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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 May 2003 (08.05.2003)

PCT

(10) International Publication Number
WO 03/039067 A1

(51) International Patent Classification⁷: H04L 9/18

(21) International Application Number: PCT/SE02/01830

(22) International Filing Date: 9 October 2002 (09.10.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0103623-5 1 November 2001 (01.11.2001) SE

(71) Applicant *(for all designated States except US)*: **KREATEL COMMUNICATIONS AB** [SE/SE]; Teknikringen 4C, S-58330 Linköping (SE).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **CARLSSON, Henrik** [SE/SE]; Vasavägen 30, S-58233 Linköping (SE). **HELSTAD, Dag** [SE/SE]; Hjälmgatan 16B, S-58217 Linköping (SE). **ÖSTERLIND, Christer** [SE/SE]; Spjutvägen 13, S-19532 Märsta (SE). **SPARR, Tomas** [SE/SE]; Handskerydsvägen 9A, S-57140 Nässjö (SE).

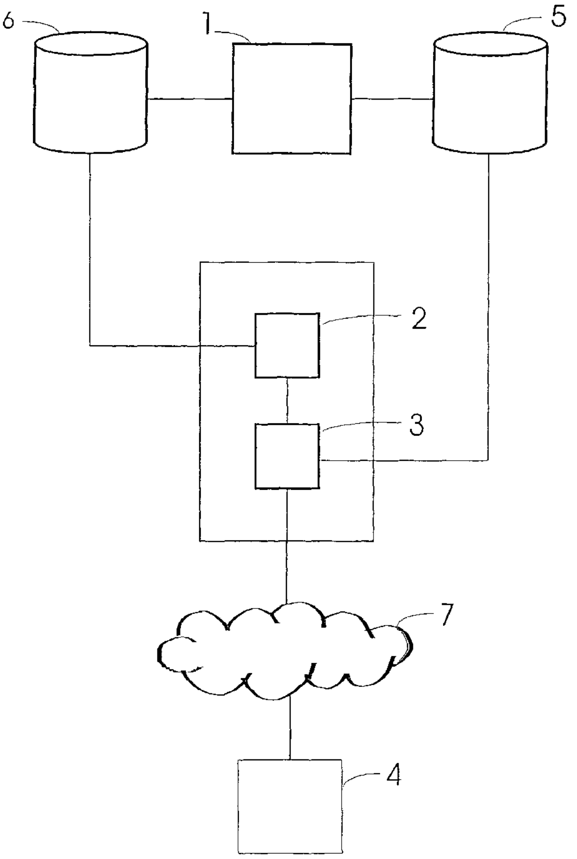
(74) Agent: **WILLQUIST & PARTNERS PATENTBYRÅ AB**; Platensgatan 9C, S-58220 Linköping (SE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, 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, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR ENCRYPTING MEDIA STREAM PACKETS EITHER DYNAMICALLY OR STATICALLY BY A PROXY AND A PRE-PROCESSOR



(57) Abstract: Method and apparatus for encrypting a media stream sent from a server (2) via an encryption proxy (3) to a client (4), connected to the encryption proxy (3) over a network (7), where packets of the media stream are either statically encrypted by a pre-processor (1) or dynamically encrypted by the encryption proxy (3). The pre-processor (1) selects which packets of the media stream that are to be statically encrypted and which packets that are to be dynamically encrypted as defined in an encryption scheme (5).

Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

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.

METHOD AND APPARATUS FOR ENCRYPTING MEDIA STREAM PACKETS EITHER DYNAMICALLY OR STATICALLY BY A PROXY AND A PRE-PROCESSOR

The present invention relates to a method defined in the preamble of claim 1.

The present invention also relates to an apparatus defined in the preamble of claim 5.

In order to send a media stream, such as video or audio, from a server over a network to a client, it is necessary for the content owner to protect the content from being accessed, re-distributed, manipulated or illegally copied.

A commonly used encryption scheme for conditional access in digital satellite and terrestrial broadcasting is Digital Video Broadcasting (DVB-CA). DVB is designed to work in simplex networks. Scrambled media stream content is multiplexed with a key distribution stream. The access decision is distributed to clients connected in the network. Frequent attacks of the system based on reverse engineering and information leaks from insiders have forced the content distributors to refine their protection in steps. The drawback is the difficulties in handling backward comparability when upgrading systems that has been compromised. The relative complexity of distribution content keys in a simplex network and the access processing taking place at the client makes the system very resource (CPU) demanding. The decryption uses a separate processing unit on a smart card, which makes the decryption expensive.

