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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 April 2001 (26.04.2001)

PCT

(10) International Publication Number
WO 01/30083 A1

(51) International Patent Classification[7]: H04N 7/167, 7/16, 5/00

(21) International Application Number: PCT/US00/28942

(22) International Filing Date: 19 October 2000 (19.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/160,355 19 October 1999 (19.10.1999) US

(71) Applicant *(for all designated States except US)*: **THOMSON LICENSING S.A.** [FR/FR]; 46, quai Alphonse Le Gallo, F-92648 Boulogne Cedex (FR).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **DUFFIELD, David, Jay** [US/US]; 5459 Fall Creek Road, Indianapolis, IN 46220 (US). **DEISS, Michael, Scott** [US/US]; 1103 Indian Pipe Lane, Zionsville, IN 46007 (US).

(74) Agents: **TRIPOLI, Joseph, S.** et al.; Thomson Multimedia Licensing Inc., P.O. Box 5312, Princeton, NJ 08540 (US).

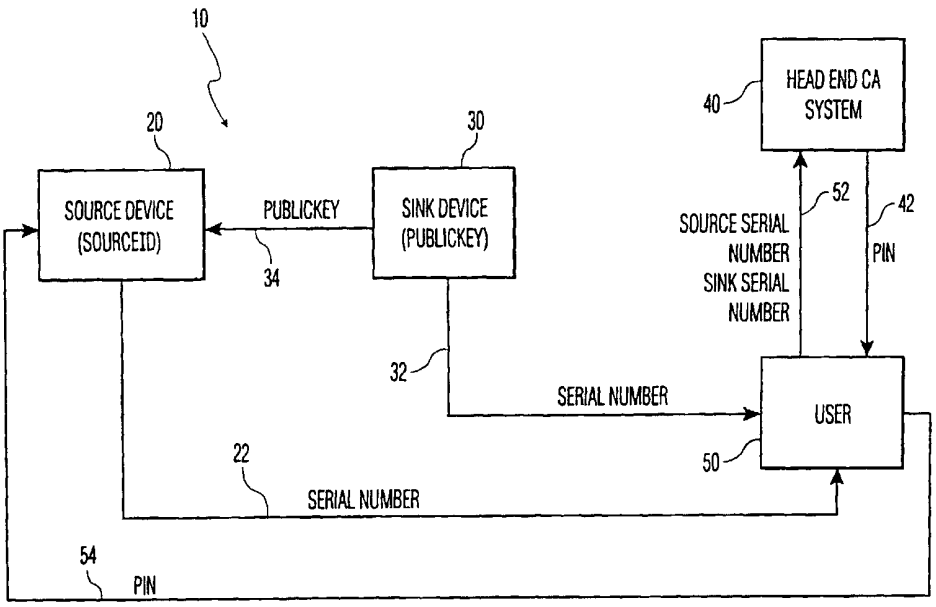
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD OF VERIFYING AUTHORIZATION FOR COMMUNICATING PROTECTED CONTENT



(57) Abstract: A method for verifying that a source device is authorized to communicate otherwise protected content to a sink device in a conditional access system using identification codes.

WO 01/30083 A1

SYSTEM AND METHOD OF VERIFYING AUTHORIZATION FOR COMMUNICATING PROTECTED CONTENT

Field of Invention

The present invention relates generally to digital audio/video transmission systems, and more particularly to a method and system for authenticating access to otherwise protected content.

Background of Invention

Extended Conditional Access (XCA) is a system for protecting digital encoded audio/video (A/V) content during transmission and storage. Under the XCA system, content of economic value is scrambled, or encrypted, to prevent unauthorized access. XCA allows recording of scrambled content, but does not permit descrambling of content that is not legitimate. Legitimate content is that which is an original or otherwise authorized by the copyright owner, for example. Of course, descrambling refers to the process of decryption. Since non-legitimate content is not descrambled, it cannot be viewed.

