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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 January 2006 (26.01.2006)

PCT

(10) International Publication Number
WO 2006/008596 A1

(51) International Patent Classification[7]: H04L 9/00, H04N 7/167

(21) International Application Number: PCT/IB2005/001899

(22) International Filing Date: 1 July 2005 (01.07.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/888,349 9 July 2004 (09.07.2004) US

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(71) Applicant *(for LC only)*: **NOKIA INC.** [US/US]; 6000 Connection Drive, Irving, TX 75039 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **PAILA, Toni** [FI/FI]; Luoteispolku 10, FIN-10160 Degerby (FI). **KARRAS, Timo** [FI/FI]; Varputie 2L, FIN-02270 Espoo (FI). **JYSKE, Eero** [FI/FI]; Lehdokkitie 7 A 13, FIN-01300 Vantaa (FI). **LAHTINEN, Pekka** [FI/FI]; Melkonkatu 7 B 50, FIN-00210 Helsinki (FI). **MULLER, Dominique** [CH/FI]; Museokatu 31 A 25, FIN-00100 Helsinki (FI).

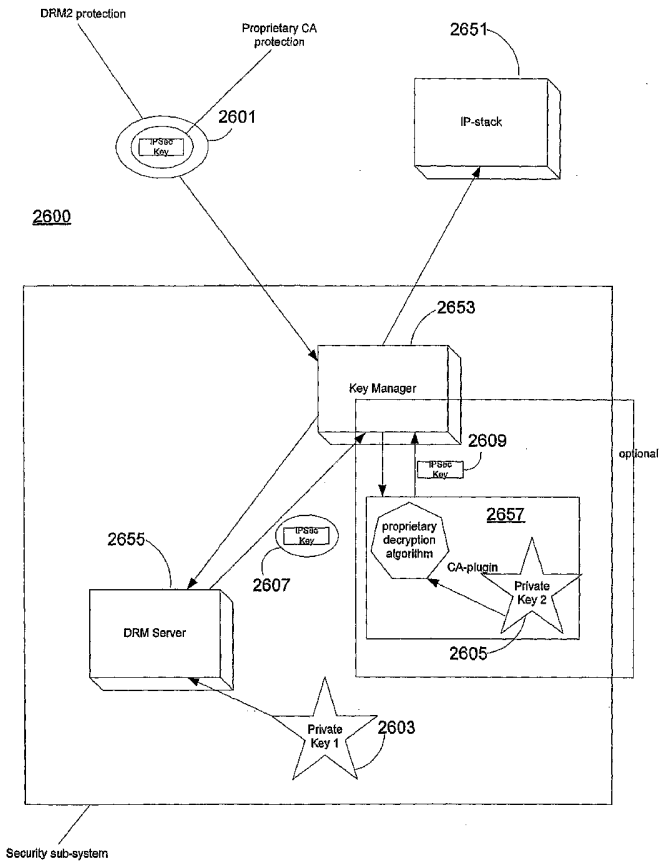
(74) Agent: **WRIGHT, Bradley, C.**; Banner & Witcoff, Ltd., 1001 G. Street, N.W., 11th Floor, Washington, DC 20001-4597 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Continued on next page]

(54) Title: MANAGING TRAFFIC KEYS DURING A MULTI-MEDIA SESSION



(57) Abstract: The present invention provides methods, apparatuses, and systems for delivering protected multimedia content to a receiving device. Portions of protected multi-media content and associated key information are inserted in a same time slice burst. Multi-media content is processed into a plurality of content datagrams, in which each content datagram is associated with a corresponding component. Key information may be processed as a keystream that is logically separate from the components. A content datagram may be encrypted with an associated key. A receiving device receives the time slice burst with the plurality of content datagrams and associated key datagrams of the keystream. The receiving device consequently decrypts the plurality of content datagrams. Also, key information may be processed as key datagrams that are included with at least one component, in which each component comprises an associated plurality of content datagrams.

WO 2006/008596 A1

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

Published:

— *with international search report*

— *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.

MANAGING TRAFFIC KEYS DURING A MULTI-MEDIA SESSION

FIELD OF THE INVENTION

[01] This invention relates to delivering protected multi-media content. In particular, the invention provides apparatuses and methods for providing encryption keys with the associated content.

BACKGROUND OF THE INVENTION

[02] Video streaming, data streaming, and broadband digital broadcast programming are increasing in popularity in wireless network applications, e.g., Internet Protocol (IP) multicast services. To support these wireless applications, wireless broadcast systems transmit data content that support data services to many wireless terminals simultaneously. Digital media content or other data is broadcasted using various application protocols, transport protocols and network protocols. For example, a broadcast system provides IP data broadcast where audio-visual service is transmitted so that MPEG4-AVC video, MPEG4-AAC audio and auxiliary data components are packetized and encapsulated to RTP and/or ALC. The packets are subsequently formatted to UDP and IP and transmitted over MPE in MPEG2-TS (for example DVB-H). In a packet-switched domain, the concept of a multi-media session may require that one or more session components (audio, video and auxiliary data in above case) are logically bound together. The portions of the multi-media session are sent between a common start time and end time. However, with a broadcast environment all receivers that are able to receive the broadcast signal can receive the data carried by the broadcast signal. It is important that the content seller limits access to multi-media content so that only entitled receivers can present the multi-media content to users.

[03] In order to enhance revenue collections, a user is often permitted to access premium multi-media services only if the user subscribes to the service or orders the service (e.g., pay per view). However, without effectively controlling access by the content seller, a

user may access the content without paying for the content if the user bypasses the protection mechanism.

[04] What are needed are apparatuses, methods, and systems that facilitate adequate control procedures that effectively limit access to multi-media content.

BRIEF SUMMARY OF THE INVENTION

[05] An aspect of the present invention provides methods, apparatuses, and systems for delivering protected multi-media content to a receiving device. Portions of protected multi-media content and associated key information are inserted in a same time slice burst. Consequently, key information may be frequently changed while maintaining synchronization with the multi-media content. In one embodiment of the invention, time slice bursts are sent from a transmitting apparatus to a receiving device by a communications system that includes a DVB-H system, a DVB-T system, an ATSC system, and an ISDB-T system.

[06] With an aspect of the invention, multi-media content is partitioned into components. Multi-media content is processed into a plurality of content datagrams, in which each content datagram is associated with a corresponding component. Key information is processed as at least one keystream that is a logically separate from the components, even though the key information is inserted in the same time slice burst as the associated multi-media content. A keystream comprises a plurality of key datagrams, each key datagram containing a key that is associated with at least one content datagram. A content datagram may be encrypted with an associated key. A receiving device receives the time slice burst with the plurality of content datagrams and associated key datagrams of the at least one keystream. The receiving device consequently decrypts the plurality of content datagrams.

[07] With another aspect of the invention, key information is processed as key datagrams that are included with at least one component. Each component comprises an associated plurality of content datagrams. A content datagram may be encrypted with an associated key.

[08] With another aspect of the invention, static security data is sent to a receiving device by transmitting the static security data separately from the time slice burst that carries content information and associated key information. In one embodiment of the invention, a transmitting apparatus transmits the static security data in an electronic service guide (ESG).

[09] With another aspect of the invention, key datagrams are associated with a higher priority level than content datagrams. Consequently, a receiving device can process a key datagram in order to extract a key before routing associated content datagrams to a message stack and decrypting the associated content datagrams.

[10] With another aspect of the invention, a key is encrypted at a level of encryption. The encrypted key may be further encrypted with an additional level of encryption. A receiving device processes the encrypted key in order to obtain the decrypted key. The receiving device subsequently decrypts received content with the decrypted key.

[11] With another aspect of the invention, a new security plug-in software module is deployed at a receiving device to replace a current security plug-in software module. In one embodiment of the invention, the new security plug-in software module is configured as an installation package that is encrypted as a protected message. The receiving device receives the protected message over a communications channel. The receiving device decrypts the protected message to obtain the installation package. Consequently, the new security plug-in software module is installed by executing the installation package.

BRIEF DESCRIPTION OF THE DRAWINGS

[12] A more complete understanding of the present invention and the advantages thereof may be acquired by referring to the following description in consideration of the accompanying drawings, in which like reference numbers indicate like features and wherein:

[13] Figure 1 shows transmission of Internet Protocol (IP) services utilizing time slice transmission in accordance with an embodiment of the invention;

[14] Figure 2 shows a protocol stack that supports transmission of multi-media data in accordance with an embodiment of the invention;

[15] Figure 3 shows a component configuration for a multi-media session according to an embodiment of the invention;

[16] Figure 4 shows a component configuration for a multi-media session shown according to an embodiment of the invention;

[17] Figure 5 shows a variation of the component configuration shown in Figure 4 according to an embodiment of the invention;

[18] Figure 6 shows a variation of the component configuration shown in Figure 4 according to an embodiment of the invention;

[19] Figure 7 shows a variation of the component configuration shown in Figure 4 according to an embodiment of the invention;

[20] Figure 8 shows a variation of the component configuration shown in Figure 4 according to an embodiment of the invention;

[21] Figure 9 shows a variation of the component configuration shown in Figure 4 according to an embodiment of the invention;

[22] Figure 10 shows a component configuration for a multi-media session according to an embodiment of the invention;

[23] Figure 11 shows a variation of the component configuration shown in Figure 10 according to an embodiment of the invention;

[24] Figure 12 shows a variation of the component configuration shown in Figure 10 according to an embodiment of the invention;

[25] Figure 13 shows a variation of the component configuration shown in Figure 10 according to an embodiment of the invention;

[26] Figure 14 shows a variation of the component configuration shown in Figure 10 according to an embodiment of the invention;

[27] Figure 15 shows a variation of the component configuration shown in Figure 10 according to an embodiment of the invention;

[28] Figure 16 shows a variation of the component configuration shown in Figure 10 according to an embodiment of the invention;

[29] Figure 17 shows a procedure for receiving a multi-media session in accordance with an embodiment of the invention;

[30] Figure 18 shows a flow diagram for the architecture shown in Figure 17 in accordance with an embodiment of the invention;

[31] Figure 19 shows a system for protected content transfer that supports DVB-H IPDC (IP datacast) services according to prior art;

[32] Figure 20 shows a system that supports DVB-H IPDC services in accordance with an embodiment of the invention;

[33] Figure 21 show a flow diagram for transmitting data for DVB-H IPDC services in the system shown in Figure 20 in accordance with an embodiment of the invention;

[34] Figure 22 shows a system that supports DVB-H IPDC services in accordance with an embodiment of the invention;

[35] Figure 23 shows a system that supports DVB-H IPDC services in accordance with an embodiment of the invention;

[36] Figure 24 shows an apparatus for that supports a transmission module as shown in Figures 20, 22, and 23 in accordance with an embodiment of the invention;

[37] Figure 25 shows an apparatus that receives a multi-media broadcast and that applies IPSec keys in accordance with an embodiment of the invention;

[38] Figure 26 shows an apparatus that receives a multi-media broadcast and that decrypts the IPSec keys in accordance with an embodiment of the invention; and

[39] Figure 27 shows a system for deploying a security plug-in software module in accordance with an embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[40] In the following description of the various embodiments, reference is made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration various embodiments in which the invention may be practiced. It is to be understood that other embodiments may be utilized and structural and functional modifications may be made without departing from the scope of the present invention.