There is, therefore, a need for an improved method and apparatus, which encrypts a media stream sent over a network.

One object of the present invention is to provide such an improved method and apparatus, which has configurable requirements on CPU utilisation on both the client and the server, and which is built on open standards.

In accordance with the preferred embodiment of the present invention, this object is accomplished by providing a method and apparatus as defined in the characterising parts of the independent claims 1 and 5.

The details of the preferred embodiment of the invention are set forth in the accompanying drawings and the description below. Other features and advantages of the invention will become apparent from the description, the drawings and the claims.

In the drawings:

Fig 1 is a block diagram of an encryption system

Fig 2 is a flowchart showing the steps performed when the media stream is encrypted.

In a preferred embodiment of the present invention, the media stream is a Moving Picture Experts Group Transport Stream (MPEG-2 TS), which refers to the family of digital video compression standards and file formats developed by this group. MPEG-2 TS achieves high compression rate by for most of the frames storing only the changes from one frame to another instead of each entire frame. The person skilled in the art understands, however, that the invention is applicable on other media streams as well, such as MPEG-1 Audio Layer-3 (MP3) and MPEG-2 Packet Stream (MPEG-2 PS).

In fig 1 a content protection pre-processor is represented by 1. The pre-processor 1 is connected to a database 6 from which it gets the MPEG-2 TS to process. A server 2 connected to an encryption proxy 3 gets the pre-processed MPEG-2 TS from the database 6. The pre-processor 1 and the encryption proxy 3 are both connected to an encryption scheme 5, from which they get information concerning the encryption. A client 4 communicates with the encryption proxy 3 over a network 7, e.g. Internet. Fig 1 illustrates one example of the architecture of the encryption system. The person skilled in the art understands, however, that any other constellation of the parts in the system is possible.

In order to accomplish a method that has small requirements on CPU utilisation on both the client 4 and the server 2, some TS packets are statically, e.g. on disk, encrypted and some are dynamically, real time, encrypted.

The static encryption can e.g. be done by the content owner before delivering the content to operators, which reduces the risk of “in-house theft” at the operator site.

The pre-processor 1 analyses the MPEG-2 TS and selects the TS packets which are to be statically encrypted, encrypts these and marks at the same time the TS packets which are to be dynamically encrypted. This processing is performed only once per title, e.g. once per film when the media stream is a video stream and once per audio track when the media stream is an audio stream. The encryption proxy 3 encrypts the TS packages marked by the pre-processor 1 for dynamic encryption. The dynamic encryption is, however, performed once per session. This means that even if the static encryption is cracked, watching e.g. a movie is made impossible by the dynamic encryption.

Which packets that are to be statically encrypted and which are to be dynamically encrypted is specified in the encryption scheme 5. The encryption scheme 5 contains all necessary information the pre-processor 1 and the encryption proxy 3 need in order to perform the encryption of the media stream. The content owner supplies the information stored in the encryption scheme 5. Typical information in the encryption scheme 5 is what and when to encrypt and what algorithm to use.

The combination of the pre-processor 1 and the encryption proxy 3 makes the inventive system flexible, with full control over what to encrypt and when (static or dynamic). The system can e.g. be optimised for a low CPU usage, high security or low cost etc. The flexibility of the system lead to that different kinds of encryption algorithms may be used, in which all packets, some packets or no packets at all can be encrypted.

Since the pre-processor 1 marks the packets (a sub set of the total number of packets) to encrypt dynamically meaning that not all encryption need to be done in real time, there are small requirements on CPU utilisation on the host running the encryption proxy 3. The requirements on CPU are configurable through the encryption scheme 5.

The server 2 stores the pre-processed MPEG-2 TS and creates indices. In the preferred embodiment of the invention the server 2 is a Video-on-Demand (VoD) server. VoD gives a user the possibility to order a movie or other program content for immediate viewing on e.g. the TV. The client 4, e.g. a Set-Top-Box (STB) client, comprises a web browser allowing the user to choose e.g. a movie. The client 4 then orders the chosen movie from the VoD server 2 via the encryption proxy 3. Since the encryption proxy 3 handles all communication with the client, the inventive system is independent of the server.

The preferred embodiment of the inventive method is based on the MPEG-2 standard for scrambling/encryption of TS packet content. The type of encryption used is fully configurable and a matter of agreement between the client 4 and the encryption proxy 3. The client 4 and the encryption proxy 3 negotiate about a set of encryption algorithms to use among multiple encryption algorithms. A two-bit bit field "transport scrambling control" in the TS header is used to indicate which kind of encryption that is used within the set of encryption algorithms according to the agreement between the client 4 and the encryption proxy 3. Multiple sets of mappings between transport scrambling control values and encryption algorithms may be supported. The client 4 gets the information of which set to use from the (URL) accessed or from the ticket received when ordering the VoD.