A distinct characteristic of the XCA architecture is the notion of conditional access (CA) and local protection. CA specifies access to protected content, such as programming. Removable security devices perform security related functions. Content of economic value is delivered using a CA service. For example, digital satellite systems scramble video content and the descrambling keys for mass distribution to their subscribers. Some subscribers may decide to purchase the content in which case they are supplied with the necessary keys to recover/obtain the descrambling key. Those subscribers choosing not to purchase the content are not provided access to these keys. In XCA terminology, this is the process of CA.

XCA systems use a return channel to receive authentication of the local keys and identities that are used for accessing content. This creates a problem in that most devices need to have a return path method of some sort to make this work.

An improved method for authenticating keys and identifiers used to access otherwise protected content in XCA and other systems which exhibit conditional access is desirable.

Summary of Invention

A method for verifying that a source device is authorized to communicate otherwise protected content (e.g. scrambled services) to a sink device in a conditional access system, the

method including: providing substantially unique identifiers associated with the source and sink devices to a validation authority. The validation authority determines an approval code using data associated with the source and sink devices, the data corresponding to the communicated identifiers; and, the source device determines a local code using the data associated with the source and sink devices, and compares at least a portion of the approval code to at least a portion of the local code for verifying the source device is authorized to communicate the content to the sink device.

Brief Description of the Figures

Figure 1 illustrates a system according to one aspect of the present invention; and,

Figure 2 illustrates a system according to a second aspect of the present invention.

Detailed Description of the Invention

According to the present invention, an owner, or user or operator of devices in an XCA system is used as part of a viable return path. A major problem, however, is encountered when utilizing an operator of a device as a return channel. A user cannot be expected to read or enter a 768-bit number accurately. However, large numbers are needed to prevent brute-force cryptanalysis attacks, i.e. trying every possible signature until one works. The problem is verifying that the message, e.g. public key, received is valid. Certificates or signatures used to do this are typically at least 20 bytes in length, and are usually closer to 100 bytes. The signature must have enough possible values to make a brute force attack infeasible. According to the invention, the same goal is accomplished with a much smaller key space by limiting what resources can be used to make a brute force attack.

Figure 1 illustrates a system 10 for authenticating access to otherwise protected content. The system 10 includes a source device 20 having an associated identifier (SOURCEID), a sink device having an associated digital key (PUBLICKEY), a user or operator 50 of the source device 20, and a head end CA, or Trusted Third Party (TTP), system 40.

The source device 20 can take the form of an access device such as a satellite set-top box (STB) or media player, such as digital video cassette (DVHS) player or digital versatile disc (DVD) player, while the sink device can take the form of á digital television (DTV).

According to another aspect of the invention both the source device 20 and sink device 30 have publicly accessible serial numbers.

Generally, in order to protect the transmission of content from source device 20 to sink device 30 such that it cannot be illicitly reproduced or otherwise improperly used, the PUBLICKEY of sink device 30 is communicated to source device 20. Content provided to by source device 20 is scrambled using the PUBLICKEY of sink device 30, and transmitted to sink device 30 in scrambled form. The sink device 30 uses the corresponding private key, to unscramble the content and to enable its proper display by the sink device 30. It should also be realized that the above may be accomplished using a two stage process wherein the content is scrambled using a symmetric algorithm, and the control word for this scrambling is sent using the PUBLICKEY.

The PUBLICKEY and SOURCEID of the sink and source devices 30, 20, respectively, are determined by the TTP using the serial numbers of these devices. The determined PUBLICKEY and SOURCEID are then separately used by the devices 20, 30 and TTP to authenticate that the devices 20, 30 may operate in combination to access the content.

The user 50 obtains the serial numbers from the respective source and sink devices 20, 30 (for example, by reading them off the devices) and calls the head end CA system to enable use of the source and sink devices 20, 30 in combination. The user 50 provides these serial numbers to the head end CA system 40 as communication 52. These serial numbers can be provided in a voice communication or electronically, or acoustically for example. The Head End CA system 40 has access to a database that converts the provided serial numbers to SOURCEID and PUBLICKEY data. Hence, the head end CA system 40 can identify the SOURCEID and PUBLICKEY data of the source device 20 and sink device 30 from these communicated serial numbers, e.g. by using a lookup. According to another aspect of the present invention, it is important that the relationship between the serial numbers and SOURCEID is not public, and not readily ascertainable.