[41] Figure 1 shows transmission of Internet Protocol (IP) services utilizing time slice transmission in accordance with an embodiment of the invention. A base station broadcasts data packets for a plurality of IP services using data streams 101, 103, 105, and 107. (Each data stream is allocated a portion of a data rate capacity.) In the embodiment, the base station may support functionality that is typically assumed by a base transceiver station (BTS), a base station controller (BSC), a combination of a BTS and a BSC, and a node B, which is a third Generation (3G) designation of a base transceiver station. Data transmission is essentially continuous such that data packets for an IP service are continuously being conveyed through a data stream.

[42] In order to mitigate the loss of data packets, data streams 101, 103, 105, and 107 are mapped by base stations into bursts of data packets 109, 111, 113, and 115, respectively, in which bursts are transmitted over radio channels rather than data streams 101, 103, 105, and 107. Each data stream (101, 103, 105, and 107), and consequently each burst (109, 111, 113, and 115), supports at least one data service. Thus, each burst may support a plurality of data services (e.g., a group of related data services).

[43] Data rates associated with bursts 109, 111, 113, and 115 are typically greater than data rates that are associated with data streams 101, 103, 105, and 107 so that a corresponding

number of data packets can be sent in a shorter amount of time. In the embodiment, data streams 101, 103, 105, and 107 correspond to continuous data rates of approximately 100 Kbit/sec. Bursts 109, 111, 113, and 115 typically correspond to approximately 4 Mbit/sec (but may be in excess of 10 Mbit/sec) with an approximate one second duration. However, other embodiments may use different data rates for data streams 101-107 and for bursts 109-115.

[44] In the embodiment, the entire data rate capacity is allocated to a burst at a given time. As shown in Figure 1, bursts 109, 111, 113, and 115 are interleaved in time. An idle time duration (during which data packets are not transmitted for the particular data service) occurs between consecutive transmissions of a burst (e.g., burst 109). A wireless broadcast system can utilize the idle time duration during which the wireless terminal can be instructed to transfer to another base station to complete a handover. The other base station may transmit the same data as the base station previously serving the wireless terminal using a different center frequency and a different amount of phase shift. The utilization of time slicing enables a terminal to reduce the consumption of electrical power that is provided by a power source (typically a battery).

[45] Bursts are typically transmitted periodically by a base station. For example, a subsequent burst may occur T seconds after burst 109, in which a burst is transmitted every T seconds. The wireless terminal may maintain precise timing, as with the Global Positioning System (GPS), to determine an absolute time at which each burst occurs. In another embodiment, the wireless terminal is provided information about a time period in each burst, informing the wireless terminal about the subsequent burst. With an embodiment of the invention, the time period information includes a real-time parameter (corresponding to "delta-t" with DVB-H) that indicates a time interval from the beginning of a time slice burst to the beginning of the next time slice burst of the same service and that is signaled in a MPE section header. The time period may be included in an IP packet, a multiprotocol encapsulated frame, any other packet frame, and a third generation (3G) or General Packet Radio Service (GPRS) channel or modulation data, such as transmitter parameter signaling. Alternatively, the wireless terminal may detect an occurrence of a burst by receiving a signal preamble, which may be a data sequence

that is known a priori to the wireless terminal. In another embodiment, the wireless terminal may receive an overhead message on an overhead channel from a base station. The overhead message may contain timing information regarding the occurrence of bursts. The overhead channel may be logically or physically distinct from the downlink radio channel that supports the transmission of bursts.

[46] Bursts 109, 111, 113, and 115 may be formatted by using a multi-protocol encapsulation in accordance with Section 7 of European Standard EN 301 192 "Digital Video Broadcasting (DVB), DVB specification for data broadcasting." The encapsulation may conform to Internet Protocol (IP) standards.

[47] In an embodiment of the invention, a Digital Video Broadcast (DVB-H) provides mobile media services to wireless terminals, e.g., handheld wireless units. In the embodiment, the DVB-H system is compatible with DVB-T (digital video broadcast for terrestrial operation) and supports enhancements to better support operation of wireless handheld terminals. The DVB-H system supports Internet Protocol (IP) based data services in which the information may be transmitted as IP datagrams. The DVB-H system incorporates enhancements (with respect to a DVB-T system) that facilitates access to IP based DVB services on wireless handheld wireless terminals. (Alternative embodiments of the invention support variations of digital video broadcast systems including DVB-T, ATSC, and ISDB-T.) The DVB-H enhancements are based on the physical layer of the DVB-T physical layer with a number of service layer enhancements aimed at improving battery life and reception in the handheld environment. Thus, the DVB-H enhancements compliment existing digital terrestrial services, offering service providers the possibility to extend the market to the wireless handheld market.

[48] Figure 2 shows an internet protocol (IP) stack 200 that supports transmission of multi-media data in accordance with an embodiment of the invention. Digital media content or other data is broadcasted using various application protocols, transport protocols and network protocols. With IP stack 200, an IP data broadcast supports an audio-visual service having MPEG4-AVC video 201, MPEG4-AAC audio 203 and auxiliary data 205 components. Each component (201, 203, or 205) is processed by coder 207, coder 209, or

coder 211 in order to obtain packets that are formatted for Real Time Protocol (RTP) layer 213. The packets (datagrams) are subsequently processed by UDP (user datagram protocol) layer 215 and Internet Protocol (IP) layer 217. Datagrams are associated with time slice bursts by formatting the datagrams using a multi-protocol encapsulation (typically corresponding to a link layer in the OSI model) such as, for example, in accordance with Section 7 of European Standard EN 301 192 "Digital Video Broadcasting (DVB), DVB specification for data broadcasting." The encapsulation may conform to Internet Protocol (IP) standards.

[49] A multi-media session typically is associated with one or more session components (audio, video and auxiliary data in above case) that are logically bound together. The parts of the session are sent between a common start time and end time. Both start time and/or end time of can be either defined or undefined.

[50] Figure 3 shows a component configuration 300 for a multi-media session 301 according to an embodiment of the invention. Component 303 corresponds to a plurality of datagrams (including datagrams 309 and 315); component 305 corresponds to a plurality of datagrams (including datagrams 311 and 317); and component 307 corresponds to a plurality of datagrams (including datagrams 313 and 319). Components 303, 305, and 307 are transmitted within IP packets that are encapsulated to messaging of an underlying bearer layer. Each component 303, 305, and 307 has a defined source IP address, destination IP address, and port used in the IP packets that carry data associated with the component. Different components may have an independently defined source IP address, a destination IP address, and a port. In variations of the embodiment, a multi-media session may have a different number of components.

[51] While exemplary component configuration 300 shows datagram alignment between components 303, 305, 307, the embodiment supports configurations in which the datagrams are not aligned and the number of datagrams for each component is different from that of the other components. For example, the number of datagrams for an audio component is typically less than the number of datagrams for a video component during a given time interval.

[52] Figure 4 shows a component configuration 400 for a multi-media session 401 according to an embodiment of the invention. Components 403, 405, and 407 are encrypted with the same key that changes periodically in keystream 409 during multi-media session 401. (In Figures 4-16, a datagram that is encrypted with key k_i is denoted as E_i. (Keystream 409 is a logical channel that contains key information and that is separate from the media components.) Similarly, a datagram associated with the j^{th} component and that is encrypted with the i^{th} key associated with the j^{th} component is denoted as E_{ji}.) The embodiment supports different encryption methods that are applied to component 403, 405, or 407, including:

- IPSEC-ESP (so called IP-level encryption; see RFC on IPSEC-ESP)
- Payload of the application session packet encrypted (for example SRTP or DCF of OMA DRM 1.0 or 2.0)
- Encryption

The above encryption methods may be applied separately or in combination during multi-media session 401. Components 403, 405, and 407 correspond to a different plurality of content datagrams. Keystream 409 includes a plurality of associated datagrams, each associated datagram corresponding to an encryption key. Encryption is typically performed on an individual datagram (e.g., packet) basis. For example, content datagrams 415, 425, 427, 435, and 437 are encrypted with key k_1 (corresponding to associated datagram 411) and content datagram 417 is encrypted with k_2 (corresponding to associated datagram 413).

[53] Keystream 409 utilizes a delivery protocol such as RTP, ALC/FLUTE, UHTTP, DVBSTP, IP with a payload, and UDP with a payload. The keys delivered in keystream 409 are typically protected by another key that the entitled receiver has in order to access the contents of keystream 409 that carries keys, thus enabling access to the components 403, 405, and 407. The delivery of keystream 409 is optionally synchronized with components 403, 405, and 407, e.g., RTP timestamps with the use of RTP Control Protocol).

[54] Figure 5 shows a variation of the component configuration shown in Figure 4 according to an embodiment of the invention. Component configuration 500 is similar to

component configuration 400. Multi-media session 501 includes components 503, 505, and 507 and keystream 509. Component 505 is encrypted with keys from keystream 509, while components 503 and 507 are not.

[55] Figure 6 shows a variation of the component configuration shown in Figure 4 according to an embodiment of the invention. Component configuration 600 is similar to component configuration 400. However, keystream 609 includes three series of keys 611, 613, and 615 that correspond to components 603, 605, and 607, respectively. The keys may change periodically but independently during multi-media session 601 but may be synchronized with each other.

[56] Figure 7 shows a variation of the component configuration shown in Figure 4 according to an embodiment of the invention. Component configuration 700 is similar to component configuration 600 except that keys for each component are carried on different keystreams that change during multi-media session 701. Rather than having one keystream, component configuration 700 utilizes three keystreams 709, 711, and 713. Keystreams 709, 711, and 713 correspond to components 703, 705, and 707, respectively.

[57] Figure 8 shows a variation of the component configuration shown in Figure 4 according to an embodiment of the invention. With component configuration 800, component 805 is encrypted with keys from keystream 809. However, keystream 809 provides keys that are currently applicable to decrypting component 805 as well as keys that will be subsequently used in decrypting component 805. In the example shown in Figure 8, key k_1 (corresponding to datagram 811) is currently applied while keys k_2 (corresponding to datagram 813) and k_3 (corresponding to datagram 815) are subsequently applied. While components 803 and 807 are not encrypted during multi-media session 801, components 803 and 807 may be encrypted with other variations of the embodiment. Having keys that will be subsequently applied enables a receiver device to smoothen key transitions during multi-media session 801. For example, the receiver device can configure the IP stack with a new key to reduce interruptions in decrypting content datagrams.