The inventive method is applicable on all kinds of decryption key distributions. The client 4 may negotiate with the encryption proxy 3 about what key distribution to use and how many packets which are to be dynamically encrypted by the encryption proxy 3. The client 4 may e.g. request encryption of only a subset of the packets marked for dynamic encryption due to small CPU resources. The encryption proxy 3 can, however, deny such a request for less encryption. The negotiation between the client 4 and the encryption proxy 3 may be encrypted in order to obtain a high security level. Another alternative is to use an encryption algorithm in the encryption scheme 5 that is adapted to certain kinds of clients, e.g. encrypt as few packets as possible (usually around 1/10) in order to reduce the CPU load of the client.

A preferred embodiment of the present invention is shown in fig 2 and the procedure for encrypting an MPEG-2 transport stream is as follows:

1. The pre-processor 1 analyses the MPEG-2 TS 6 and selects the TS packets for static and dynamic encryption according to the information in the encryption scheme 5 (step 21). The packets selected for static encryption are encrypted at once, while the packets selected for dynamic encryption only are marked by the pre-processor 1;

2. The server 2 stores the pre-processed TS on its format (step 22). Upon request from the client 4, the stored, partly encrypted, TS is streamed to the encryption proxy 3 (step 23). The request is initiated by e.g. a user choosing a movie from a web page. The client 4 and the encryption proxy 3 negotiate about which encryption set to use, before the TS is streamed to the encryption proxy 3;

3. The encryption proxy 3 encrypts the TS packets marked for dynamic encryption by the pre-processor 1, which, however, may be modified according to the negotiation between the client 4 and the encryption proxy 3 (step 24). The encryption proxy 3 then streams the encrypted TS on to the client 4 over the network 7 (step 25);

4. The client 4 decrypts all encrypted packets (step 26).

Claims

1. Method of encrypting a media stream sent from at least one server (2) via an encryption proxy (3) to a client (4), connected to the encryption proxy (3) over a network (7), **characterised in**, that packets of the media stream are either statically encrypted or dynamically encrypted and that those packets of the media stream which are to be statically encrypted and those packets which are to be dynamically encrypted are selected initially as defined in an encryption scheme (5).

2. Method according to claim 1, **characterised in**, that the method comprises the steps of:

   selecting the packets for static encryption and encrypting these and selecting the packets for dynamic encryption and marking these;

   storing the pre-processed media stream;

   streaming the stored media stream upon request;

   encrypting the packets marked for dynamic encryption and streaming the media stream on;

   decrypting all encrypted packets.

3. Method according to any of the claims 1 or 2, **characterised in**, that the static encryption is made once per media stream and that the dynamic encryption is made once per session.

4. Method according to any of the preceding claims, **characterised in**, that which encryption algorithm to use is negotiated in order to handle different kinds of clients (4).

5. Apparatus of encrypting a media stream sent from at least one server (2) via an encryption proxy (3) to a client (4), connected to the server (2) over a network (7), **characterised in**, that a pre-processor (1) is arranged to statically encrypt a first selection of packets of the media stream and to mark a second selection of packets of the media stream for dynamic encryption, that an encryption proxy

(3) is arranged to dynamically encrypt the second selection of packets and that the pre-processor (1) is arranged to select which packets that are to be statically encrypted and which packets that are to be dynamically encrypted as defined in an encryption scheme (5).

6. Apparatus according to claim 5, **characterised in**, that the server (2) is arranged to store the pre-processed media stream and to stream the pre-processed media stream to the encryption proxy (3) upon request from the client (4), that the encryption proxy (3) is arranged to encrypt the packets marked for dynamic encryption by the pre-processor (1) and to stream the media stream on to the client (4) and that the client (4) is arranged to decrypt all encrypted packets.

7. Apparatus according to claims 5 or 6, **characterised in**, that the pre-processor (1) is arranged to make the static encryption once per media stream and that the encryption proxy (3) is arranged to make the dynamic encryption once per session.

8. Apparatus according to any of claims 5 – 7, **characterised in**, that the client (4) and the encryption proxy (3) are arranged to negotiate about which encryption algorithm to use in order to handle different kinds of clients (4).

