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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 December 2010 (16.12.2010)

PCT

(10) International Publication Number
WO 2010/143088 A1

(51) International Patent Classification:
H04N 7/167 (2006.01) *H04N 5/00* (2006.01)

(21) International Application Number:
PCT/IB2010/052136

(22) International Filing Date:
13 May 2010 (13.05.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/268,152 8 June 2009 (08.06.2009) US

(71) Applicant *(for all designated States except US)*: **NDS LIMITED** [GB/GB]; One London Road, Staines Middlesex TW18 4EX (GB).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **SANDLER, Leonid** [IL/IL]; Avraham Ferera 10/74, 96429 Jerusalem (IL). **TSURIA, Yossi** [IL/IL]; 14 Rabenu Polity Street, 93390 Jerusalem (IL).

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

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

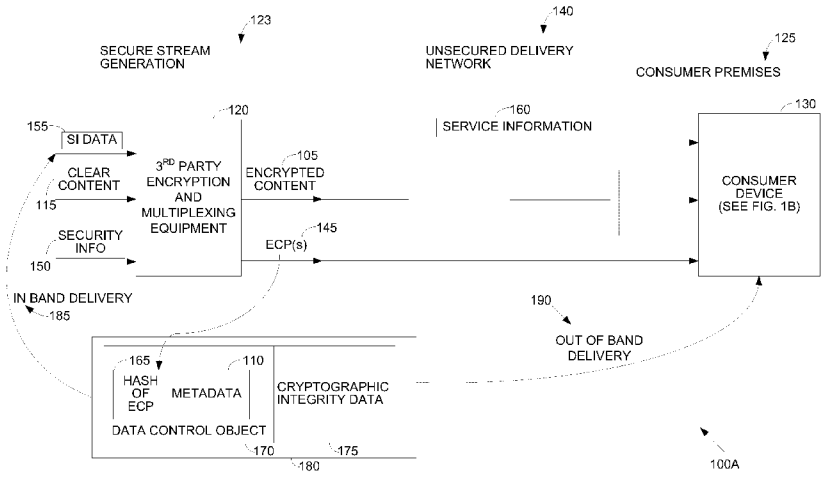
Published:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) Title: SECURE ASSOCIATION OF METADATA WITH CONTENT

FIG. 1A



(57) Abstract: A method and system for associating metadata with an encrypted content item, the method including receiving metadata for association with a content item, receiving an entitlement control packet (ECP) associated with the content item, applying a cryptographic hash function to the ECP, thereby generating an ECP hash value, combining the ECP hash value with the metadata, thereby creating a data control object, performing a cryptographic operation on the data control object, thereby generating cryptographic integrity data, and joining the cryptographic integrity data to the data control object after the cryptographic operation, wherein usage of the content by the recipient is dependent on both a validation of the ECP hash value and a validation of the cryptographic integrity data. Related apparatus and methods are also described.

WO 2010/143088 A1

SECURE ASSOCIATION OF METADATA WITH CONTENT

RELATED APPLICATION INFORMATION

The present application claims the benefit of priority from US provisional application number 61/268,152 of Leonid Sandler, et al., filed 8 June 2009, the disclosure of which is hereby incorporated herein by reference.

BACKGROUND OF THE INVENTION

The following standards are considered particularly relevant to the present invention:

Digital Video Broadcast (DVB); Support for Use of Scrambling and Conditional Access (CA) within Digital Broadcasting Systems, October 1996, ETR 289;

Information Technology - Generic Coding of Moving Pictures and Associated Audio Information: Systems, December 2000, ISO/IEC 13818-1;

OpenCable Application Platform Specifications, OCAP 1.1 Profile, August 2008, OC-SP-OCAP1.1-D02-080807; and

OpenCable Specifications, CableCARD 2.0 Interface Specification, February, 2009, OC-SP-CCIF2.0-I17-090206;

OC-SP-OCAP1.1-D02-080807; OC-SP-CCIF2.0-I17-090206; ETR 289; and ISO/IEC 13818-1 are hereby incorporated by reference.

The SHA-1 and SHA-2 hash algorithms (collectively including all of: SHA-224; SHA-256; SHA-384; and SHA-512) are specified in FIPS 180.

A list of SHA-3 hash algorithm candidates is found at: csrc.nist.gov/groups/ST/hash/sha-3/Round1/submissions_rnd1.html.

The following references, listed by publication number, are believed to reflect the current state of the art:

EP 1732005 of NEC Corporation;

WO2008/060388 of Time Warner Cable, Inc.;

US 2008/0123845 of Candelore;

US 2008/012386 of Candelore; and

US 2008/183656 of Perng, et al.

SUMMARY OF THE INVENTION

There is thus provided in accordance with an embodiment of the present invention a method for associating metadata with an encrypted content item, the method including receiving metadata for association with a content item, receiving an entitlement control packet (ECP) associated with the content item, applying a cryptographic hash function to the ECP, thereby generating an ECP hash value, combining the ECP hash value with the metadata, thereby creating a data control object, performing a cryptographic operation on the data control object, thereby generating cryptographic integrity data, and joining the cryptographic integrity data to the data control object after the cryptographic operation, wherein usage of the content by the recipient is dependent on both a validation of the ECP hash value and a validation of the cryptographic integrity data.

Further in accordance with an embodiment of the present invention the ECP includes one of an entitlement control message (ECM), and a digital rights management (DRM) content license.

Still further in accordance with an embodiment of the present invention and including sending the cryptographically associated data control object joined to the cryptographic integrity data to a recipient.

Additionally in accordance with an embodiment of the present invention the sending includes sending in- band sending.

Moreover in accordance with an embodiment of the present invention the sending includes out-of-band sending.

Further in accordance with an embodiment of the present invention the metadata includes service information.

Still further in accordance with an embodiment of the present invention the metadata includes a usage rule governing the usage of the content item.

Additionally in accordance with an embodiment of the present invention the cryptographically associating the combined ECP hash value and the metadata which include the data control object includes digitally signing the data control object, thereby generating a digital signature.

Moreover in accordance with an embodiment of the present invention the joined cryptographic integrity data includes the digital signature.

Further in accordance with an embodiment of the present invention the cryptographically associating the data control object includes encrypting the data control object according to a key, the key including a secret shared with the recipient.

Still further in accordance with an embodiment of the present invention the joined cryptographic integrity data includes a reference to the secret shared with the recipient.

Additionally in accordance with an embodiment of the present invention the cryptographic hash function includes one of SHA-1, SHA-2, and a SHA-3 candidate function.

. There is also provided in accordance with another embodiment of the present invention a method for content utilization, the method including receiving an encrypted content item, receiving an entitlement control message (ECP) associated with the encrypted content item, receiving a data control object, the data control object including an ECP hash value, metadata, and cryptographic integrity data, using the cryptographic integrity data to cryptographically verify the integrity of the data control object, applying a cryptographic hash function to the received ECP, thereby generating a second ECP hash value, comparing the second ECP hash value with the received ECP hash value, and performing metadata processing if the result of the comparing is positive, thereby assuring the metadata cryptographically corresponds to the content item.

Further in accordance with an embodiment of the present invention the ECP includes one of an entitlement control message (ECM), and a digital rights management (DRM) content license.

Still further in accordance with an embodiment of the present invention the receiving the data control object includes in-band receiving.

Additionally in accordance with an embodiment of the present invention the receiving the data control object includes out-of-band receiving.

Moreover in accordance with an embodiment of the present invention the metadata includes service information.

Further in accordance with an embodiment of the present invention the metadata includes a usage rule governing the usage of the content item.

Still further in accordance with an embodiment of the present invention the ECP hash value and the metadata included in the data control object have been digitally signed.

Additionally in accordance with an embodiment of the present invention the cryptographic integrity data includes the digital signature of the ECP hash value and the metadata.

Moreover in accordance with an embodiment of the present invention the ECP hash value and the metadata included in the data control object have been encrypted.