[58] Figure 9 shows a variation of the component configuration shown in Figure 4 according to an embodiment of the invention. Keystream 909 includes the key currently being applied to component 905 for encryption as well as keys that will be subsequently applied when the key transition is within a predetermined incremental time of the current time. For example, before key transition 951, keystream 909 includes both keys k_1 (corresponding to datagram 911) and k_2 (corresponding to datagram 913) and includes only k_2 (corresponding to datagram 915) after the key transition 951. As with component configuration 800, component configuration 900 assists the receiver device to smoothen the effects of key transitions.

[59] Figure 10 shows a component configuration 1000 for a multi-media session 1001 according to an embodiment of the invention. However, in comparison with component configurations 400-900, keys are carried in one or more of the components rather than having a separate keystream for transmitting the keys. With component configuration 100, component 1005 includes content datagrams (e.g., content datagram 1011) as well as datagram 1009 that provides key k_1 that has been used for encrypting components 1003, 1005, and 1007.

[60] Figure 11 shows a variation of the component configuration shown in Figure 10 according to an embodiment of the invention. With component configuration 1100, component 1107 provides key k_1 (corresponding to datagram 1109) and key k_2 (corresponding to datagram 1111) that are applied to component 1105 during multi-media session 1101. In the example shown in Figure 11, components 1103 and 1107 are not encrypted with the keys provided by component 1107.

[61] Figure 12 shows a variation of the component configuration shown in Figure 10 according to an embodiment of the invention. Component configuration 1200 is similar to component configuration 1100. However, keys are applied to both the component carrying key information (component 1205) as well another component (component 1203) during multi-media session 1201. However, in the example shown in Figure 12, component 1207 is not encrypted.

[62] Figure 13 shows a variation of the component configuration shown in Figure 10 according to an embodiment of the invention. With component configuration 1300, each component 1303, 1305, and 1307 carries keys that are applied to the same component during multi-media session 1301. For example, keys k_{11} (corresponding to datagram 1309) and k_{12} (corresponding to datagram 1311) are applied to component 1303. Keys k_{21} (corresponding to datagram 1313) and k_{22} (corresponding to datagram 1315) are applied to component 1305. Keys k_{31} (corresponding to datagram 1317) and k_{32} (corresponding to datagram 1319) are applied to component 1307.

[63] Figure 14 shows a variation of the component configuration shown in Figure 10 according to an embodiment of the invention. With component configuration 1400, each component 1403, 1405, and 1407 carries keys that are applied to a different component during multi-media session 1401. For example, keys k_{11} (corresponding to datagram 1413 and carried by component 1405) and k_{12} (corresponding to datagram 1419 and carried by component 1407) are applied to component 1403. Keys k_{21} (corresponding to datagram 1417 and carried by component 1407) and k_{22} (corresponding to datagram 1411 and carried by component 1403) are applied to component 1405. Keys k_{31} (corresponding to datagram 1409 and carried by component 1403) and k_{32} (corresponding to datagram 1415 and carried by component 1405) are applied to component 1407.

[64] Figure 15 shows a variation of the component configuration shown in Figure 10 according to an embodiment of the invention. With component configuration 1500, key information is carried in a content datagram rather than in a separate datagram. For example, key k_1 is included in content datagram 1509 within a concatenated portion (or with a special header) 1511 and k_2 is included in content datagram 1513 within a concatenated portion (or with a special header) 1515. Keys k_1 and k_2 are applied to datagrams in components 1503, 1505, and 1507.

[65] Figure 16 shows a variation of the component configuration shown in Figure 10 according to an embodiment of the invention. Component configuration 1600 is similar to component configuration 800, in which both the current key as well as subsequent

keys are provided. For example, component 1605 carries key k_1 (corresponding to datagram 1609) and key k_2 (corresponding to datagram 1611), where key k_1 is currently applied to components 1603 and 1607 and key k_2 is subsequently applied during multi-media session 1601. Similarly, key k_2 (corresponding to datagram 1613) and key k_3 (corresponding to datagram 1615) are subsequently carried in component 1605. As with component configuration 800, component configuration 1600 assists the receiver device to smoothen key transitions.

[66] Figure 17 shows an architecture 1700 for receiving a multi-media session in accordance with an embodiment of the invention. With architecture 1700, a receiving device receives time slice burst of data 1701 containing both the IP session components and the keystream related to the session components. Pluralities of content datagrams 1705, 1707, and 1709 correspond to component 1, component 2, and component 3, respectively. A plurality of datagrams 1711 corresponds to the keystream. Time slice burst 1701 is stored in interim buffer 1713 before forwarding the datagrams (packets) to IP stack 1721. The receiving device first extracts the keys (corresponding to datagram 1717) for the received time slice burst 1701 from interim buffer 1713. Second, the receiving device installs the extracted keys to IPSec Security Association (SA) database 1719. Also, the receiving device extracts remaining datagrams 1715 from the interim buffer and forwards them to IP stack 1721. After decryption, the processed datagrams are passed to applications 1723 for the presentation of the multi-media content. Consequently, IP stack 1721 does not reject the content datagrams (unless there are content datagrams that the receiving device did not have a corresponding key as delivered in the current time slice or a previous time slice burst). The process is repeated for a next received time slice burst 1703.

[67] Figure 18 shows flow diagram 1800 for the architecture shown in Figure 17 in accordance with an embodiment of the invention. In step 1801, a receiving device receives a time slice burst over a communications channel, e.g., a wireless channel. In step 1803, the receiving device separates components (e.g., an audio component and a video component) from the received time slice burst. In step 1805, the receiving device extracts the associated set of keys from the keystream. The extracted keys may be

applied to content datagrams contained in the time slice burst or in subsequent time slice bursts. Also, the embodiment supports configurations in which different keys are used for different datagrams in the time slice burst. The extracted keys are applied to an IPSec Security Association (SA) database (e.g., SA DB 1719 shown in Figure 17) in step 1807. In step 1809, the content datagrams are extracted from a buffer (e.g., interim buffer 1713) and sent to an IP stack (e.g., stack 1721) in step 1811. The content datagrams are subsequently decrypted and sent to the corresponding application.

[68] Figure 19 shows a system 1900 for protected content transfer that supports DVB-H IPDC (IP datacast) services according to prior art. System 1900 provides protected content transfer for DVB-H services using IPDC as specified in "Interim DVB-H IP Datacast Specifications: IP Datacast Baseline Specification: Specification of Interface I_MT", DVB Document A080, April 2004. In accordance with this specification, portions of security associated data are transmitted in an electronic service directory (ESG) in SA carousel 1921 as DRM protected SA file 1919 (which is provided by digital rights manager (DRM) 1909 by performing the protection function) and IPSec policy file 1911. As the carousel data is typically updated infrequently (e.g., once a day) system 1900 does not provide an efficient solution for key delivery, especially if one or more of the keys is updated or frequently changes.

[69] Multi-media content 1901 (corresponding to IP datagrams) is encrypted by encryption module 1903 with IPSec keys 1905 and transmitted (as performed by transmission system 1925) as time slice packets (after multi-protocol encapsulation, FEC encoding, and time slice burst formation) to receiving device 1926. Rights object (RO) 1923 (which is provided by rights object generation 1922) is transmitted to receiving device 1926 through an interaction channel, in which receiving device 1926 is provided with a means for bidirectional communications, e.g., mobile phone functionality. A user of receiving device 1926 may order service (content) and consequently receive the corresponding rights object (RO) 1933, which allows the user to decrypt the content of the ordered service. In the embodiment, rights object 1933 typically does not contain IPSec keys 1905.

[70] Receiving device 1926 processes time slice bursts with burst processing module 1927. Received packets are decrypted by decryption module 1929 with a key provided by key extraction module 1931 in order to obtain content 1935. The keys are determined from rights object 1933. The keys are typically delivered in a SA carousel as DRM protected SA files. Rights object 1933 allows receiving device 1926 to extract the keys.

[71] Figure 20 shows a system 2000 that supports DVB-H IPDC services in accordance with an embodiment of the invention. Multi-media content 2001 (corresponding to content datagrams) is encrypted by encryption module 2003 by applying IPSec keys 2005. Transmission system 2025 obtains both encrypted content datagrams from encryption module 2003 and the corresponding keys from DRM 2009. Transmission system 2025 forms corresponding datagrams that contain the keys corresponding to encrypting the content datagrams. Transmission system 2025 inserts both the encrypted content datagrams and the corresponding datagrams into a time slice burst, which is transmitted to receiving device 2026 over a communications channel. While Figure 20 does not explicitly show a radio module, the embodiment may provide wireless signal capability in order to transmit the time slice burst to receiving device 2026 over a wireless channel.

[72] Receiving device 2026 processes a received time slice burst, in which the encrypted content datagrams and corresponding datagrams (containing the corresponding keys that are used for encrypting the received content datagrams) are separated (demultiplexed) by burst processing module 2027. In the embodiment, receiving device 2026 comprises a broadband receiver for receiving DVB signals that include time slice bursts and a transceiver for bidirectional communications in a wireless network. The bidirectional communications supports service ordering by a user, OMA messaging, and security plug-in module installation. The embodiment supports different signal configurations, in which the keys are included in a separate keystream or in which keys are included in multi-media components as previously discussed with Figures 4-16. Key extraction module 2031 extracts the keys from the corresponding datagrams in order to decrypt the content datagrams, as performed by decryption module 2029. Decryption module provides decrypted content 2035 to an application (not shown) so that the content can be presented.

[73] Additionally, rights management object 2023 (as determined by rights object generator 2022) is separately transmitted to receiving device 2026 in response to a purchase order. Consequently, receiving device 2026 receives rights object 2033 to determine if receiving device 2026 is permitted to process the received content.

[74] Figure 21 show a flow diagram 2100 for transmitting data for DVB-H IPDC services in system 2000 in accordance with an embodiment of the invention. In step 2101, transmitting apparatus (e.g., transmission system 2025) determines if an obtained content datagram should be included in the current time slice burst. If not, the time slice burst (with previously obtained content datagrams and associated keys) is sent to the receiving device in step 2109.

[75] If the obtained content datagram should be included in the current time slice burst, step 2103 determines the corresponding key and encrypts the content datagram with the key in step 2105. In step 2107 the encrypted content datagram and the corresponding key information (corresponding to a corresponding datagram that may be included in multi-media component or in a keystream) is inserted in the current time slice burst.