Fig. 1

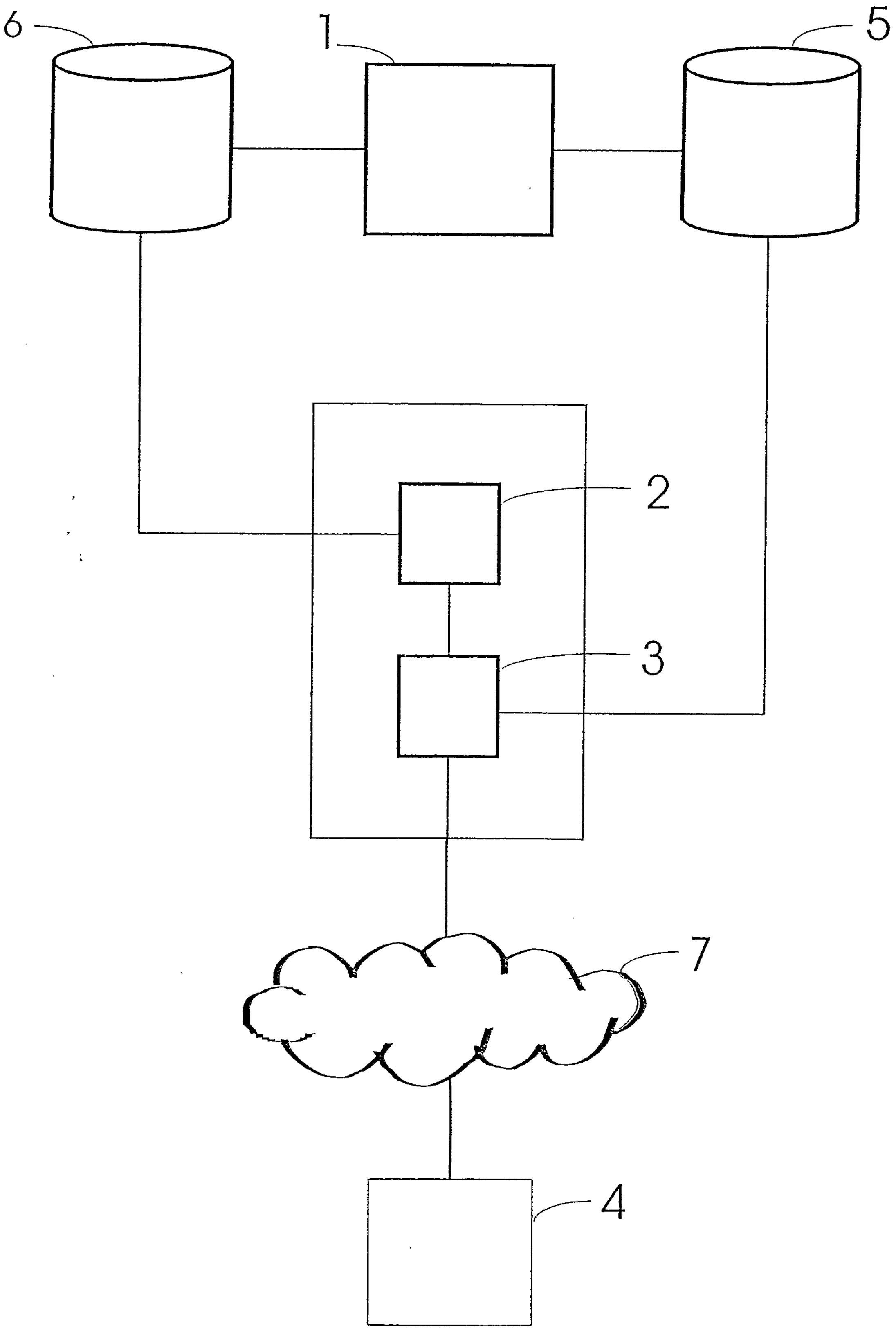
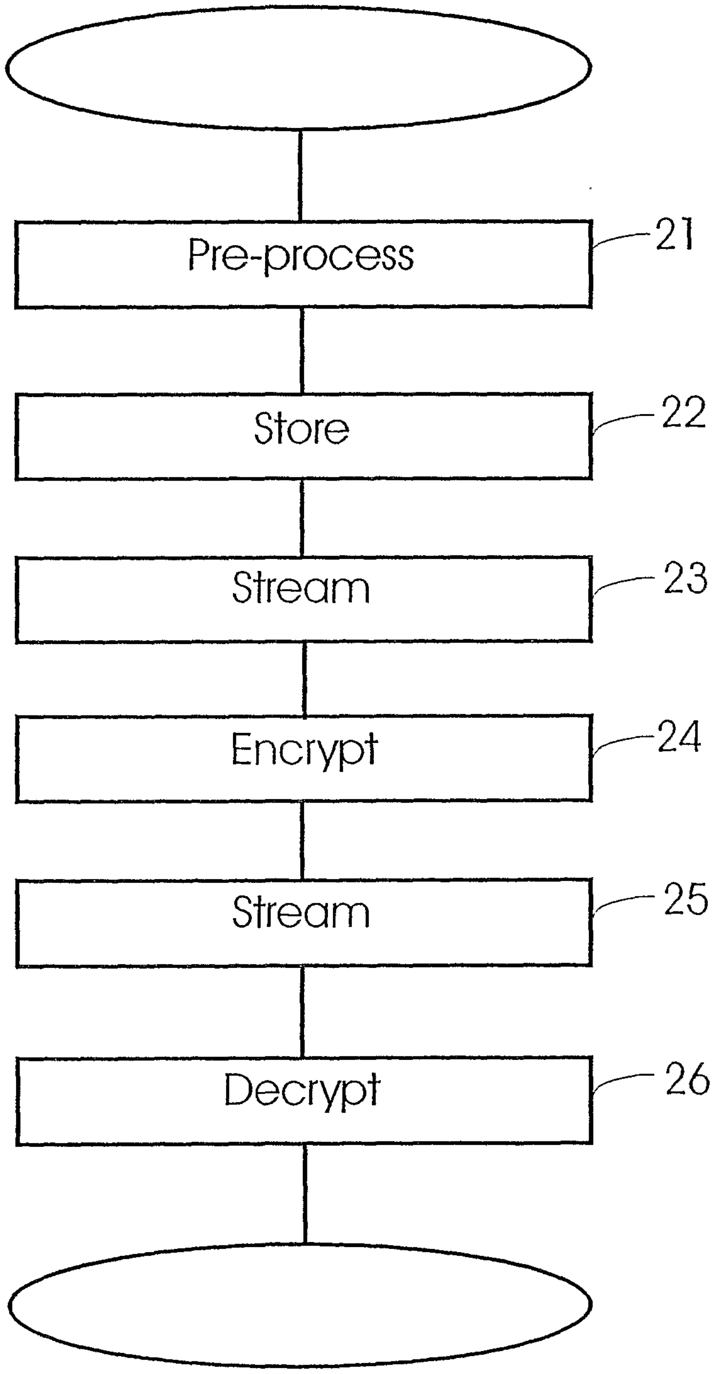