In Figure 1, the head end CA system 40 computes a hash code of these two values, e.g. the SOURCEID and PUBLICKEY as an approval hash calculation, and provides it to the user 50 as a Personal Identification Number (PIN) (illustrated as communication 42). The user 50 then enters this PIN into the source device 20 (illustrated as communication 54), which has computed the same hash, e.g., as a local hash calculation using the SOURCEID resident in the

source device 20 and PUBLICKEY provided by the sink device 30 (illustrated as communication 34). If the PIN matches the hash, then the source device 20 recognizes that the PUBLICKEY provided in communication 34 from the sink device 30 is valid for use, that the head end CA system 40 has been given this key, and that the head end CA system 40 approves it for use such that the source device 20 and sink device 30 are authorized to operate in combination with one another.

According to another aspect of the present invention, and as set forth, either the SOURCEID and/or the algorithm for computing the hash is kept secret. As will be understood by those possessing an ordinary skill in the pertinent art, the fact that a potential pirate does not have this input to the hash function effectively prevents a brute force attack with a more powerful computer.

According to another aspect of the present invention, the PIN code has a large enough space that an exhaustive search for a valid signature takes prohibitively long. One way of accomplishing this is to have the source device 20 take a significant time to approve the PIN code, either with a complex calculation, or with a waiting period after the computation, for example. A suggested value for this application, e.g., copy protection for a home A/V network, could be a 9 or 10 digit PIN, and a compute time of one second. This would force an average exhaustive search time of $5x10^8$ or $5x10^9$seconds, or approximately 16 or 160 years.

According to an alternative aspect of the present invention, another input to the hash function can be a title code or media, such as a tape or DVD, serial number. This allows for individual titles or tapes to be approved or disapproved for use, for example. One can accomplish significant time savings by storing the serial numbers for a given user 50 in the head end CA system 40 so that the user 50 does not have to provide them for each transaction.

According to another alternative aspect of the present invention, another input to the hash function can be indicative of total running time or elapsed time since the first approval. This allows the approval to automatically expire after a set time or usage. If an extra time code is needed, this can be signaled from the source device 20 to the user 50. The time codes should be sufficiently random such that the user 50 cannot effectively guess or otherwise predict what the next time code will be. If the user 50 were capable of doing this, he could call in beforehand, and essentially pre-authorize his system by getting the PIN codes before they were required.

According to yet another alternative aspect of the present invention, another PIN code based system is based on balkanizing or dividing the key space of local networks into smaller segments without going to the security extreme of using unique per-network keys.

Figure 2 illustrates another system 100 suitable for authenticating keys and identifiers used to access otherwise protected content. The system 100 includes a source device 120 having an associated SOURCEID, a sink device 130 having an associated PUBLICKEY, a user, or operator 150 of the source device 120 and a head end CA system 140.

Sink devices can be made with a relatively small number of private keys, 10,000 for example. The user 150 reads the serial numbers of the sink device 130 and source device 120 (illustrated as communication 132, 122 respectively). The user 150 then calls into the head end CA system 140, provides the serial number of the sink device 130 and source device 120, and receives the PIN code for this sink device 130 (illustrated as communications 152, 142). The PIN code can be determined via a lookup table or appropriate calculation. The user 150 then enters this PIN code into the source device 120 (illustrated as communication 154), and the source device 120 indexes to the correct public key to use for the sink device 130 using a table of public keys 160.

The table of public keys 160 is large compared to the storage of the source device 120 itself. Table 160 is encrypted, and stored at the beginning of prerecorded media (for example, tapes). This provides an easy mechanism for obtaining the public key (PUBLICKEY) when needed, as any prerecorded tape may be used to initialize the network. After that, the system 100 will work on it's own, as the source device 120 will remember the proper key or use with the sink device 130.