[76] Figure 22 shows a system 2200 that supports DVB-H IPDC services in accordance with an embodiment of the invention. In Figure 22, elements 2201, 2203, 2205, 2222, 2223, 2227, 2229, 2231, 2233, and 2235 correspond to elements 2001, 2003, 2005, 2022, 2023, 2027, 2029, 2031, 2033, and 2035 as shown in Figure 20. As with system 2000, system 2200 transmits content datagrams and corresponding key information in the same time slice burst. Key information is provided to transmission system 2225 by key message generator 2206. Key message generator may further encrypt the keys so that encrypted key information is transmitted to receiving device 2226 by transmission system 2225. DRM 2209, in conjunction with rights object generator 2222, provides rights object 2233 that corresponds to the desired DVB-H IPDC service to receiving device 2226.

[77] IPSec policy files 2211 (that may contain security association information) are separately transmitted in SA carousel 2221 from the service (content) and key messages that are multiplexed and transmitted using IPDC time slicing. In the embodiment, SA carousel 2221 is transmitted as part of the electronic service guide (ESG).

[78] Figure 23 shows a system 2300 that supports DVB-H IPDC services in accordance with an embodiment of the invention. System 2300 supports conditional access (CA) that can provide a second-level of encryption using a corresponding private key. (As will be discussed with Figure 26, IPSec keys may be encrypted by digital rights management (DRM) as well as by a CA module.) Receiving device 2326 comprises a receiver section and a terminal section. The receiver section performs burst processing, demultiplexing, and key management. The receiver section also includes CA plug-in installation and key decryption. DRM 2351 sends CA plug-in installation package 2353 to DRM 2314 so that a new CA plug-in module is installed at receiving device 2326 as will be further discussed with Figure 27. The key decryption is performed in a secure processing environment. The terminal section performs key management and key decryption in addition to the decryption (corresponding to decryption module 2329) and content rendering (corresponding to content 2335).

[79] Encryption of keys 2305 (which are used to encrypt content 2301 by encryption module 2303) is performed by key encryption module 2311. Key encryption module 2311 comprises CA module 2308 and DRM 2309. Thus, key encryption module 2311 may provide two levels of encryption. Both the encrypted key information and the content datagrams are included in the same time slice burst by transmission system 2325.

[80] Correspondingly, decryption of the received key information is performed by key decryption module 2317. Key decryption module 2317 comprises DRM 2314 and CA module 2315. Key decryption module 2317 performs two levels of decryption that correspond to the two levels of encryption. Burst processing module 2327 decrypts the received content datagrams using the decrypted keys provided by key manager 2313. Received content datagrams are decrypted by decryption module 2329 of the terminal section. Key manager 2313 receives the key information that is demultiplexed by module 2327 and forwards the key information to key decryption module 2317 (which is associated with a trusted environment) for DRM and CA decryption.

[81] In the embodiment, the rights object (RO) is transmitted as an OMA DRM 2 message (according to the proposed Open Mobile Alliance Digital Rights Management Version

2.0) from DRM 2309 to DRM 2314. The rights object is typically transmitted separately from the time slice bursts.

[82] Figure 24 shows apparatus 2400 that supports a transmission system (e.g., 2025, 2225, and 2325) as shown in Figures 20, 22, and 23 in accordance with an embodiment of the invention. In the embodiment, apparatus 2400 performs functions typically associated with a link layer (the second layer of the OSI protocol model). Processor 2405 obtains encrypted datagrams from an encryption module (not shown) through encryption interface 2401 and corresponding key information from a key generator (not shown) through key interface 2403. Transmission interface 2407 encodes the datagrams for forward error correction at the receiving device, performs multi-protocol encapsulation, and formats the time slice burst with the encoded datagrams. (In the embodiment, the datagrams include both content datagrams and corresponding datagrams containing the keys.)

[83] Figure 25 shows apparatus 2500 for a receiving device (e.g., receiving devices 1926, 2026, 2226, and 2326 as shown in Figure 19, 20, 22, and 23, respectively) that receives a multi-media broadcast and that applies IPSec keys in accordance with an embodiment of the invention. Apparatus 2500 processes a time slice burst (e.g., time slice bursts 2501 and 2503) in order to extract the content datagrams and associated keystream. In the embodiment shown in Figure 25, time slice burst 2501 or time slice burst 2503 has content datagrams (e.g., content datagrams 2505, 2507, and 2509) with ESP capsulated IP-packets containing service content and corresponding key datagrams (e.g., corresponding datagram 2511) comprising UDP key-messages. The keys in an UDP key-message may be protected with DRM.

[84] Apparatus 2500 is capable of distinguishing between service content and key-messages. Consequently, receiver module 2551 separates content datagrams from key datagrams. In the embodiment, key datagrams are given a higher priority level than content datagrams by the transmitting apparatus (not shown). In the embodiment, the priority level associated with a datagram is indicated by a field, e.g., a type of service (ToS) field or a differentiated services field. Thus, key datagrams are sent to IP stack 2553 before

corresponding content datagrams so that more time may be allotted for key processing by key decryption module 2555. Key decryption module is presented encrypted keys from IP stack 2553 through key manager 2559.

[85] The embodiments shown in Figures 17 and 25 include the keys in the same time slice burst as the associated content datagram. However, in another embodiment, keys in a time slice burst are associated with decrypting content datagrams that are contained in the next time slice burst, thus allowing more time for key processing.

[86] The decrypted keys are presented to IPSec module 2557 so that the associated content datagrams in IP stack 2553 can be decrypted and presented to client 2561.

[87] Figure 26 shows apparatus 2600 that receives a multi-media broadcast and that decrypts received IPSec keys 2601 in accordance with an embodiment of the invention. Key manager 2653 routes the encrypted IPSec key to DRM server 2655 to decrypt a second-level of encryption using a public decryption algorithm and private key 2603. DRM server 2655 returns second-level decrypted key 2607 to key manager 2653. If the key manager 2653 determines that the key is encrypted with a first-level of encryption, key manager 2653 routes the second-level decrypted key to CA plug-in software module 2657. CA plug-in module 2657 utilizes a secret decryption algorithm and private key 2605 to decrypt second-level decrypted key 2607. In an embodiment of the invention, the secret decryption algorithm corresponds to a DVB common scrambling algorithm (CSA), which is available from the European Telecommunications Standards Institute (ETSI). CA plug-in software module 2657 returns decrypted key 2609 to key manager 2653, which forwards decrypted key 2609 to IP stack 2651.

[88] In the embodiment, CA plug-in module 2657 performs a first-level of decryption that is optional and that is based on an operator-specific CA-method that includes an associated private key and an associated decryption algorithm. The second-level of encryption is based on an open standard, e.g., OMA DRM2. Because the first-level of encryption is optional, key manager 2653 determines whether a first-level of encryption has been applied to second-level decrypted key 2607. If so, key manager 2653 routes second-level decrypted key 2607 to CA plug-in software module 2657. If not, key manager 2653

routes second-level decrypted key 2607 directly to IP stack 2651 because second-level decrypted key 2607 is completely decrypted.

[89] In the embodiment, key manager 2653 determines whether second-level decrypted key 2607 has been first-level encrypted by examining an associated encryption indicator (not shown), e.g., a header or a message field. The associated encryption indicator indicates 'YES' if second-level decrypted key 2607 has been first-level encrypted and 'NO' if second-level decrypted key 2607 has not been first-level encrypted. If second-level decrypted key 2607 has been first-level encrypted, the associated encryption indicator is not first-level encrypted.

[90] Figure 27 shows system 2700 for deploying a new security plug-in software module 2701 at receiving device 2750 in accordance with an embodiment of the invention. Security plug-in software module 2701 is formatted as an installation package 2705 (e.g., a SIS file as supported by Symbian). Installation package 2705 is protected (e.g., with OMA-DRM2) to form protected package 2707 and delivered to a receiving device using a delivery mechanism. The embodiment supports different communications channels in a delivery mechanism, including a wireless communications channel in which the receiving device is a wireless terminal. The received protected package 2707 is directed to application installer 2751, which is a trusted application. Application installer 2751 extracts new security plug-in software module 2701 from protected package 2707 and replaces current security plug-in software module 2755 that is currently installed at the receiving device 2750 with new security plug-in software module 2701. In order to extract new security plug-in software module 2701, receiving device 2750 receives rights object 2703 that is processed by DRM 2753. Consequently, DRM 2753 indicates to application installer 2751 that security plug-in software module replacement is permitted.

[91] In embodiments of the invention, component configurations as shown in Figures 3-16 may be incorporated in systems as shown in Figures 20, 22, and 23.

[92] As can be appreciated by one skilled in the art, a computer system with an associated computer-readable medium containing instructions for controlling the computer system can be utilized to implement the exemplary embodiments that are disclosed herein. The

computer system may include at least one computer such as a microprocessor, digital signal processor, and associated peripheral electronic circuitry.

[93] While the invention has been described with respect to specific examples including presently preferred modes of carrying out the invention, those skilled in the art will appreciate that there are numerous variations and permutations of the above described systems and techniques that fall within the spirit and scope of the invention as set forth in the appended claims.

We Claim:

1. A method for transmitting data by a communications system during a multi-media session comprising a plurality of media components, comprising:

(A) encrypting a first datagram with a first key and including the first encrypted datagram in a first component of the multi-media session, the first datagram containing content;

(B) transmitting the first encrypted datagram of the first component in a time slice burst; and

(C) transmitting first key information in the time slice burst, wherein the first key information contains the first key.

2. The method of claim 1, wherein (C) comprises:

(i) including the first key information in a corresponding datagram in a first keystream of the multi-media session; and

(ii) transmitting the corresponding datagram of the first keystream in the time slice burst.

3. The method of claim 1, further comprising:

(D) encrypting a second datagram with a second key and including the second encrypted datagram in the first component of the multi-media session, the second encrypted datagram containing content;

(E) transmitting the second encrypted datagram in the time slice burst; and

(F) transmitting second key information in the time slice burst, wherein the second key information contains the second key.

4. The method of claim 2, further comprising:

(D) encrypting a second datagram with the first key and including the second encrypted datagram in a second component of the multi-media session, the second encrypted datagram containing content; and

(E) transmitting the second encrypted datagram in the time slice burst.

5. The method of claim 2, further comprising:

(D) transmitting a second datagram of a second component in the time slice burst without encrypting the second datagram.

6. The method of claim 2, further comprising:

(D) encrypting a second datagram with a second key and including the second encrypted datagram in a second component of the multi-media session, the second component containing associated content;

(E) transmitting the second encrypted datagram in the time slice burst; and

(F) including the second key in an associated datagram of the first keystream in the time slice burst.