Fig. 2


Pre-process
21
Store
22
Stream
23
Encrypt
24
Stream
25
Decrypt
26

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 02/01830

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 9/18

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)

IPC7: H04L, H04N, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ, INSEPC, TOB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6055314 A (SPIES ET AL), 25 April 2000 (25.04.00), column 3, line 52 - column 4, line 10, abstract --	1-8
A	WO 0064111 A1 (UNIFREE, L.L.C.), 26 October 2000 (26.10.00), abstract --	1-8
A	WO 0048375 A1 (LOUDEYE TECHNOLOGIES, INC.), 17 August 2000 (17.08.00), page 10, line 18 - page 11, line 15, abstract --	1-8
A	EP 1111838 A2 (XEROX CORPORATION), 27 June 2001 (27.06.01), abstract --	1-8

☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 17 January 2003	Date of mailing of the international search report 27 -01- 2003
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer ALEXANDER LAKIC/BS Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 02/01830

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 9948296 A1 (INTERTRUST TECHNOLOGIES CORPORATION), 23 Sept 1999 (23.09.99), page 30, line 13 - line 24, abstract -- --------	1-8

INTERNATIONAL SEARCH REPORT

Information on patent family members

30/12/02

International application No.

PCT/SE 02/01830

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6055314 A	25/04/00	NONE	
WO 0064111 A1	26/10/00	NONE	
WO 0048375 A1	17/08/00	AU 2988600 A	29/08/00
		AU 2988700 A	29/08/00
		AU 2988800 A	29/08/00
		EP 1151592 A	07/11/01
		EP 1151611 A	07/11/01
		EP 1151612 A	07/11/01
		JP 2002537572 T	05/11/02
		WO 0048399 A	17/08/00
		WO 0048400 A	17/08/00
		AU 7735300 A	30/04/01
		EP 1221238 A	10/07/02
		WO 0124530 A	05/04/01
EP 1111838 A2	27/06/01	NONE	
WO 9948296 A1	23/09/99	CA 2323781 A	23/09/99
		CN 1301459 T	27/06/01
		EP 1062812 A	27/12/00
		JP 2002507868 T	12/03/02
		US 6247354 B	19/06/01
		US 6260408 B	17/07/01