Prerecorded media such as tapes are conventionally encrypted with some other, stronger encryption system. In the present invention, only the digital link from source device 120 to sink device 130 is encrypted with this weaker local key. While the local key is not unique to this network, it will be very difficult to profitably make copies of material if 10,000 different versions of the tape are required for each title.

In the event that one of the 10,000 local keys of the above-described system 100 becomes known, "pirate" users might continually use the same PIN code to allow content to be played using any source device 120. System 100 may be improved by making the PIN

code a hash function of the SOURCEID, as well as the index into the table of public keys 160. This forces the user 50 to obtain a unique PIN for each source device 120. If an overwhelming number of requests come in for a given public key in the index table 160, then that can be used as a signal that a private key has been compromised.

CLAIMS

1. A method for verifying that a source device is authorized to communicate protected content to a sink device comprising:

receiving at said source device an approval code associated with said source and sink devices;

determining, in said source device, a local code using data associated with said source and sink devices; and

comparing at least a portion of said approval code to at least a portion of said local code.

2. The method according to claim 1, wherein said approval code is determined based on a hash calculation using identifiers uniquely associated with said source and sink devices and wherein said local code is determined based on a hash calculation using data from said sink device and a source identifier prestored in said source device.

3. The method according to claim 2, wherein said data associated with said source device for determining said local code is not public information and wherein said data associated with said sink device for determining said local code is public information.

4. The method of Claim 2, wherein said identifiers are serial numbers or other identification codes accessible to a user, and wherein said data from said sink device used in said hash calculation is a public key.

5. A method for verifying that a source device is authorized to communicate protected content to a sink device comprising:

providing substantially unique identifiers associated with said source and sink devices to a validation authority;

receiving from said validation authority an approval code, said approval code using data corresponding to said identifiers;

determining, in said source device, a local code using said data associated with said source and sink devices, and

comparing at least a portion of said approval code to at least a portion of said local code.

6. The method of Claim 5, further comprising said validation authority providing said at least portion of said approval code to a user, and said user providing said at least portion of said approval code to said source device.

7. The method of Claim 5, wherein said substantially unique identifiers are provided to said validation authority by said user.

8. The method of Claim 5, wherein said source device is selected from one of an access device and a media player and wherein said sink device is a digital television.

9. The method of Claim 5, wherein said data associated with said source device is secured so as not to be readily ascertainable by said user.

10. The method of Claim 5, wherein said data associated with said source and sink devices comprises a unique identification indicative of said source device and a public encryption key associated with said sink device.

11. The method of Claim 10, wherein said unique identification indicative of said source device is secured from a user of said source device.

12. The method of Claim 1, further comprising said source device communicating whether said source device is authorized to provide said content to said sink device to a user, and intentionally delaying communicating whether or not said compared approval code and local code are consistent.

13. A method for authenticating at least one security key and at least one identifier used to access protected content, said method comprising:

receiving at a first device a plurality of security keys with said content;

receiving said identifier at said first device to be used to provide said content to a second device, said identifier being associated with said second device;

selecting one of said plurality of security keys using said first device; and,

providing said content to said second device using said first device and selected security key.

14. The method according to claim 13, further comprising providing a serial identification indicative of said second device for accessing said content to a validation authority.

15. The method according to claim 14, further comprising determining an identifier associated with said second device using said serial identification.

16. The method of Claim 13, wherein said plurality of security codes are indexed in a table of keys and said identifier is the index of said select key in the table of keys and a result of a hash function of said identifier.

17. A method for verifying that a source device having an associated substantially unique identification and serial number and a sink device having a substantially unique key and serial number should have access to content by using a validation authority, wherein said unique identification is secured from access by a user of said source device, said method comprising:

providing said serial numbers to said validation authority;

said validation authority determining said substantially unique identifier using said serial numbers; and, if said access to said content is authorized,

said validation authority determining an authorization identifier using said substantially unique identifier;

said source device determining a local identifier using said substantially unique identifier; and,

verifying said source device and sink device should have access to content if said authorization identifier and local identifier correspond to one another.