Further in accordance with an embodiment of the present invention the encrypted ECP hash value and the metadata have been encrypted according to a key, the key including a secret shared with the sender of the received data control object.

Still further in accordance with an embodiment of the present invention the cryptographic integrity data includes a reference to the shared secret.

Additionally in accordance with an embodiment of the present invention the using the cryptographic integrity data to cryptographically verify the ECP hash value and the metadata includes using the key to decrypt the encrypted ECP hash value and metadata.

Moreover in accordance with an embodiment of the present invention the cryptographic hash function includes one of SHA-1, SHA-2, and SHA-3 candidate function.

There is also provided in accordance with still another embodiment of the present invention a system for associating metadata with an encrypted content item, the system including a metadata receiver operative to receive metadata for association with a content item, an entitlement control packet (ECP) receiver operative to receive an ECP associated with the content item, a cryptographic engine operative to apply a cryptographic hash function to the ECP, thereby generating an ECP hash value, a processor operative to combine the ECP hash value with the metadata, thereby creating a data control object, a second

cryptographic engine which performs a cryptographic operation on the data control object, thereby generating cryptographic integrity data, and a second processor which joins the cryptographic integrity data to the data control object after the cryptographic operation, wherein usage of the content by the recipient is dependent on both a validation of the ECP hash value and a validation of the cryptographic integrity data.

There is also provided in accordance with still another embodiment of the present invention a system for content utilization, the system including a content receiver operative to receive an encrypted content item, an entitlement control packet (ECP) receiver operative to receive an ECP associated with the encrypted content item, a data control object receiver operative to receive a data control object , the data control object including an ECP hash value, metadata, and cryptographic integrity data, a cryptographic engine operative to use the cryptographic integrity data to cryptographically verify the integrity of the data control object, a second cryptographic engine operative to apply a cryptographic hash function to the received ECP, thereby generating a second ECP hash value, a comparing processor operative to compare the second ECP hash value with the received ECP hash value, and a metadata processor operative to perform metadata processing if the result of the comparing is positive, thereby assuring the metadata cryptographically corresponds to the content item.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

Figs. 1A and 1B, taken together, are a simplified block diagram of data flow in a content distribution system, in which encrypted content and metadata associated with the encrypted content are depicted, the content distribution system constructed and operative in accordance with an embodiment of the present invention;

Fig. 2 is a simplified block diagram depicting production, during secure stream generation, of a secure metadata object in the system of Figs. 1A and 1B;

Fig. 3A is a simplified block diagram of a first embodiment of a secure metadata object of Figs. 1A and 1B;

Fig. 3B is a simplified block diagram of a second embodiment of the secure metadata object of Figs. 1A and 1B;

Fig. 4 is a simplified block diagram depicting, at a consumer device, an evaluation of the secure metadata object in the system of Figs. 1A and 1B; and

Figs. 5 - 6 are simplified flowcharts of preferred methods of operation of the system of Fig. 1.

DETAILED DESCRIPTION OF AN EMBODIMENT

Reference is now made to Figs. 1A and 1B, which, taken together, are a simplified block diagram of data flow in a content distribution system 100A, 100B, in which encrypted content 105 and metadata 110 associated with the encrypted content 105 are depicted, the content distribution system 100A, 100B constructed and operative in accordance with an embodiment of the present invention. Those skilled in the art will appreciate that the metadata 110 is generated outside of the content distribution system 100A, 100B.

Throughout the present specification and claims the term "metadata" is used for ease of description. However, any appropriate cryptographic equivalent of the metadata may be used in the methods and systems described herein.

Content protection systems are typically based on encryption of the clear content 115. As is well known in the art, encryption of the clear content 115 is according to secret keys (not depicted), also known as control words. The keys are delivered separately to a consumer device 130 in some form of entitlement control packets (ECPs). For example and without limiting the generality of the foregoing, ECPs 145 may comprise Entitlement Control Messages (ECMs) defined by the MPEG2 System standard (ISO/IEC 13818-1, referred to above), or, alternatively, so called "content licenses" used in various DRM (digital rights management) systems.

Those skilled in the art will appreciate that each individual ECP 145 is uniquely associated with at least one portion of the encrypted content 105. For example, one crypto-period (a *crypto-period* is the time span during which a specific cryptographic key (control word) is intended for use.). For example and without limiting the generality of the foregoing, if the individual ECP 145 comprises an ECM, then the ECM is required by the consumer device 130 in order to produce a control word enabling decryption of the a first portion of encrypted content 105 for one crypto-period. A second ECM is required by the consumer device 130 in order to produce a control word enabling decryption of a second portion of encrypted content for the next crypto-period, and so forth for each ensuing crypto-period.

In some cases it is necessary to provide additional information to the consumer device 130 (hereinafter, "metadata" 110), as explained below. The metadata 110, in such cases, is often cryptographically associated with such encrypted content 105. Further, it is often the case that any underlying content protection system cannot be utilized or modified in order to cryptographically associate the metadata 110 with the encrypted content 105. For example and without limiting the generality of the foregoing, clear content 115 (the term "clear", as used herein, as in, "clear content", is used to mean not encrypted; that is to say, clear content is content which is not encrypted) may be encrypted using a 3rd party system 120. As a non-limiting example of a typical 3rd party system 120, the 3rd party system 120 would comprise an MPEG2 compliant encryption and multiplexing 3rd party system 120. The 3rd party system 120, which is operative during secure stream generation 123 typically further comprises components of a conditional access (CA) system. Decryption of the encrypted content 105 is performed on consumer premises 125 in the consumer device 130 comprising by a 3rd party security component 135 such as CableCard (see, for instance, OC-SP-CCIF2.0-I17-090206 and OC-SP-OCAP1.1-D02-080807, referred to above).

Typically, the 3rd party security component 135, such as the CableCard, comprises an interface which cannot be modified or extended for the purposes of metadata insertion. However, other components in the consumer device 130 may require metadata 110 related, for example, to usage rules of the encrypted content 105 in a home network environment. Such metadata 110 must be securely associated with the content 105. If the metadata 110 is not securely associated with the content 105, there is a chance that decoupling between the content 105 and the metadata 110 may occur, particularly while the content is in an unsecured delivery network 140 during delivery to the consumer premises 125. Alternatively, decoupling between the content 105 and the metadata 110 may occur at a later time at the consumer premises 125.

One method of the present invention allows secure association of any kind of metadata 110 with the encrypted content 105 in any environment or system wherein the encrypted content 105 is already associated with any form of entitlement control packets 145. It is appreciated that the method of the present

invention described herein enables performing the association of the encrypted content 105 with the metadata 110 without any understanding of the entitlement control packets 145 and without any cooperation from the owner of the entitlement control packets 145.

Those skilled in the art will appreciate that the method of the present invention described herein that establishes a cryptographic association between metadata 110 and the ECP 145 is cryptographically identical to the cryptographic association between the metadata 110 and the encrypted content 105 itself.

The operation of the system of Figs. 1A and 1B is now described. Clear content 115 is input into the 3rd party system 120. It is appreciated that the description of the encryption and multiplexing system 120 herein as an MPEG2 compliant encryption and multiplexing system 120 is by way of example only, and is not meant to be limiting. The 3rd party system 120 encrypts the clear content 115 and outputs the encrypted content 105. Security information 150 is also input into the 3rd party system 120. The 3rd party system 120 processes the input security information 150, and outputs ECPs 145. In addition, service information (SI) related data 155 is input into the 3rd party system 120 and Service Information (SI) 160 is output.

Reference is now additionally made to Fig. 2, which is a simplified block diagram depicting production, during secure stream generation, of a secure metadata object 180 in the system of Figs. 1A and 1B. Each individual ECP 145 is input into a cryptographic hash function 210. Any appropriate cryptographic hash function may be used, such as, example and without limiting the generality of the foregoing, SHA-1; SHA-2 (collectively including all of: SHA-224; SHA-256; SHA-384; and SHA-512); and various SHA-3 candidates. SHA-1 and SHA-2 are specified in FIPS 180. A list of SHA-3 candidates is found, at the time the present application was drafted, at: csrc.nist.gov/groups/ST/hash/sha-3/Round1/submissions_rnd1.html. The hash function 210 produces a hash 165 of the ECP 145.