7. The method of claim 2, further comprising:

(D) encrypting a second datagram with a second key and including the second encrypted datagram in a second component of the multi-media session, the second encrypted datagram containing associated content;

(E) transmitting the second encrypted datagram in the time slice burst; and

(F) including the second key in an associated datagram of a second keystream in the time slice burst.

8. The method of claim 2, wherein the first keystream includes a subsequent key, the subsequent key being applied to an encryption of the first component at a subsequent time.

9. The method of claim 2, wherein the first keystream includes a subsequent key, the subsequent key being applied to an encryption of the first component within a subsequent time.

10. The method of claim 1, further comprising:

(D) encrypting the first key information before transmitting the first key information.

11. The method of claim 1, wherein (A) through (C) are performed in the communications systems selected from the group consisting of a DVB-H system, a DVB-T system, an ATSC system, and an ISDB-T system.

12. The method of claim 1, wherein the first datagram comprises an IP packet.

13. The method of claim 1, wherein the first key comprises an IPSec key.

14. A computer-readable medium having computer-executable instructions for performing the steps recited in claim 1.

15. A computer-readable medium having computer-executable instructions for performing the steps recited in claim 2.

16. A computer-readable medium having computer-executable instructions for performing the steps recited in claim 3.

17. A method for receiving data by a communications system during a multi-media session comprising a plurality of media components, comprising:

(A) receiving a time slice burst comprising a first encrypted datagram and first key information, the first encrypted datagram being associated with a first component of the multi-media session, the first encrypted datagram containing content;

(B) determining a first key from the first key information; and

(C) decrypting the first encrypted datagram with the first key.

18. The method of claim 17, wherein (B) comprises:

(i) processing a corresponding datagram that contains the first key information, the corresponding datagram being included in a first keystream associated with the multi-media session.

19. The method of claim 17, further comprising:

(D) receiving a second encrypted datagram and second key information in the time slice burst, the second encrypted datagram being included in the first component of the multi-media session, the second datagram containing content;

(E) determining a second key from the second key information; and

(F) decrypting the second encrypted datagram with the second key.

20. The method of claim 18, further comprising:

(D) receiving a second encrypted datagram in the time slice burst, the second encrypted datagram being included in another component of the multi-media session, the second encrypted datagram containing content; and

(E) decrypting the second encrypted datagram with the first key.

21. The method of claim 18, further comprising:

(D) receiving a second datagram in the time slice burst, the second datagram being included in another of the plurality of media components, the second datagram not being encrypted.

22. The method of claim 18, further comprising:

(D) receiving a second encrypted datagram and an associated datagram in the time slice burst, the second encrypted datagram being included in another of the plurality of media components, the second encrypted datagram containing content, the associated datagram being included in the first keystream;

(E) determining a second key from the associated datagram; and

(F) decrypting the second encrypted datagram with the second key.

23. The method of claim 18, further comprising:

(D) receiving a second encrypted datagram and an associated datagram in the time slice burst, the second encrypted datagram being included in another of the plurality of media components, the second encrypted datagram containing content, the associated datagram being included in another keystream;

(E) determining a second key from the associated datagram; and

(F) decrypting the second encrypted datagram with the second key.

24. The method of claim 18, wherein the first keystream includes a subsequent key, the subsequent key being applied to decrypt the first component at a subsequent time.

25. The method of claim 18, wherein the first keystream includes a subsequent key, the subsequent key being applied to decrypt the first component within a subsequent time.

26. The method of claim 17, further comprising:

(D) decrypting the first key before performing (C).

27. The method of claim 17, wherein (A) through (C) are performed in the communications systems selected from the group consisting of a DVB-H system, a DVB-T system, an ATSC system, and an ISDB-T system.

28. The method of claim 17, wherein the first datagram comprises an IP packet.

29. The method of claim 17, wherein the first key comprises an IPSec key.

30. A computer-readable medium having computer-executable instructions for performing the steps recited in claim 17.

31. A computer-readable medium having computer-executable instructions for performing the steps recited in claim 18.

32. A computer-readable medium having computer-executable instructions for performing the steps recited in claim 19.

33. A method for transmitting data by a communications system during a multi-media session comprising a plurality of media components, comprising:

(A) encrypting a first datagram with a first key and including the first encrypted datagram in a first component of the multi-media session, the first datagram containing content;

(B) transmitting the first encrypted datagram in a time slice burst; and

(C) transmitting a corresponding datagram comprising the first key in the time slice burst, the corresponding datagram being included in the first component.

34. The method of claim 33, further comprising:

(D) encrypting a second datagram with a second key and including the second encrypted datagram in the first component;

(E) transmitting the second encrypted datagram in the time slice burst; and

(F) transmitting an associated datagram comprising the second key in the time slice burst, the associated datagram being included in the first component.

35. The method of claim 33, further comprising:

(D) encrypting a second datagram with the first key and including the second encrypted datagram in a second component of the multi-media session;

(E) transmitting the second encrypted datagram in the time slice burst.

36. The method of claim 33, further comprising:

(D) transmitting another datagram of another component in the time slice burst without encrypting the other datagram.

37. The method of claim 36, further comprising:

(E) encrypting a second datagram with the first key and including the second encrypted datagram in a second component of the multi-media session; and

(F) transmitting the second encrypted datagram in the time slice burst.

38. The method of claim 33, further comprising:

(D) encrypting a second datagram with a second key and including the second datagram in a second component of the multi-media session, the second datagram containing content;

(E) transmitting the second encrypted datagram in the time slice burst; and

(F) transmitting a different datagram, the second key being included in the different datagram, the different datagram being included in the second component.

39. A method for transmitting data during a multi-media session comprising a plurality of components, comprising:

(A) encrypting a first datagram with a first key and including the first datagram in a first component of the multi-media session, the first datagram containing content;

(B) transmitting the first encrypted datagram in a time slice burst;

(C) transmitting a corresponding datagram and including the first key in the corresponding datagram, the corresponding datagram being included in another component in the time slice burst;

(D) encrypting a second datagram with a second key and including the second datagram in the other component of the multi-media session, the second datagram containing content;

(E) transmitting the second encrypted datagram in the time slice burst; and

(F) transmitting an associated datagram in the time slice burst and including the second key in the associated datagram, the associated datagram being included in the first component.

40. A method for transmitting data during a multi-media session, comprising:

(A) encrypting a first datagram with a first key and including the first encrypted datagram in a first component of the multi-media session, the first datagram containing content;

(B) including the first key in the first datagram; and

(C) transmitting the first datagram in a time slice burst.

41. The method of claim 40, further comprising:

(D) encrypting a second datagram with the first key and including the second encrypted datagram in another component of the multi-media session, the second datagram containing content; and

(E) transmitting the second encrypted datagram in the time slice burst.

42. The method of claim 33, further comprising:

(D) transmitting a subsequent datagram that contains a subsequent key and including the subsequent datagram in the first component, the subsequent key being subsequently applied to encrypt the first component.

43. The method of claim 42, wherein the subsequent key is subsequently applied to encrypt another component.

44. The method of claim 33, wherein (A) through (C) are performed in the communications system selected from the group consisting of a DVB-H system, a DVB-T system, an ATSC system, and an ISDB-T system.

45. The method of claim 33, wherein the first datagram comprises an IP packet.

46. The method of claim 33, wherein the first key comprises an IPSec key.

47. A computer-readable medium having computer-executable instructions for performing the steps recited in claim 33.

48. A method for receiving data by a communications system during a multi-media session comprising a plurality of media components, comprising:

(A) receiving a first encrypted datagram and a corresponding datagram in a time slice burst, the first encrypted datagram and the corresponding datagram being

included in a first component of the multi-media session, the first encrypted datagram containing content;

(B) determining a first key from the corresponding datagram; and

(C) decrypting the first encrypted datagram with the first key.

49. The method of claim 48, further comprising:

(D) receiving a second encrypted datagram and a different datagram in the time slice burst, the second encrypted datagram being included in the first component, the second encrypted datagram containing content;

(E) determining a second key from the different datagram; and

(F) decrypting the second encrypted datagram with the second key.

50. The method of claim 48, further comprising:

(D) receiving a second encrypted datagram in the time slice burst, the second encrypted datagram being included in another component of the multi-media session, the second encrypted datagram containing content; and

(E) decrypting the second encrypted datagram with the first key.

51. The method of claim 48, further comprising:

(D) receiving a second datagram in the time slice burst, the second datagram being included in another component of the multi-media session, the second datagram not being encrypted.

52. The method of claim 51, further comprising:

(E) receiving a third datagram in the time slice burst, the third datagram being included in an additional component of the multi-media session, the third datagram containing content; and

(F) decrypting the third datagram with the first key.

53. The method of claim 48, further comprising:

(D) receiving a second encrypted datagram and a different datagram in the time slice burst, the second encrypted datagram and the different datagram being included in another component of the multi-media session, the second encrypted datagram containing content;

(E) determining a second key from the different datagram; and

(F) decrypting the second encrypted datagram with the second key.

54. A method for receiving data by a communications system during a multi-media session, comprising:

(A) receiving a first encrypted datagram, a second encrypted datagram, a third datagram, and a fourth datagram in a time slice burst, the first encrypted datagram and fourth datagram being included in a first component of the multi-media session, the second encrypted datagram and the third datagram being included in a second component of the multi-media session, the first encrypted datagram and the second encrypted datagram containing multi-media content;

(B) determining a first key from third datagram;

(C) decrypting the first encrypted datagram with the first key;

(D) determining a second key from the fourth datagram; and

(E) decrypting the second encrypted datagram with the second key.

55. A method for receiving data during a multi-media session comprising a plurality of media components, comprising:

(A) receiving a first datagram in a time slice burst, the first datagram being included in a first component of the multi-media session, the first datagram containing content;

(B) determining a first key from the first datagram; and

(C) decrypting the first datagram with the first key.

56. The method of claim 55, further comprising:

(D) receiving a second encrypted datagram in the time slice burst, the second encrypted datagram being included in another component, the second encrypted datagram containing content; and

(E) decrypting the second encrypted datagram with the first key.

57. The method of claim 48, further comprising:

(D) receiving a subsequent datagram that contains a subsequent key, the subsequent datagram being included in the first component, and using the subsequent key to decrypt of the first component.

58. The method of claim 57, further comprising:

(E) using the subsequent key to decrypt a second component.

59. A computer-readable medium having computer-executable instructions for performing the steps recited in claim 48.

60. The method of claim 48, wherein (A) through (C) are performed in the communications system selected from the group consisting of a DVB-H system, a DVB-T system, an ATSC system, and an ISDB-T system.