18. The method of Claim 17, further comprising said validation authority providing said at least portion of said authorization identification to a user, and said user providing said authorization identification to said source device.

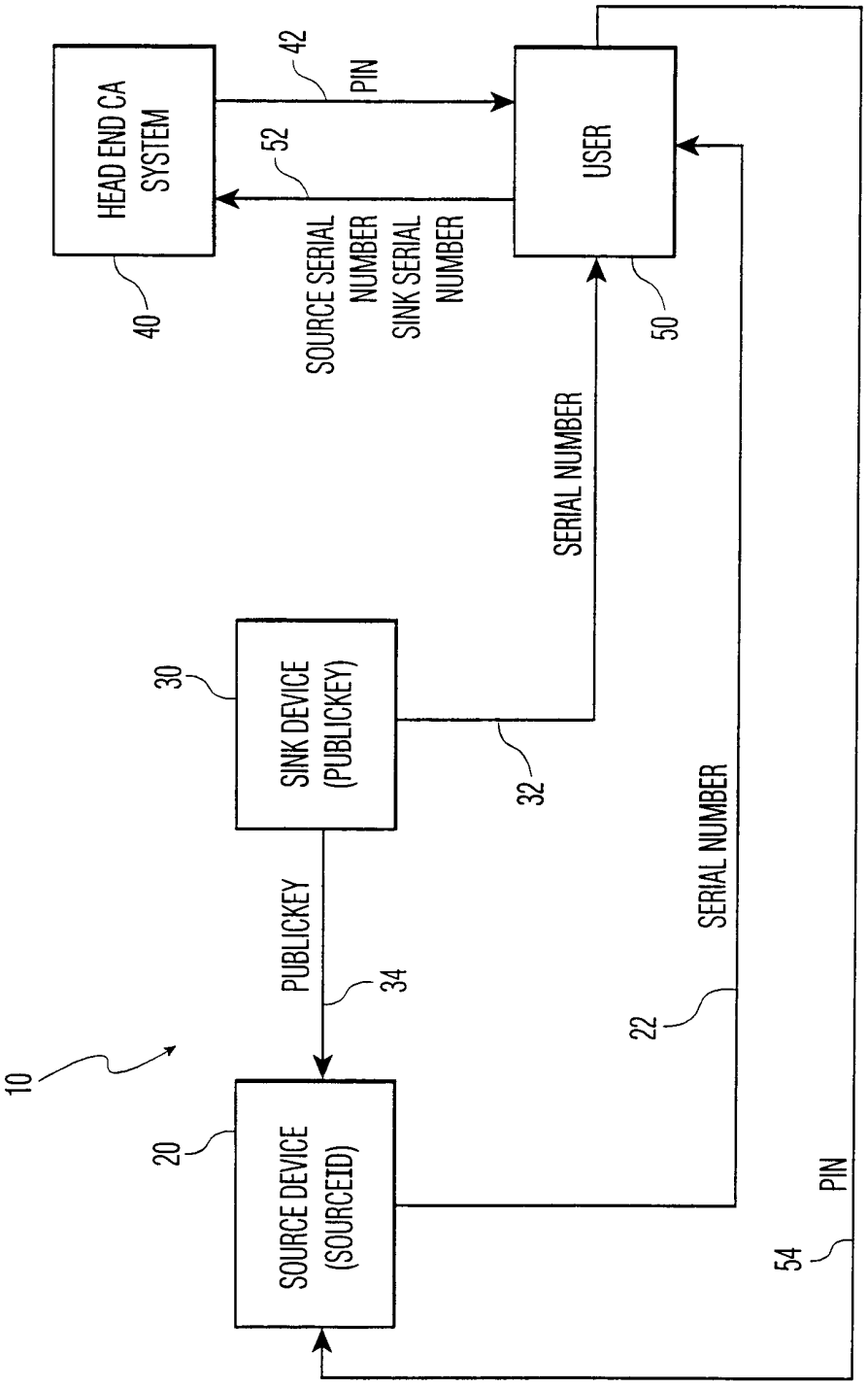

HEAD END CA SYSTEM
40
42
PIN
52
SOURCE SERIAL NUMBER
SINK SERIAL NUMBER
USER
50
SERIAL NUMBER
30
SINK DEVICE (PUBLICKEY)
32
PUBLICKEY
34
SERIAL NUMBER
22
10
20
SOURCE DEVICE (SOURCEID)
54
PIN