The hash 165 of the ECP 145 is combined with the metadata 110, thereby producing a data control object 170. A crypto-engine 220 cryptographically associates the combined ECP hash 165 value and the metadata

110 which comprise the data control object 170, thereby generating cryptographic integrity data 175. The cryptographic integrity data 175 is joined to the data control object 170, thereby producing the secure metadata object 180. The secure metadata object 180 then sent to the consumer device 130. The nature of the joining of the cryptographic integrity data 175 to the data control object 170 is detailed below.

Throughout the present specification and claims the term "data control object 170" is used for ease of description. However, any appropriate cryptographic equivalent of the data control object 170 may be used in the methods and systems described herein.

The sending of the secure metadata object 180 to the consumer device 130 may be performed by any appropriate method known in the art for sending data between devices. For ease of depiction, Figs. 1A and 1B depict an in-band delivery method 185, whereby the secure metadata object 180 is sent to the consumer device 130 comprised in the SI data 155, as a portion of the service information 160. Alternatively, where an out-of-band delivery channel 190 is operative, the secure metadata object 180 may be sent to the consumer device 130 as out-of-band data. Out-of-band delivery channels 190 are known in the art, and include, for example and without limiting the generality of the foregoing, IP communication.

Returning to the discussion of the ECP 145 of Fig. 2, an encryptor 230 receives the clear content 115 and, using a control word 240 as an encryption key, encrypts the clear content 115. The 3rd party system 120 produces the ECP 145 for the control word 240, as is well know in the art.

The nature of the secure metadata object 180 is now discussed. Reference is now additionally made to Fig. 3A, which is a simplified block diagram of the secure metadata object 180 of Figs. 1A and 1B. In the first embodiment of the secure metadata object 180 of Figs. 1A and 1B, after the ECP 145 is prepared by the 3rd party system 120, a copy of the ECP 145 is input into a hash function 210, thereby producing the hash of the ECP 165. The hash of the ECP 165 is joined to the metadata 110, typically by concatenation of the hash of the ECP 165 and the metadata 110. The joined hash of the ECP 165 and metadata

110 are then cryptographically signed, thereby producing a cryptographic signature 310 of the joined hash of the ECP 165 and metadata 110. It is appreciated that the cryptographic signature 310 of Fig. 3A corresponds to the cryptographic integrity data 175 of Figs. 1A and 1B. For example and without limiting the generality of the foregoing, the cryptographic signature 310 can be produced using any appropriate well known public key infrastructure (PKI) signature routine. Those skilled in the art will appreciate that the hash of the ECP 165 is used the present embodiment of the invention only for size optimization. In principle, the entire ECP 145 itself can be used as well in the present embodiment of the invention. The use of the cryptographically signed joined hash of the ECP 165 and metadata 110 in the consumer premises 125 is described below.

Reference is now additionally made to Fig. 3B, which is a simplified block diagram of a second embodiment of the secure metadata object 180 of Figs. 1A and 1B. In the second embodiment of the data control object of Figs. 1A and 1B, after the ECP 145 is prepared by the 3rd party system 120, a copy of the ECP 145 is input into a hash function 210, thereby producing the hash of the ECP 165. The hash of the ECP 165 is joined to the metadata 110, typically by concatenation of the hash of the ECP 165 and the metadata 110. The joined hash of the ECP 165 and metadata 110 are then encrypted, thereby producing an encrypted data object 320 comprising the joined hash of the ECP 165 and metadata 110. For example and without limiting the generality of the foregoing, the encrypted data object 320 can be produced using any appropriate well known encryption algorithm, such as, but not limited to AES, 3DES, or Serpent. Those skilled in the art will appreciate that the hash of the ECP 165 is used the present embodiment of the invention only for size optimization. In principle, the entire ECP 145 itself can be used as well in the present embodiment of the invention. The use of the encrypted data object 320 in the consumer premises 125 is described below.

A reference 330 to a shared secret is appended to the encrypted data object 320 prior to sending the encrypted data object 320 to the consumer premises 125. The shared secret is a secret shared by the crypto-engine 220 and the

consumer device 130. The encrypted data object 320 is typically encrypted using the actual shared secret as an encryption key.

It is appreciated that if the secure metadata object 180 is received at the consumer device 130 comprising the encrypted data object 320 comprising the joined hash of the ECP 165 and metadata 110, then the consumer device 130 will have to decrypt the encrypted data object 320 in order to access and validate the hash of the ECP 165 and metadata 110.

Returning to the discussion of Fig. 1B, reference is now additionally made to Fig. 4, which is a simplified block diagram depicting, at the consumer device 130, an evaluation of the secure metadata object 180 in the system of Figs. 1A and 1B. The secure metadata object 180 is received at the consumer device 130. The following discussion relates to the two embodiments of the secure metadata object 180 described above with reference to Figs. 3A and 3B, specifically: in the first embodiment, the data control object 170 is appended to a cryptographic signature 310; and in the second embodiment, the data control object 170 is appended to the reference 330 to a shared secret. Nonetheless, the embodiments described are not meant to be limiting and are brought in an exemplary fashion.

If the secure metadata object 180 is appended to the cryptographic signature 310, it is inputted into a crypto-engine 420 for validation. Alternatively, If the secure metadata object 180 is appended to the reference 330 to the shared secret, it is inputted into a crypto-engine 420 for decryption. In any event, the decrypted or validated data control object 170 separated to the metadata 110 and the hash of the ECP 165.

A received ECP 445 is input into a hash function 410, the hash function 410 being identical to the hash function 210 (Fig. 2) used during secure stream generation. A hash 165A of the ECP is output by the hash function 410. The hash 165A of the received ECP 445 is compared to the hash of the ECP 165 received in the secure metadata object 180.

If the two hashes, hash 165A of the received ECP 445 and the hash 165 of the ECP received in the secure metadata object 180 do not match, the comparison is determined to have failed. However, if the two hashes, hash 165A

of the received ECP 445 and the hash 165 of the ECP received in the secure metadata object 180 do match, the comparison is determined to have succeeded.

Reference is now made to Figs. 5 - 6, which are simplified flowcharts of preferred methods of operation of the system of Fig. 1. Figs. 5 - 6 are believed to be self-explanatory in light of the above discussion.

It is appreciated that software components of the present invention may, if desired, be implemented in ROM (read only memory) form. The software components may, generally, be implemented in hardware, if desired, using conventional techniques. It is further appreciated that the software components may be instantiated, for example: as a computer program product; on a tangible medium; or as a signal interpretable by an appropriate computer.

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 by the appended claims and equivalents thereof:

What is claimed is:

CLAIMS

1. A method for associating metadata with an encrypted content item, the method comprising:

receiving metadata for association with a content item;

receiving an entitlement control packet (ECP) associated with the content item;

applying a cryptographic hash function to the ECP, thereby generating an ECP hash value;

combining the ECP hash value with the metadata, thereby creating a data control object;

performing a cryptographic operation on the data control object, thereby generating cryptographic integrity data; and

joining the cryptographic integrity data to the data control object after the cryptographic operation,

wherein usage of the content by the recipient is dependent on both a validation of the ECP hash value and a validation of the cryptographic integrity data.

2. The method according to claim 1 and wherein the ECP comprises one of: an entitlement control message (ECM); and a digital rights management (DRM) content license.

3. The method according to either claim 1 or claim 2 and further comprising sending the cryptographically associated data control object joined to the cryptographic integrity data to a recipient.