61. The method of claim 48, wherein the first datagram comprises an IP packet.

62. The method of claim 48, wherein the first key comprises an IPSec key.

63. An apparatus for transmitting data during a multi-media session comprising a plurality of media components, comprising:

a first interface that obtains a content datagram encrypted with a corresponding key, the encrypted content datagram containing content during the multi-media session;

a second interface that obtains the corresponding key;

a transmission interface that includes the encrypted content datagram in a time slice burst; and

a processor that instructs the transmission interface to include key information with the encrypted content datagram in the time slice burst, the key information containing the corresponding key.

64. The apparatus of claim 63, wherein the processor further forms a keystream that is separate from the plurality of media components, and wherein the keystream includes the key information.

65. The apparatus of claim 63, wherein the processor further includes the key information in a same component as the encrypted content datagram.

66. The apparatus of claim 63, wherein the processor further includes the key information in a different component as the encrypted content datagram.

67. The apparatus of claim 63, further comprising:

a radio module that modulates a wireless signal with the time slice burst.

68. An apparatus for transmitting data during a multi-media session comprising a plurality of media components, comprising:

means for encrypting a plurality of content datagrams, each content datagram being encrypted with an associated key, each associated key being included in key information; and

means for transmitting the plurality of encrypted content datagrams in a time slice burst along with the key information.

69. The apparatus of claim 68, further comprising:

means for encrypting the key information.

70. The apparatus of claim 68, further comprising:

means for obtaining the plurality of content datagrams corresponding to a plurality of components, each component being associated with a type of content during the multi-media session.

71. An apparatus for receiving data during a multi-media session, comprising:

means for receiving a time slice burst during a multi-media session, the time slice burst containing a plurality of content datagrams and key information, each content datagram being encrypted by an associated key included in the key information;

means for determining the associated key for each said content datagram; and

means for decrypting each said content datagram with the associated key.

72. The apparatus of claim 71, wherein the means for determining the associated key comprises:

means for decrypting the associated key before performing the means for decrypting each said content datagram.

73. The apparatus of claim 71, further comprising:

means for separating the plurality of content datagrams for each corresponding component, each said corresponding component being associated with a type of content during the multi-media session.

74. A method for providing data by a communications system during a multi-media session comprising a plurality of media components, comprising:

(A) encrypting a first datagram with a first key and including the first encrypted datagram in a first component of the multi-media session, the first datagram containing content;

(B) transmitting the first encrypted datagram in a time slice burst;

(C) transmitting first key information in the time slice burst, wherein the first key information contains the first key;

(D) receiving the time slice burst with the first encrypted datagram and the first key information;

(E) determining the first key from the first key information; and

(F) decrypting the first encrypted datagram with the first key.

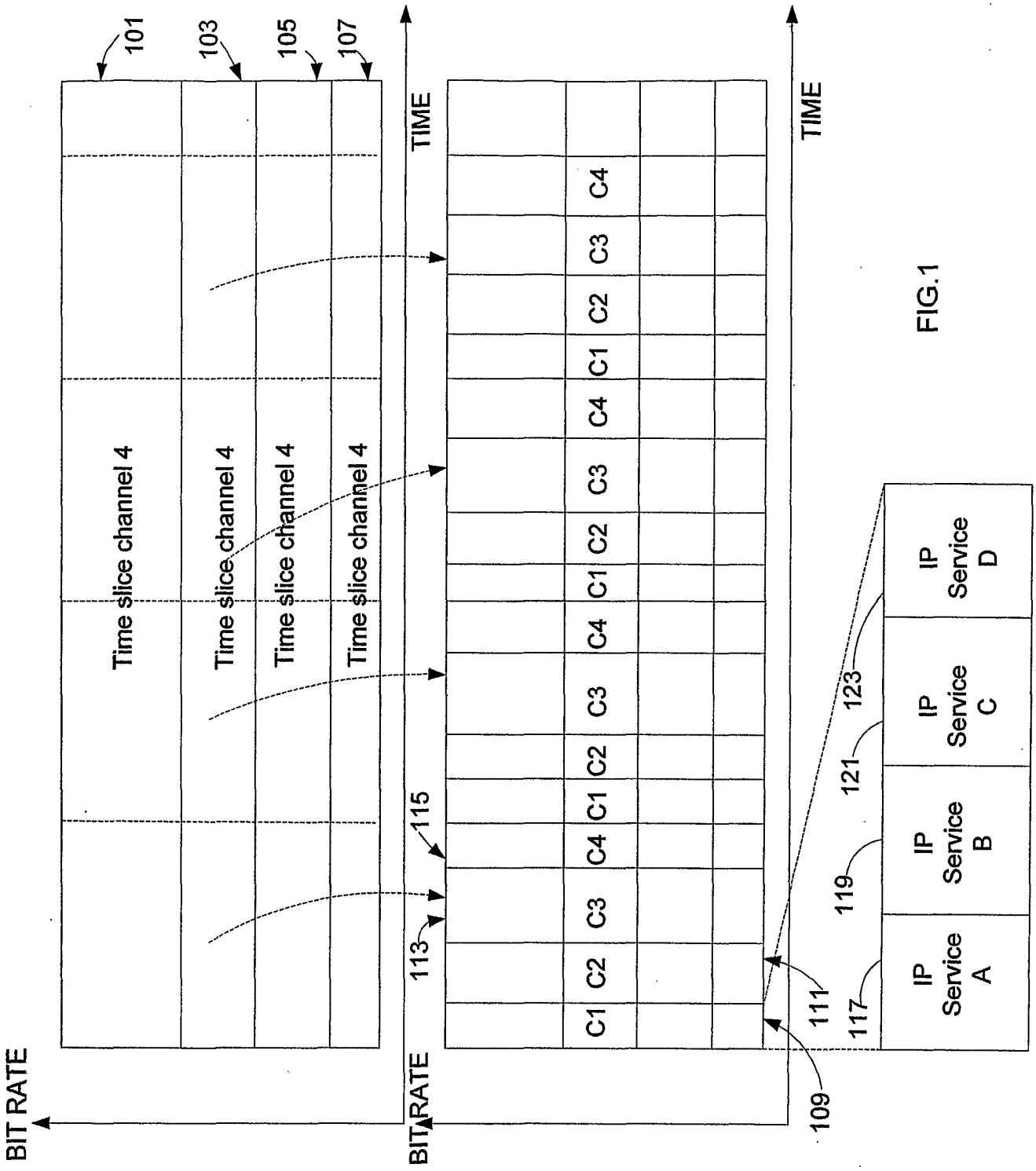

101
103
105
107
Time slice channel 4
Time slice channel 4
Time slice channel 4
Time slice channel 4
TIME
BIT RATE
115
113
C1 C2 C3 C4 C1 C2 C3 C4 C1 C2 C3 C4
TIME
BIT RATE
109
111
117
119
121
123
IP Service A
IP Service B
IP Service C
IP Service D

FIG.1

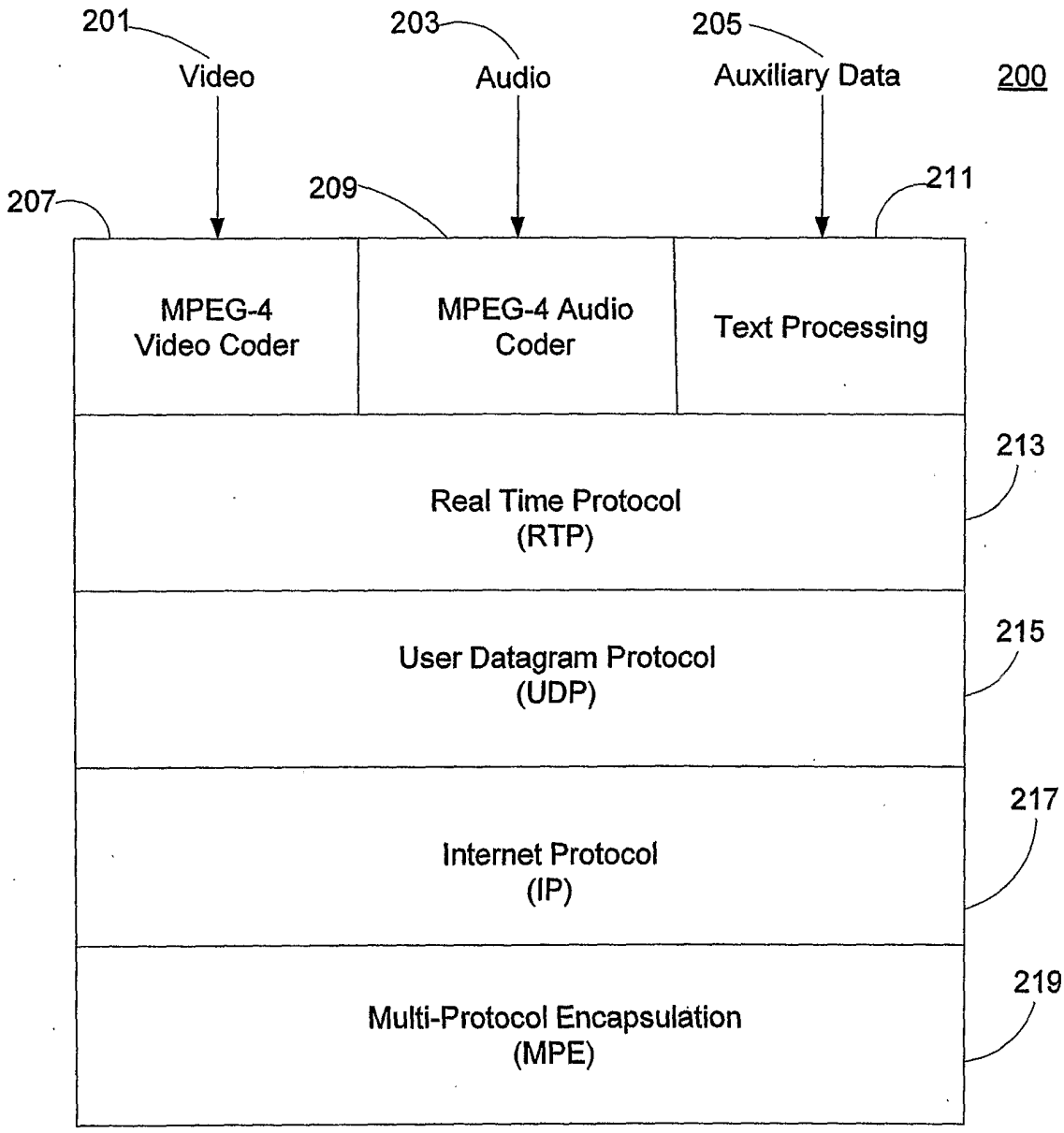

201
Video
203
Audio
205
Auxiliary Data
200
207
209
211
MPEG-4 Video Coder
MPEG-4 Audio Coder
Text Processing
213
Real Time Protocol (RTP)
215
User Datagram Protocol (UDP)
217
Internet Protocol (IP)
219
Multi-Protocol Encapsulation (MPE)