FIG. 1

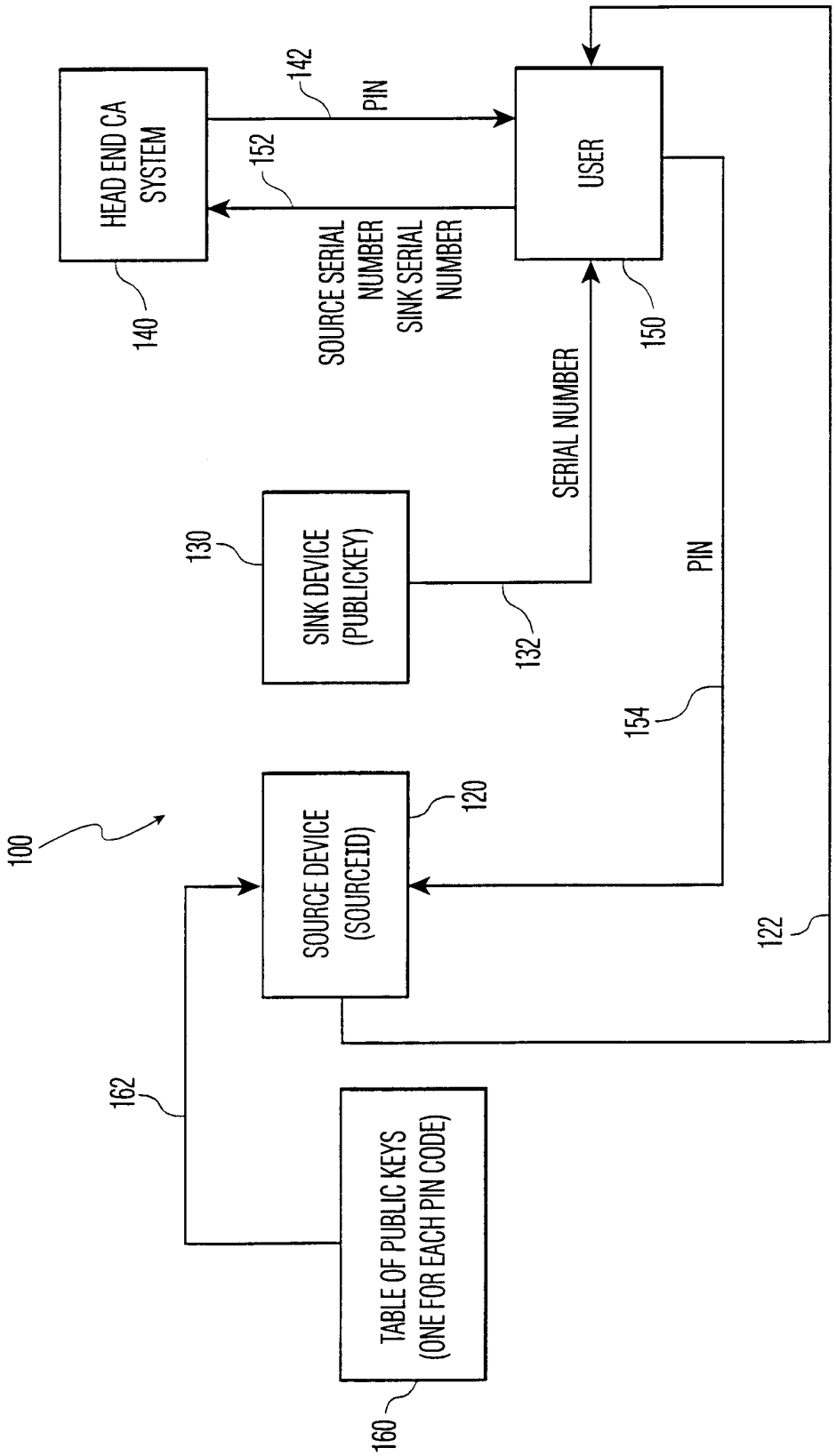

HEAD END CA SYSTEM
140
142
PIN
152
SOURCE SERIAL NUMBER
SINK SERIAL NUMBER
USER
150
SERIAL NUMBER
130
SINK DEVICE (PUBLICKEY)
132
PIN
154
100
SOURCE DEVICE (SOURCEID)
120
122
162
TABLE OF PUBLIC KEYS (ONE FOR EACH PIN CODE)
160

FIG. 2

INTERNATIONAL SEARCH REPORT

Inter ›nal Application No
PCT/US 00/28942

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/167 H04N7/16 H04N5/00

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)
IPC 7 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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 99 22372 A (SONY ELECTRONICS INC) 6 May 1999 (1999-05-06) abstract; figures 5A,7 page 4	1,5,13, 17
A	WO 99 07150 A (SCIENTIFIC ATLANTA) 11 February 1999 (1999-02-11) page 8, line 8 - line 25 page 10, line 19 - line 24 page 11, line 11 - line 14 page 52, line 27 - line 29	1,5,13, 17
A	US 5 420 866 A (WASILEWSKI ANTHONY J) 30 May 1995 (1995-05-30) column 1, line 14 -column 7, line 7 figures 1-8	1,5,13, 17

-/--

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

[X] Patent family members are listed in 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
5 February 2001	12/02/2001

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, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Tito Martins, J

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter onal Application No
PCT/US 00/28942

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 858 184 A (NDS LTD) 12 August 1998 (1998-08-12) column 1, line 12 -column 7, line 20 figures 1-5	1,5,13, 17