4. The method according to claim 3 and wherein the sending comprises sending in- band sending.

5. The method according to claim 3 and wherein the sending comprises out-of-band sending.

6. The method according to any of claims 1 - 5 and wherein the metadata comprises service information.

7. The method according to any of claims 1 - 5 and wherein the metadata comprises a usage rule governing the usage of the content item.

8. The method according to any of claims 1 - 7 and wherein the cryptographically associating the combined ECP hash value and the metadata which comprise the data control object comprises digitally signing the data control object, thereby generating a digital signature.

9. The method according to claim 8 and wherein the joined cryptographic integrity data comprises the digital signature.

10. The method according to any of claims 1 - 7 and wherein the cryptographically associating the data control object comprises encrypting the data control object according to a key, the key comprising a secret shared with the recipient.

11. The method according to claim 10 and wherein the joined cryptographic integrity data comprises a reference to the secret shared with the recipient.

12. The method according to any of claims 1 - 11 and wherein the cryptographic hash function comprises one of: SHA-1; SHA-2; and a SHA-3 candidate function.

13. A method for content utilization, the method comprising:

receiving an encrypted content item;

receiving an entitlement control message (ECP) associated with the encrypted content item;

receiving a data control object, the data control object comprising:

an ECP hash value;

metadata; and

cryptographic integrity data;

using the cryptographic integrity data to cryptographically verify the integrity of the data control object;

applying a cryptographic hash function to the received ECP, thereby generating a second ECP hash value;

comparing the second ECP hash value with the received ECP hash value; and

performing metadata processing if the result of the comparing is positive, thereby assuring the metadata cryptographically corresponds to the content item.

14. The method according to claim 13 and wherein the ECP comprises one of: an entitlement control message (ECM); and a digital rights management (DRM) content license.

15. The method according to either claim 13 or claim 14 and wherein the receiving the data control object comprises in-band receiving.

16. The method according to either claim 13 or claim 14 and wherein the receiving the data control object comprises out-of-band receiving.

17. The method according to any of claims 13 - 16 and wherein the metadata comprises service information.

18. The method according to any of claims 13 - 16 and wherein the metadata comprises a usage rule governing the usage of the content item.

19. The method according to any of claims 13 - 18 and wherein the ECP hash value and the metadata comprised in the data control object have been digitally signed.

20. The method according to claim 19 and wherein the cryptographic integrity data comprises the digital signature of the ECP hash value and the metadata.

21. The method according to any of claims 13 - 18 and wherein the ECP hash value and the metadata comprised in the data control object have been encrypted.

22. The method according to claim 21 and wherein the encrypted ECP hash value and the metadata have been encrypted according to a key, the key comprising a secret shared with the sender of the received data control object.

23. The method according to either claim 21 or claim 22 and wherein the cryptographic integrity data comprises a reference to the shared secret.

24. The method according to any of claims 21 - 23 and wherein the using the cryptographic integrity data to cryptographically verify the ECP hash value and the metadata comprises using the key to decrypt the encrypted ECP hash value and metadata.

25. The method according to any of claims 13 - 24 and wherein the cryptographic hash function comprises one of: SHA-1; SHA-2; and SHA-3 candidate function.

26. A system for associating metadata with an encrypted content item, the system comprising:

a metadata receiver operative to receive metadata for association with a content item;

an entitlement control packet (ECP) receiver operative to receive an ECP associated with the content item;

a cryptographic engine operative to apply a cryptographic hash function to the ECP, thereby generating an ECP hash value;

a processor operative to combine the ECP hash value with the metadata, thereby creating a data control object;

a second cryptographic engine which performs a cryptographic operation on the data control object, thereby generating cryptographic integrity data; and

a second processor which joins the cryptographic integrity data to the data control object after the cryptographic operation,

wherein usage of the content by the recipient is dependent on both a validation of the ECP hash value and a validation of the cryptographic integrity data.

27. A system for content utilization, the system comprising:

a content receiver operative to receive an encrypted content item;

an entitlement control packet (ECP) receiver operative to receive an ECP associated with the encrypted content item;

a data control object receiver operative to receive a data control object , the data control object comprising:

an ECP hash value;

metadata; and

cryptographic integrity data;

a cryptographic engine operative to use the cryptographic integrity data to cryptographically verify the integrity of the data control object;

a second cryptographic engine operative to apply a cryptographic hash function to the received ECP, thereby generating a second ECP hash value;

a comparing processor operative to compare the second ECP hash value with the received ECP hash value; and

a metadata processor operative to perform metadata processing if the result of the comparing is positive, thereby assuring the metadata cryptographically corresponds to the content item.

5

FIG. 1A

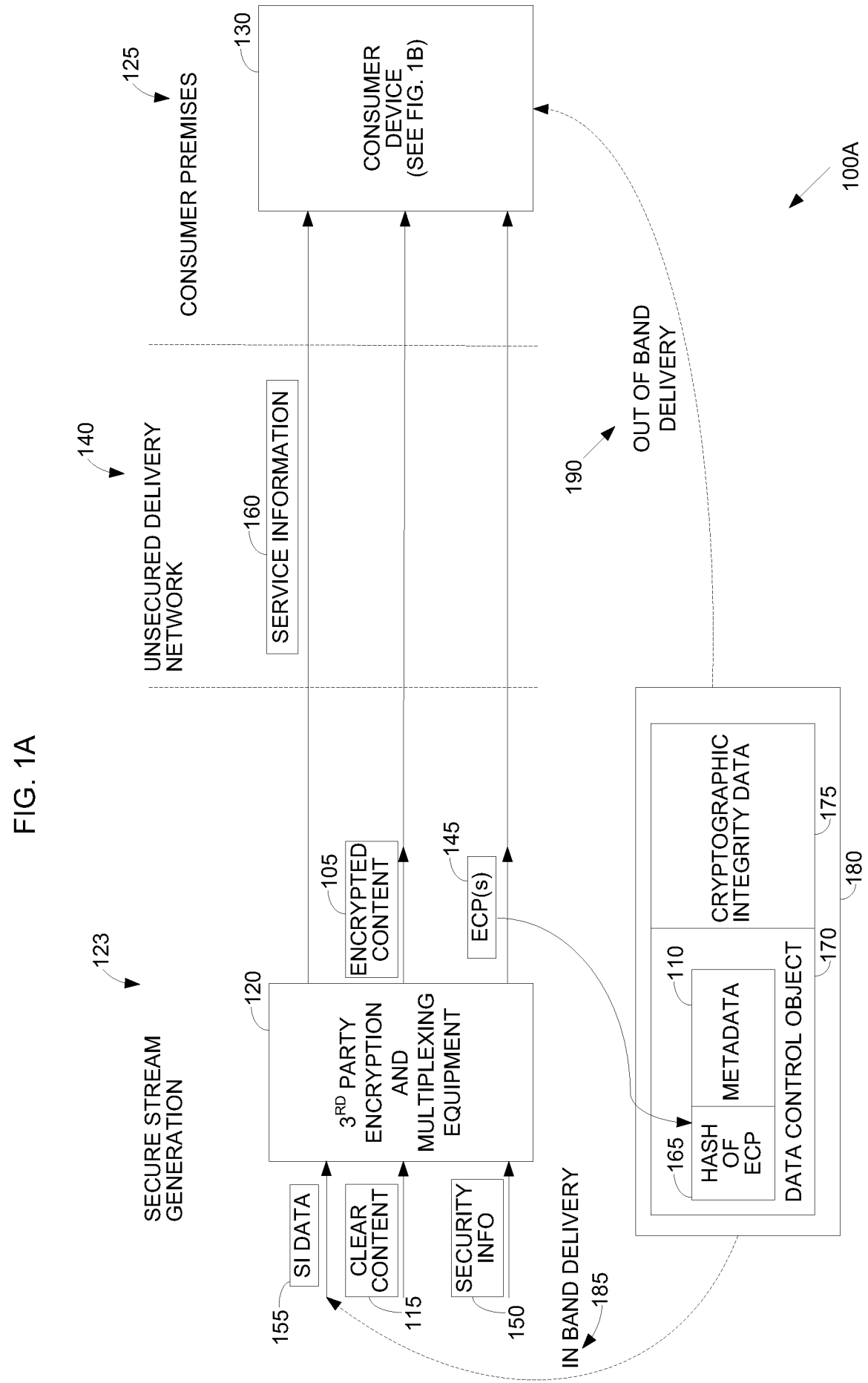

100A
CONSUMER PREMISES
125
CONSUMER DEVICE (SEE FIG. 1B)
130
UNSECURED DELIVERY NETWORK
140
SERVICE INFORMATION
160
OUT OF BAND DELIVERY
190
SECURE STREAM GENERATION
123
3RD PARTY ENCRYPTION AND MULTIPLEXING EQUIPMENT
120
ENCRYPTED CONTENT
105
ECP(s)
145
CRYPTOGRAPHIC INTEGRITY DATA
175
METADATA
110
HASH OF ECP
165
DATA CONTROL OBJECT
170
180
SI DATA
155
CLEAR CONTENT
115
SECURITY INFO
150
IN BAND DELIVERY
185