FIG. 2

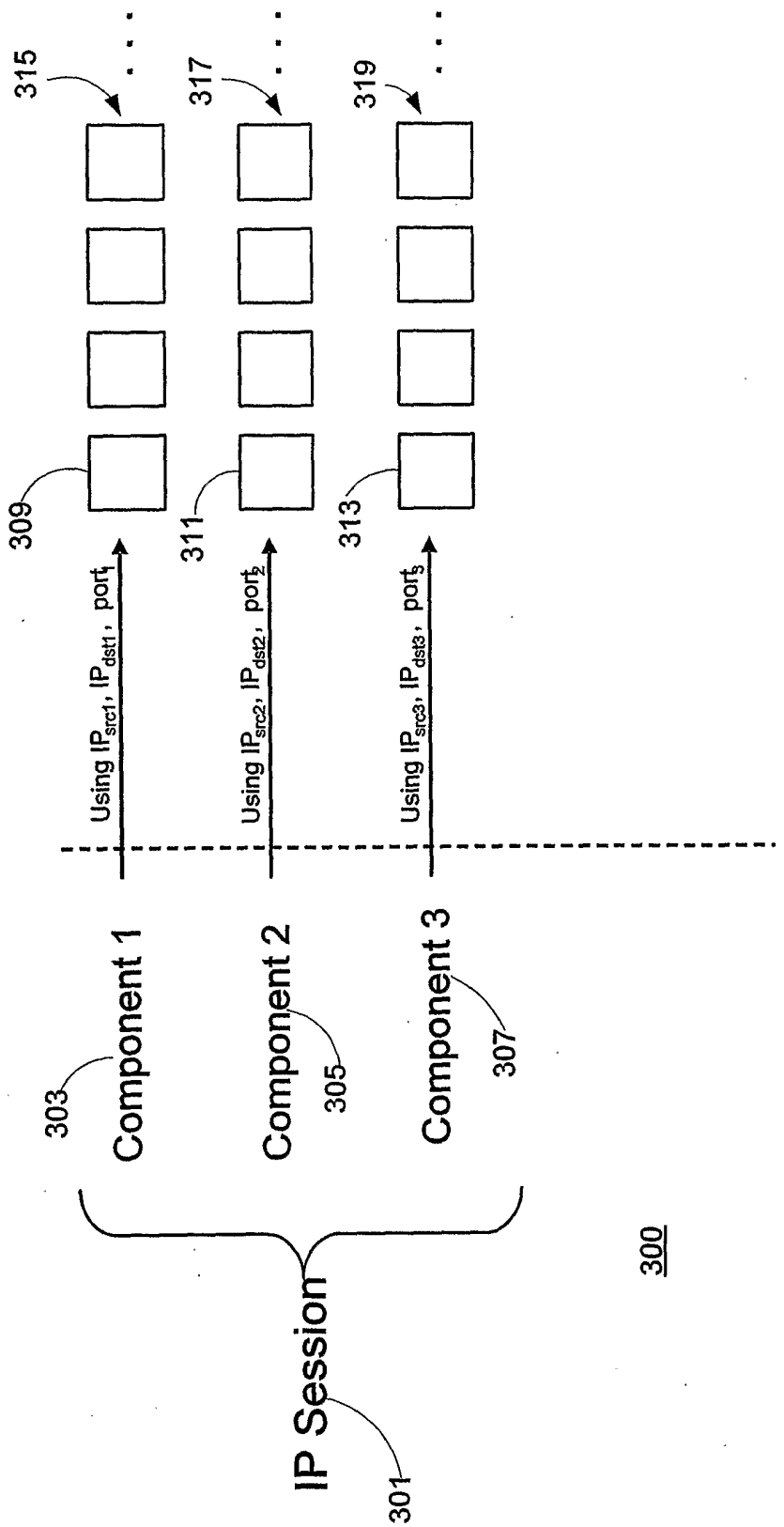

315
317
319
309
311
313
Using IP_{src1}, IP_{dst1}, $port_1$
Using IP_{src2}, IP_{dst2}, $port_2$
Using IP_{src3}, IP_{dst3}, $port_3$
Transmitted as a stream of IP packets
303
Component 1
305
Component 2
307
Component 3
IP Session
301
300

FIG. 3

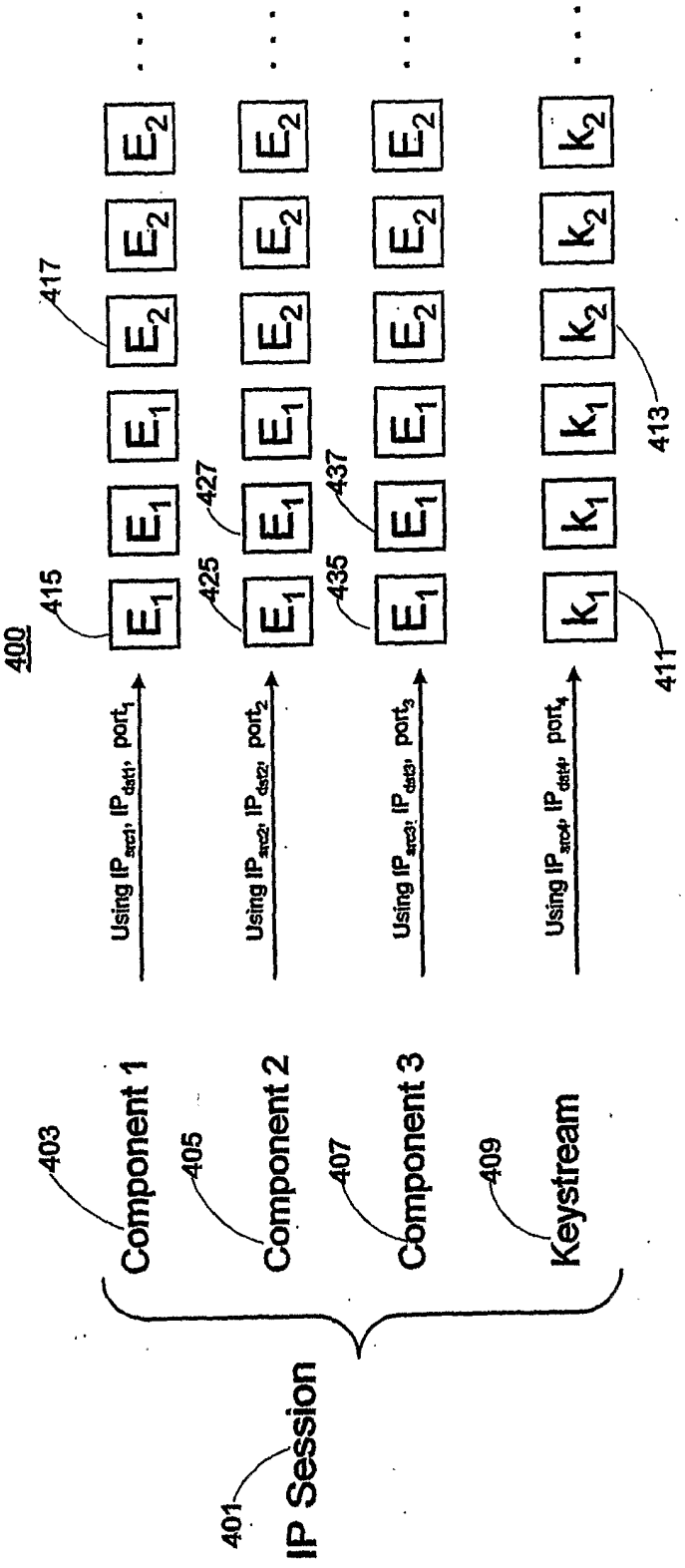

400
401
IP Session
403
Component 1
405
Component 2
407
Component 3
409
Keystream
411
413
415
417
425
427
435
437
Using IP_{src1}, IP_{dst1}, $port_1$
Using IP_{src2}, IP_{dst2}, $port_2$
Using IP_{src3}, IP_{dst3}, $port_3$
Using IP_{src4}, IP_{dst4}, $port_4$
E_1
E_2
k_1
k_2

FIG. 4

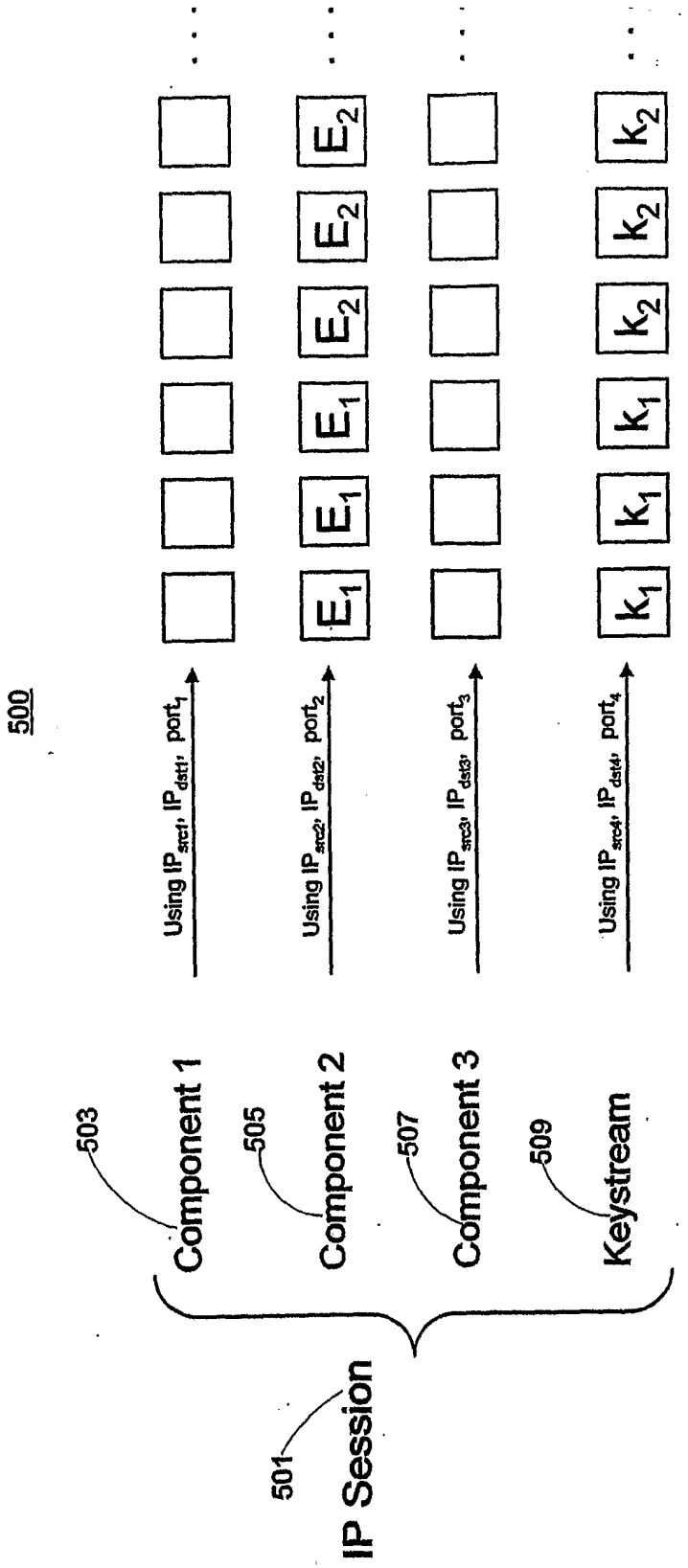

500
IP Session
501
Component 1
503
Component 2
505
Component 3
507
Keystream
509
Using IP_src1, IP_dst1, port_1
Using IP_src2, IP_dst2, port_2
Using IP_src3, IP_dst3, port_3
Using IP_src4, IP_dst4, port_4
E_1
E_2
k_1
k_2

