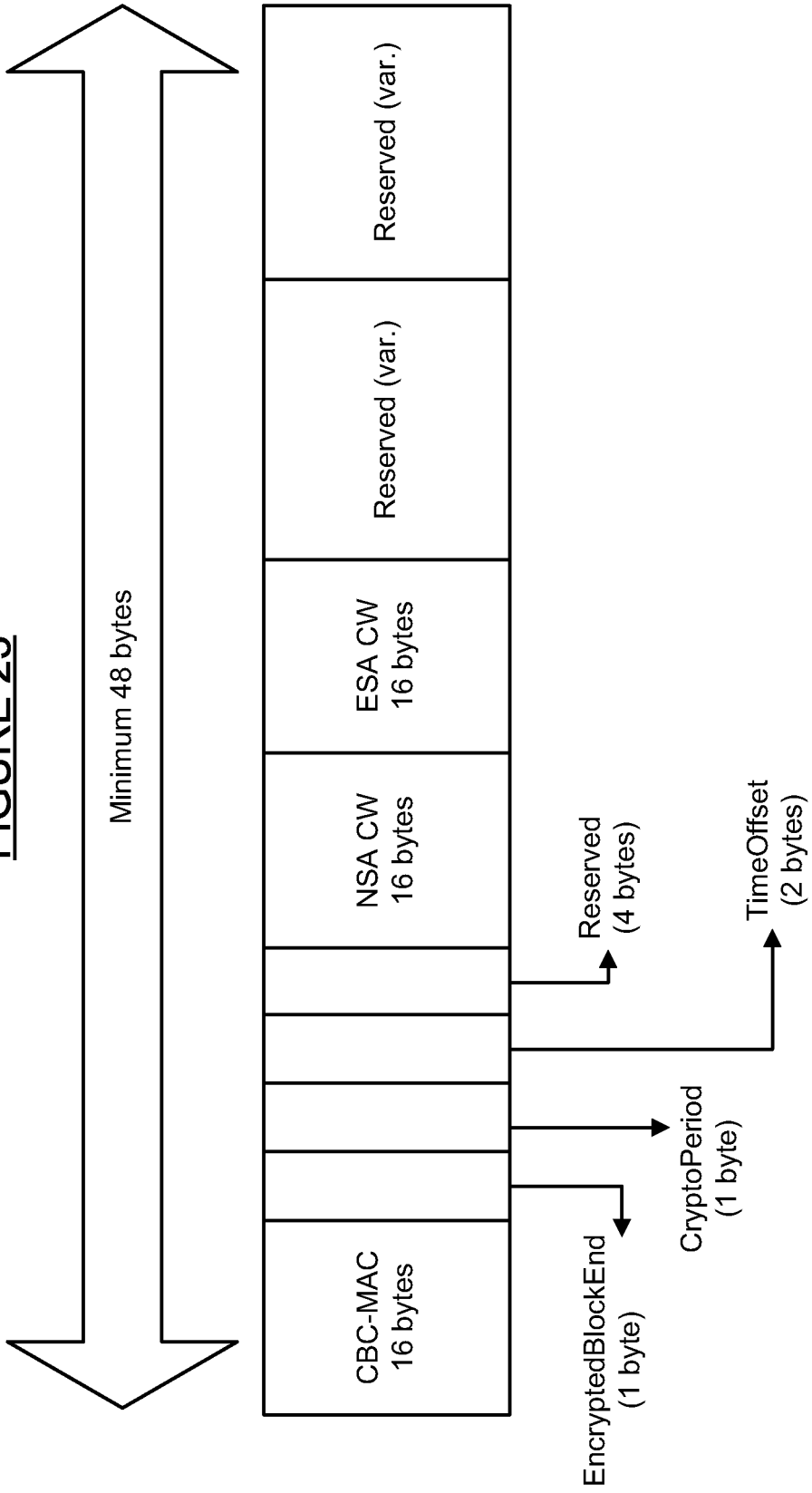


FIGURE 23


Minimum 48 bytes
CBC-MAC
16 bytes
NSA CW
16 bytes
ESA CW
16 bytes
Reserved (var.)
Reserved (var.)
EncryptedBlockEnd
(1 byte)
CryptoPeriod
(1 byte)
Reserved
(4 bytes)
TimeOffset
(2 bytes)

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2008/050541

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/00 H04N7/167

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 H04L

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 practical, search terms used)
EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2004/057830 A (KONINKL PHILIPS ELECTRONICS NV [NL]; VAN DEN HEUVEL SEBASTIAAN A F [NL]) 8 July 2004 (2004-07-08)	1,6-9, 12-15, 20-23, 26-29
Y	page 2, line 29 - page 3, line 10 page 4, line 17 - line 23 page 8, line 31 - page 9, line 27 page 10, line 27 - line 31; figure 3	5,10,19, 24
X	WO 98/21852 A (SCIENTIFIC ATLANTA [US]) 22 May 1998 (1998-05-22) page 8, line 12 - page 9, line 14 page 12, line 20 - page 13, line 23 page 14, line 11 - line 13	1,8-15, 22-29

-/--

[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 document 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
14 October 2008	27/10/2008

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	Holper, Georges

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2008/050541

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2005/066353 A1 (FRANSDONK ROBERT [US]) 24 March 2005 (2005-03-24) paragraph [0024] paragraph [0045]	5,10,19, 24
A	US 2005/144468 A1 (NORTHCUTT J D [US] ET AL) 30 June 2005 (2005-06-30) paragraphs [0207] - [0209], [0217], [0218]	1,15,29

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2008/050541

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2004057830 A	08-07-2004	AU 2003303169 A1	14-07-2004
		CN 1729668 A	01-02-2006
		JP 2006511151 T	30-03-2006
		KR 20050087843 A	31-08-2005
		US 2006285686 A1	21-12-2006
WO 9821852 A	22-05-1998	AU 7182398 A	03-06-1998
		BR 9712999 A	25-01-2000
		EP 1023795 A1	02-08-2000
		JP 3700982 B2	28-09-2005
		JP 2000516422 T	05-12-2000
		JP 3978441 B2	19-09-2007
		JP 2004312772 A	04-11-2004
		US 5937067 A	10-08-1999
US 2005066353 A1	24-03-2005	NONE	
US 2005144468 A1	30-06-2005	US 2008148063 A1	19-06-2008