FIG. 1B

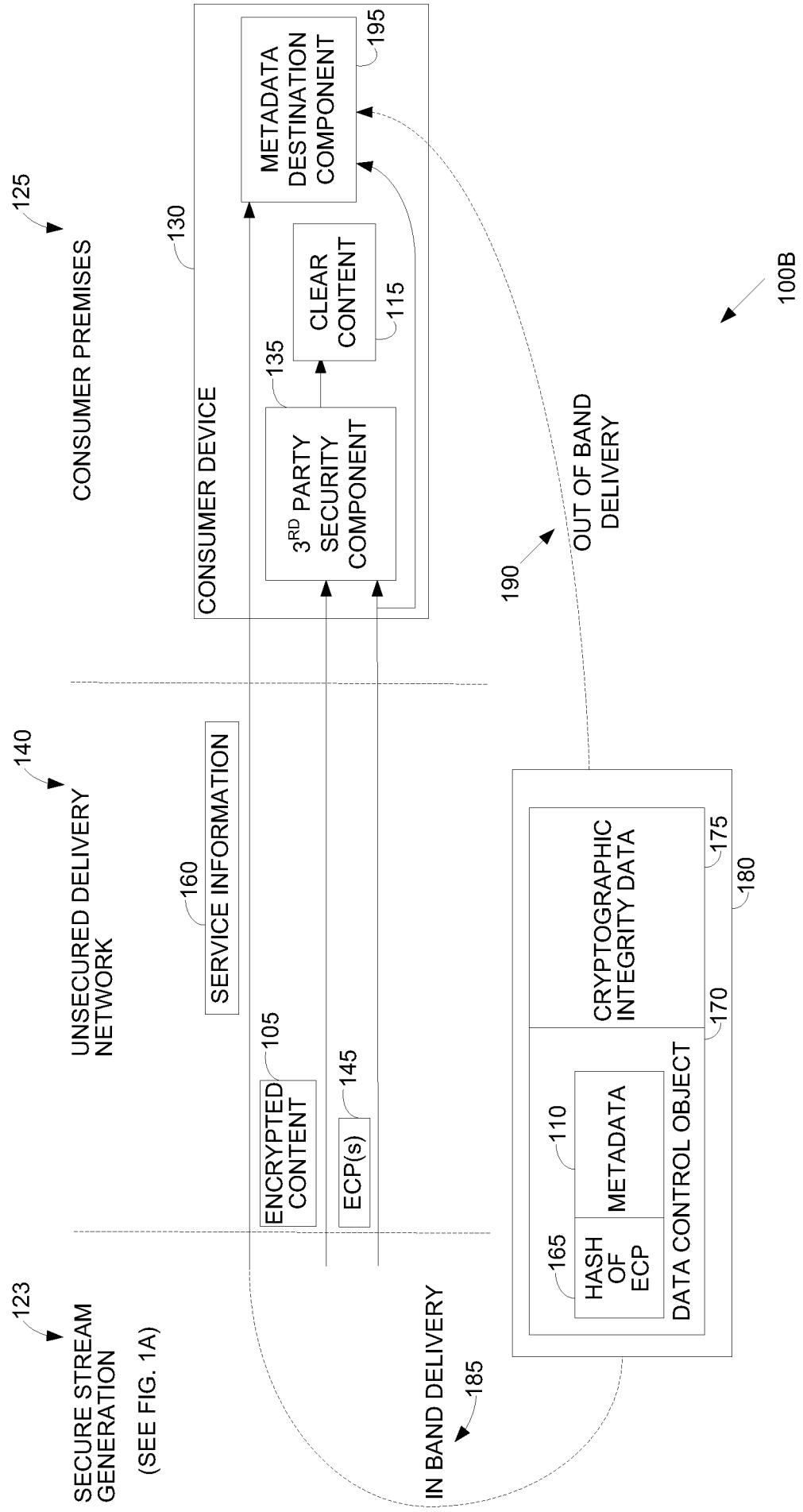

100B
125
CONSUMER PREMISES
130
CONSUMER DEVICE
METADATA DESTINATION COMPONENT
195
CLEAR CONTENT
115
135
3RD PARTY SECURITY COMPONENT
190
OUT OF BAND DELIVERY
140
UNSECURED DELIVERY NETWORK
160
SERVICE INFORMATION
105
ENCRYPTED CONTENT
145
ECP(s)
CRYPTOGRAPHIC INTEGRITY DATA
175
180
170
DATA CONTROL OBJECT
110
METADATA
165
HASH OF ECP
123
SECURE STREAM GENERATION
(SEE FIG. 1A)
IN BAND DELIVERY
185