A	"FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM" , EBU REVIEW- TECHNICAL,BE,EUROPEAN BROADCASTING UNION. BRUSSELS, NR. 266, PAGE(S) 64-77 XP000559450 ISSN: 0251-0936 the whole document	1,5,13, 17
P,A	WO 00 56068 A (THOMSON LICENSING S A ;DEISS MICHAEL SCOTT (US); ESKICIOGLU AHMET) 21 September 2000 (2000-09-21) page 2, line 14-29 page 4, line 4 -page 5, line 14 figures 1-8	1,5,13, 17

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte onal Application No
PCT/US 00/28942

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9922372 A	06-05-1999	AU 1103599 A	17-05-1999
		EP 1012840 A	28-06-2000
WO 9907150 A	11-02-1999	AU 1581699 A	08-03-1999
		AU 8670598 A	22-02-1999
		AU 8679798 A	22-02-1999
		AU 8679898 A	22-02-1999
		AU 8764298 A	22-02-1999
		AU 8823398 A	22-02-1999
		AU 8823698 A	22-02-1999
		EP 1010323 A	21-06-2000
		EP 1010324 A	21-06-2000
		EP 1010325 A	21-06-2000
		EP 1013091 A	28-06-2000
		EP 1000508 A	17-05-2000
		EP 1000509 A	17-05-2000
		EP 1000511 A	17-05-2000
		WO 9907145 A	11-02-1999
		WO 9907146 A	11-02-1999
		WO 9907147 A	11-02-1999
		WO 9907148 A	11-02-1999
		WO 9907149 A	11-02-1999
		WO 9909743 A	25-02-1999
		US 6105134 A	15-08-2000
US 5420866 A	30-05-1995	AU 687844 B	05-03-1998
		AU 7220994 A	17-10-1995
		CA 2186368 A,C	05-10-1995
		JP 2940639 B	25-08-1999
		JP 9511369 T	11-11-1997
		WO 9526597 A	05-10-1995
EP 0858184 A	12-08-1998	IL 120174 A	28-10-1999
		GB 2322030 A,B	12-08-1998
WO 0056068 A	21-09-2000	AU 3629100 A	04-10-2000