FIG. 2

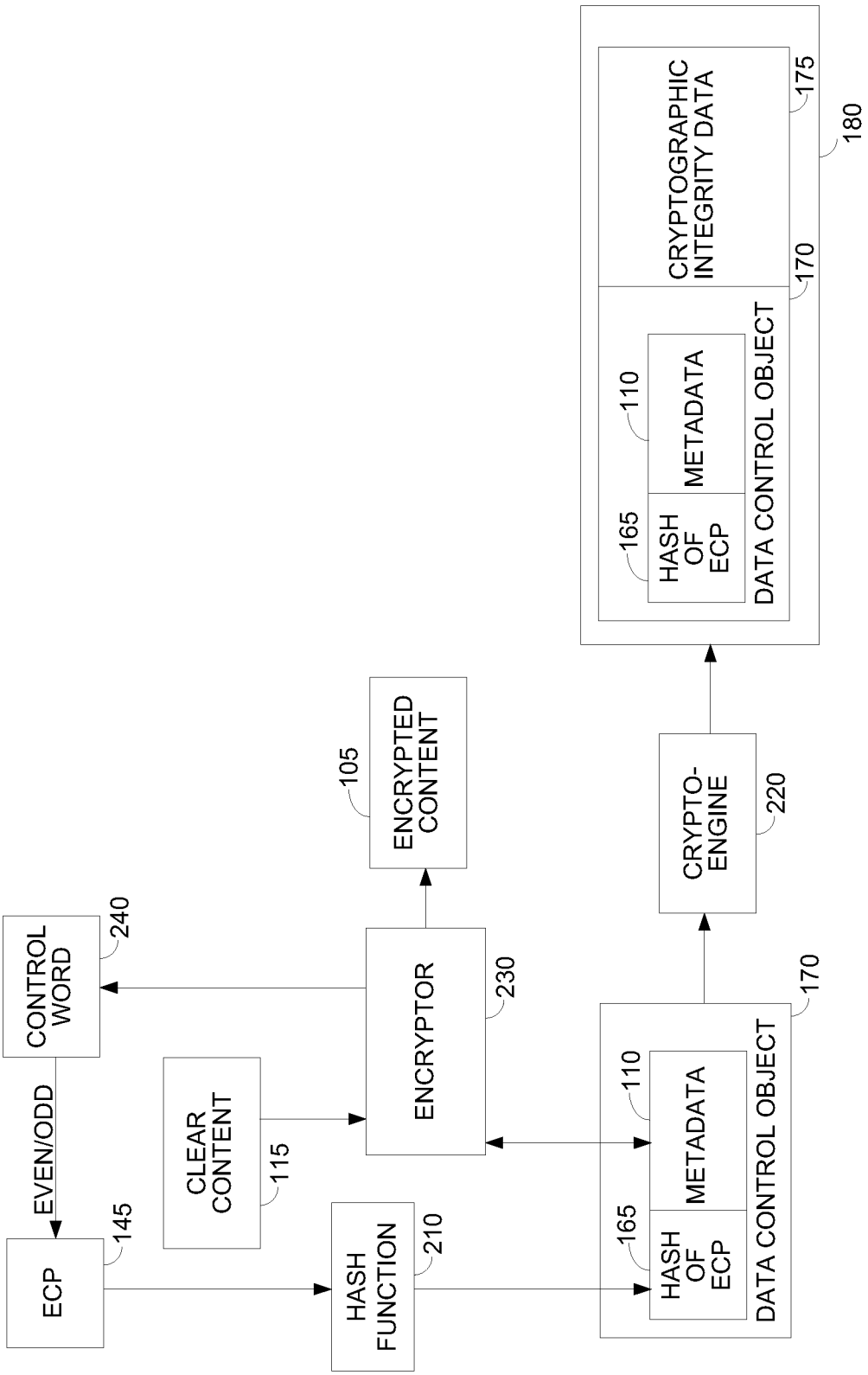

ECP
145
EVEN/ODD
CONTROL WORD
240
CLEAR CONTENT
115
HASH FUNCTION
210
ENCRYPTOR
230
ENCRYPTED CONTENT
105
CRYPTO-ENGINE
220
DATA CONTROL OBJECT
170
HASH OF ECP
165
METADATA
110
CRYPTOGRAPHIC INTEGRITY DATA
175
180

FIG. 3A

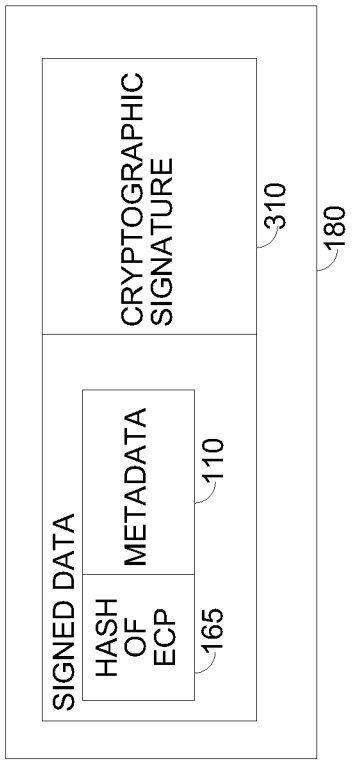

SIGNED DATA
HASH OF ECP
165
METADATA
110
CRYPTOGRAPHIC SIGNATURE
310
180

FIG. 3B

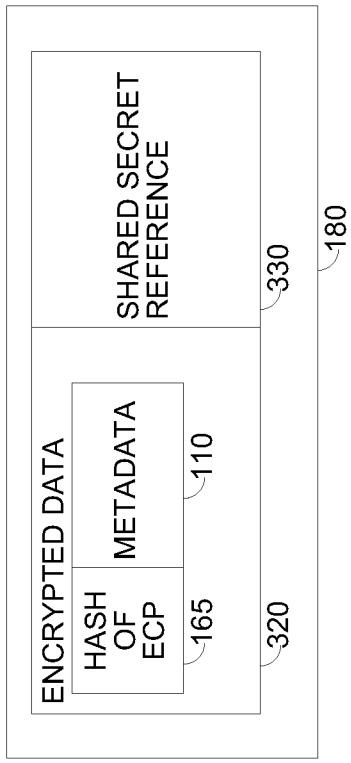

ENCRYPTED DATA
HASH OF ECP
165
METADATA
110
320
SHARED SECRET REFERENCE
330
180

FIG. 4

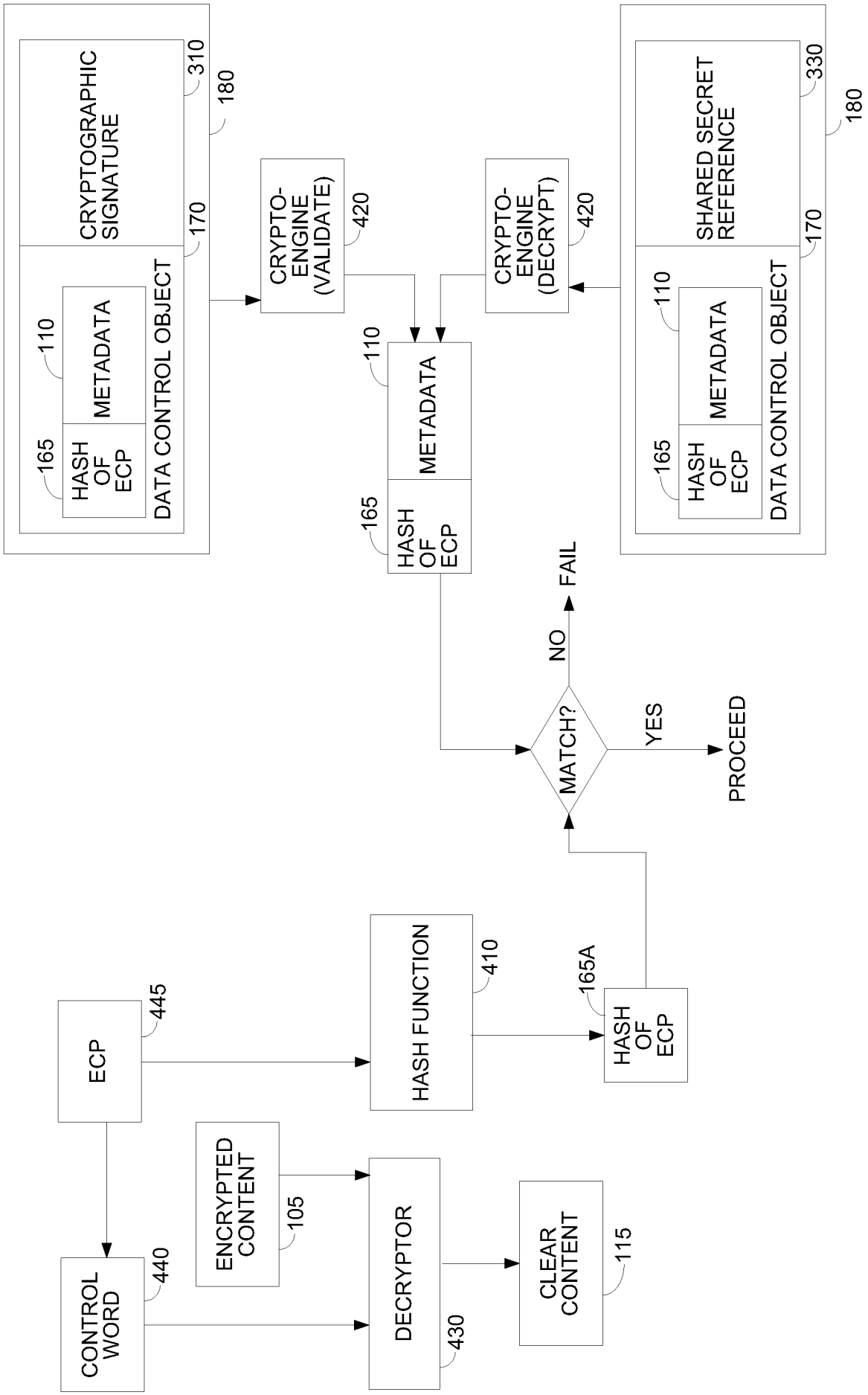

CRYPTOGRAPHIC SIGNATURE
310
180
METADATA
110
HASH OF ECP
165
DATA CONTROL OBJECT
170
CRYPTO-ENGINE (VALIDATE)
420
CRYPTO-ENGINE (DECRYPT)
420
SHARED SECRET REFERENCE
330
180
METADATA
110
HASH OF ECP
165
DATA CONTROL OBJECT
170
NO
FAIL
MATCH?
YES
PROCEED
ECP
445
HASH FUNCTION
410
165A
HASH OF ECP
CONTROL WORD
440
ENCRYPTED CONTENT
105
DECRYPTOR
430
CLEAR CONTENT
115

FIG. 5

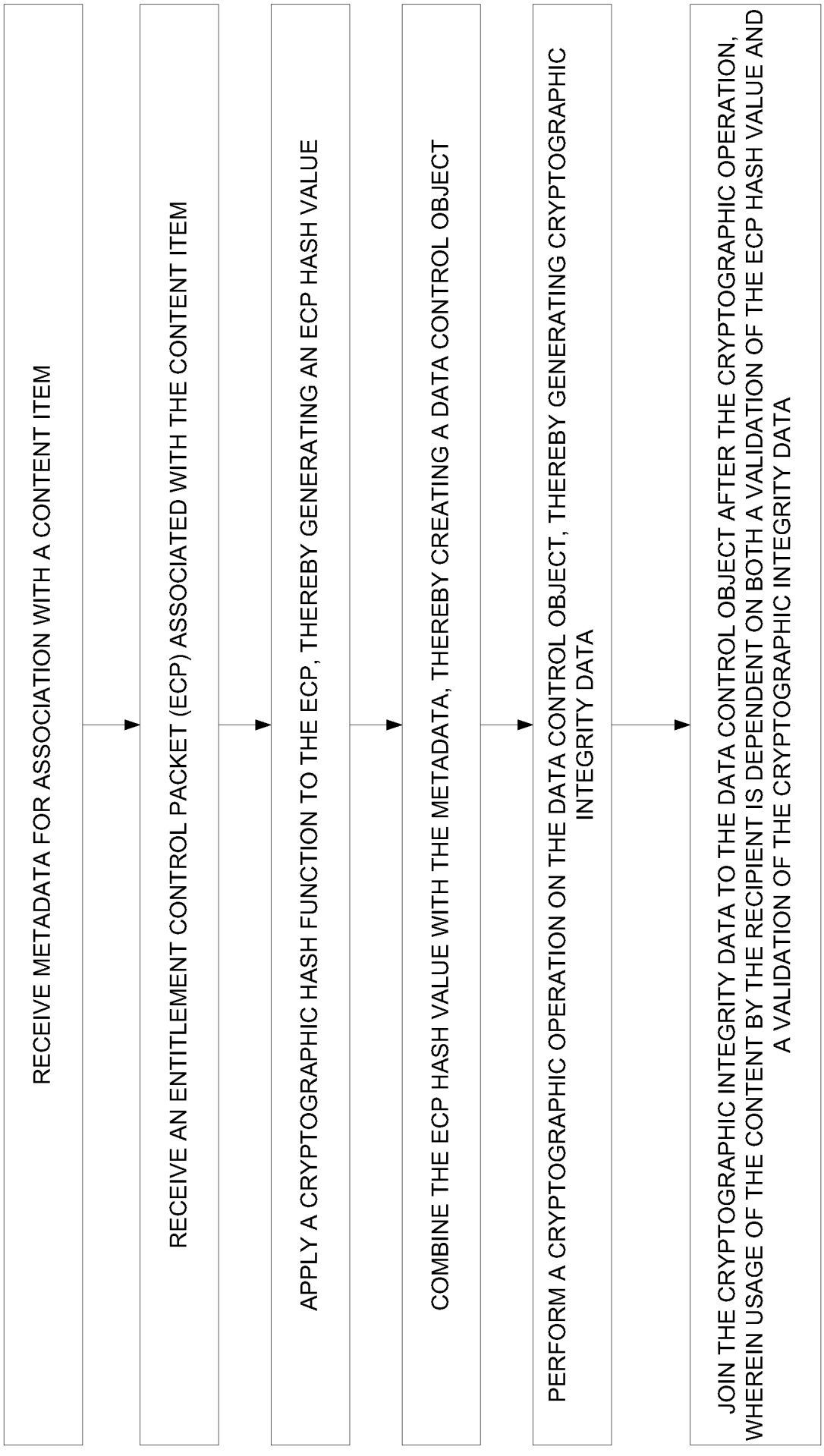
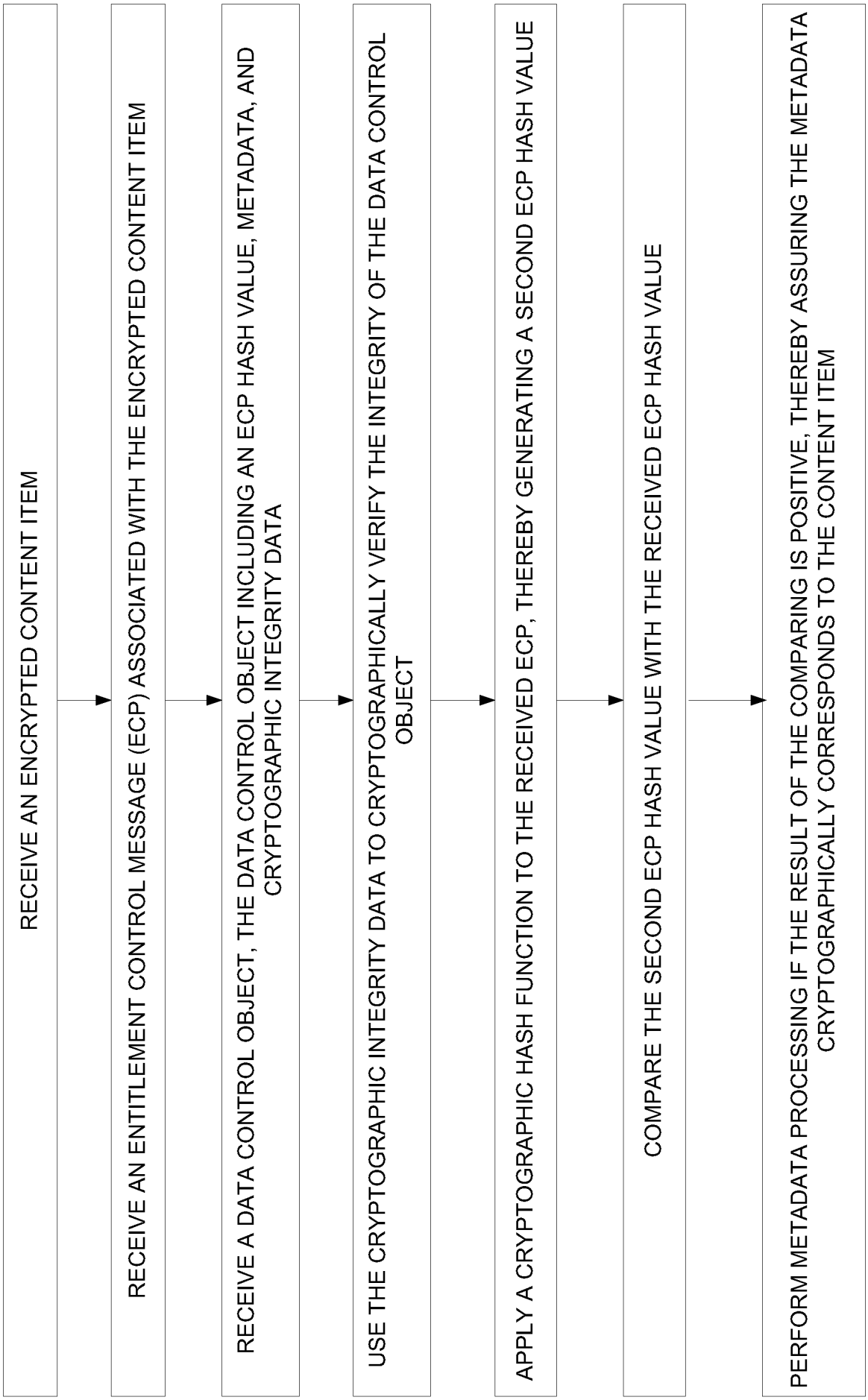

RECEIVE METADATA FOR ASSOCIATION WITH A CONTENT ITEM
RECEIVE AN ENTITLEMENT CONTROL PACKET (ECP) ASSOCIATED WITH THE CONTENT ITEM
APPLY A CRYPTOGRAPHIC HASH FUNCTION TO THE ECP, THEREBY GENERATING AN ECP HASH VALUE
COMBINE THE ECP HASH VALUE WITH THE METADATA, THEREBY CREATING A DATA CONTROL OBJECT
PERFORM A CRYPTOGRAPHIC OPERATION ON THE DATA CONTROL OBJECT, THEREBY GENERATING CRYPTOGRAPHIC INTEGRITY DATA
JOIN THE CRYPTOGRAPHIC INTEGRITY DATA TO THE DATA CONTROL OBJECT AFTER THE CRYPTOGRAPHIC OPERATION, WHEREIN USAGE OF THE CONTENT BY THE RECIPIENT IS DEPENDENT ON BOTH A VALIDATION OF THE ECP HASH VALUE AND A VALIDATION OF THE CRYPTOGRAPHIC INTEGRITY DATA

FIG. 6


RECEIVE AN ENCRYPTED CONTENT ITEM
RECEIVE AN ENTITLEMENT CONTROL MESSAGE (ECP) ASSOCIATED WITH THE ENCRYPTED CONTENT ITEM
RECEIVE A DATA CONTROL OBJECT, THE DATA CONTROL OBJECT INCLUDING AN ECP HASH VALUE, METADATA, AND CRYPTOGRAPHIC INTEGRITY DATA
USE THE CRYPTOGRAPHIC INTEGRITY DATA TO CRYPTOGRAPHICALLY VERIFY THE INTEGRITY OF THE DATA CONTROL OBJECT
APPLY A CRYPTOGRAPHIC HASH FUNCTION TO THE RECEIVED ECP, THEREBY GENERATING A SECOND ECP HASH VALUE
COMPARE THE SECOND ECP HASH VALUE WITH THE RECEIVED ECP HASH VALUE
PERFORM METADATA PROCESSING IF THE RESULT OF THE COMPARING IS POSITIVE, THEREBY ASSURING THE METADATA CRYPTOGRAPHICALLY CORRESPONDS TO THE CONTENT ITEM

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2010/052136

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04N7/167 H04N5/00
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04N

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, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 03/055219 A2 (ERICSSON TELEFON AB L M [SE]) 3 July 2003 (2003-07-03) the whole document page 1, line 10 - line 13 page 1, line 22 - line 26 page 2, line 30 - line 31 page 3, line 4 - line 18 page 3, line 25 - page 5, line 2 page 5, line 9 - page 6, line 2 page 6, line 10 - line 21 page 13, line 15 - line 19 page 14, line 7 - line 22 page 17, line 3 - line 12 page 18, line 7 - line 29 page 19, line 21 - line 22 page 20, line 19 - line 23 figures 1,2,5,7 ----- -/--	1-27

[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
13 October 2010	21/10/2010

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	Fantini, Federico

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2010/052136

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/047952 A1 (VAN DEN HEUVEL SEBASTIAAN ANTO [NL] ET AL) 2 March 2006 (2006-03-02) * abstract paragraph [0001] - paragraph [0004] paragraph [0009] - paragraph [0011] paragraph [0016] - paragraph [0017] paragraph [0019] paragraph [0023] paragraph [0025] - paragraph [0027] paragraph [0039] - paragraph [0043] paragraph [0064] - paragraph [0065] paragraph [0067] - paragraph [0074] paragraph [0078] paragraph [0085] paragraph [0097]	1-27
A	EP 1 732 005 A1 (NEC CORP [JP]; JAPAN BROADCASTING CORP [JP]) 13 December 2006 (2006-12-13) * abstract paragraph [0002] - paragraph [0003] paragraph [0005] paragraph [0007] paragraph [0019] paragraph [0022] - paragraph [0023] paragraph [0025] paragraph [0027] paragraph [0029] paragraph [0047] - paragraph [0049] paragraph [0056] - paragraph [0066] paragraph [0069] - paragraph [0072] paragraph [0084] - paragraph [0087] paragraph [0095] - paragraph [0096] paragraph [0100] figure 4	1-27
A	WO 02/079955 A2 (NDS LTD [GB] NDS LTD [GB]; SHEN ORR CHAIM [IL]; HIBSHOOSH ELIPHAZ [IL]) 10 October 2002 (2002-10-10) page 1, line 28 - page 2, line 2 page 2, line 16 - line 24 page 9, line 25 - line 32 page 10, line 15 - line 27 page 13, line 20 - line 33 page 15, line 10 - line 20 page 20, line 19 - line 23 page 22, line 5 - line 12 page 28, line 4 - line 23 page 29, line 11 - line 29 page 30, line 7 - line 14 page 34, line 32 - page 35, line 18 page 36, line 5 - line 9 figures 1,7	1-27

-/--

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2010/052136

C(Continuation). *DOCUMENTS CONSIDERED TO BE RELEVANT*

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2008/139335 A1 (NDS LTD [GB]; TSURIA YOSSI [IL]; SANDLER LEONID [IL]; BAR-ON GERSHON [) 20 November 2008 (2008-11-20) page 10, line 26 - page 11, line 27 page 16, line 12 - line 20 page 21 - page 24 figures 9,12,13,14	1-27
A	US 2007/124796 A1 (WITTKOTTER ERLAND [US]) 31 May 2007 (2007-05-31) paragraph [0062] - paragraph [0065] paragraph [0069] - paragraph [0071] paragraph [0089] paragraph [0113] paragraph [0117] paragraph [0131] paragraph [0143]	1-27
A	US 2008/086757 A1 (PESTONI FLORIAN [US]) 10 April 2008 (2008-04-10) paragraph [0001] paragraph [0018] - paragraph [0021] paragraph [0023] paragraph [0029] - paragraph [0031] paragraph [0033] paragraph [0036] - paragraph [0037] figure 8	1-27

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2010/052136

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 03055219 A2	03-07-2003	AT 443970 T	15-10-2009
		AU 2002359118 A1	09-07-2003
		CN 1620810 A	25-05-2005
		EP 1454493 A2	08-09-2004
		HK 1078713 A1	25-09-2009
		JP 4472989 B2	02-06-2010
		JP 2005513664 T	12-05-2005
US 2006047952 A1	02-03-2006	AU 2003269360 A1	04-05-2004
		BR 0315403 A	16-08-2005
		CN 1706169 A	07-12-2005
		WO 2004036870 A2	29-04-2004
		JP 2006503367 T	26-01-2006
		KR 20050061545 A	22-06-2005
		US 2010178033 A1	15-07-2010
EP 1732005 A1	13-12-2006	JP 4009634 B2	21-11-2007
		JP 2005285089 A	13-10-2005
		WO 2005086006 A1	15-09-2005
		US 2007277245 A1	29-11-2007
WO 02079955 A2	10-10-2002	AU 2002233609 A2	15-10-2002
		EP 1410140 A2	21-04-2004
		US 2009154697 A1	18-06-2009
		US 2004111613 A1	10-06-2004
WO 2008139335 A1	20-11-2008	NONE	
US 2007124796 A1	31-05-2007	NONE	
US 2008086757 A1	10-04-2008	NONE	