FIG. 5

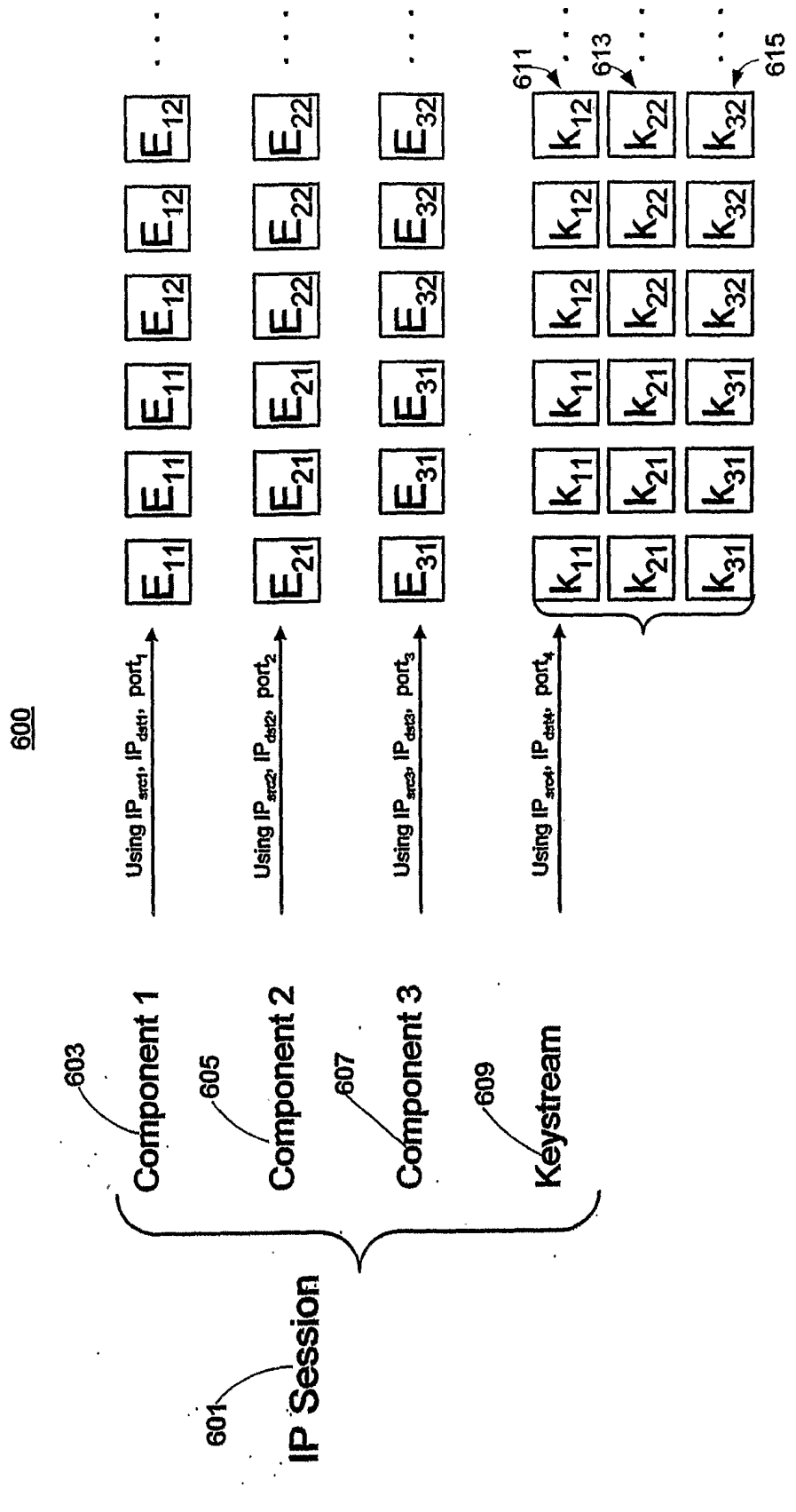

600
601
IP Session
603
Component 1
605
Component 2
607
Component 3
609
Keystream
611
613
615
Using IP_src1, IP_dst1, port_1
Using IP_src2, IP_dst2, port_2
Using IP_src3, IP_dst3, port_3
Using IP_src4, IP_dst4, port_4
E11 E11 E11 E12 E12 E12 E12 ...
E21 E21 E21 E22 E22 E22 E22 ...
E31 E31 E31 E32 E32 E32 E32 ...
K11 K11 K11 K12 K12 K12 K12 ...
K21 K21 K21 K22 K22 K22 K22 ...
K31 K31 K31 K32 K32 K32 K32 ...

FIG. 6

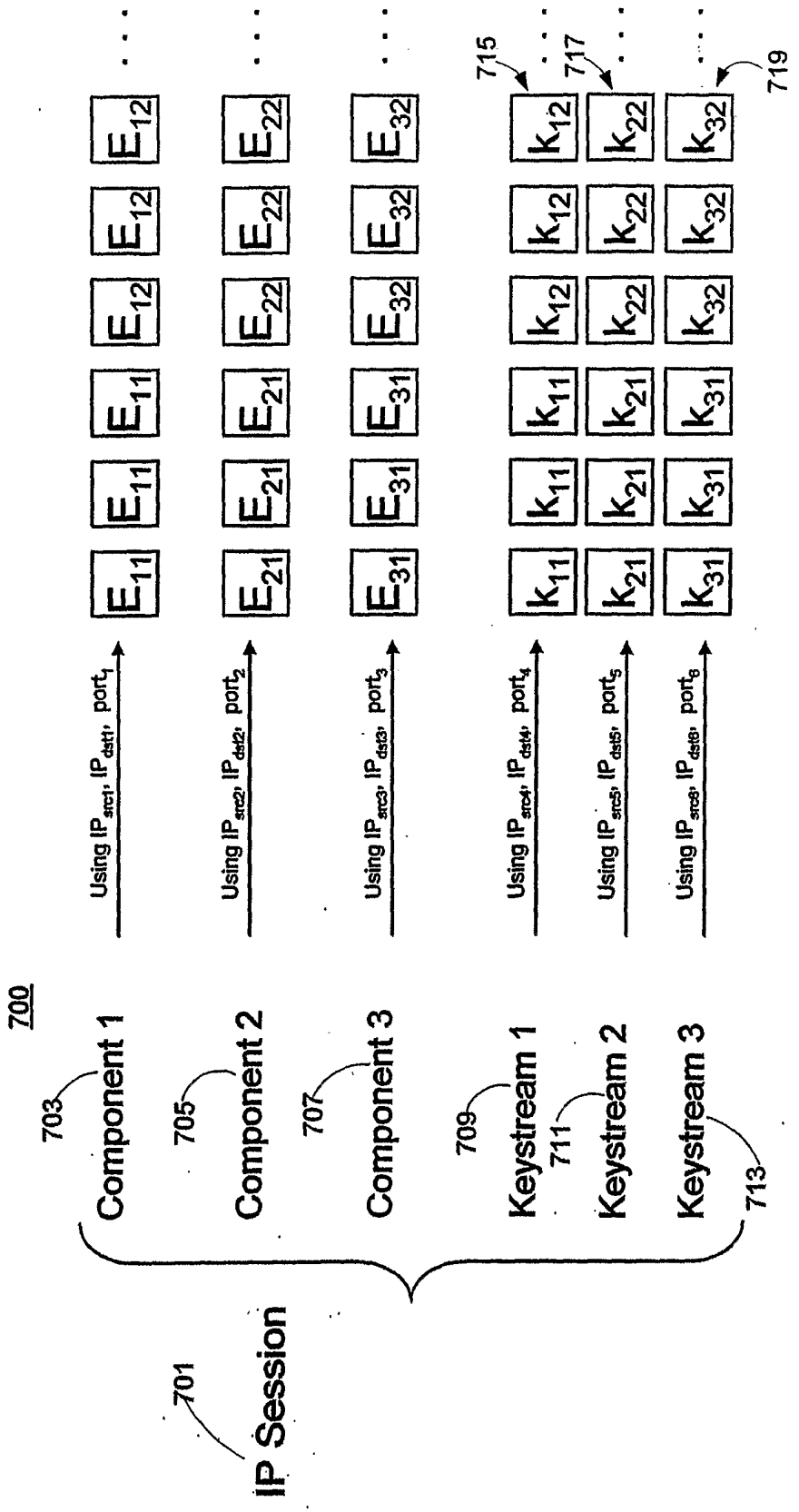

700
IP Session
701
Component 1
703
Component 2
705
Component 3
707
Keystream 1
709
Keystream 2
711
Keystream 3
713
715
717
719
Using IP_src1, IP_dst1, port_1
Using IP_src2, IP_dst2, port_2
Using IP_src3, IP_dst3, port_3
Using IP_src4, IP_dst4, port_4
Using IP_src5, IP_dst5, port_5
Using IP_src6, IP_dst6, port_6
E11 E11 E11 E12 E12 E12 . . .
E21 E21 E21 E22 E22 E22 . . .
E31 E31 E31 E32 E32 E32 . . .
K11 K11 K11 K12 K12 K12 . . .
K21 K21 K21 K22 K22 K22 . . .
K31 K31 K31 K32 K32 K32 . . .

FIG. 7

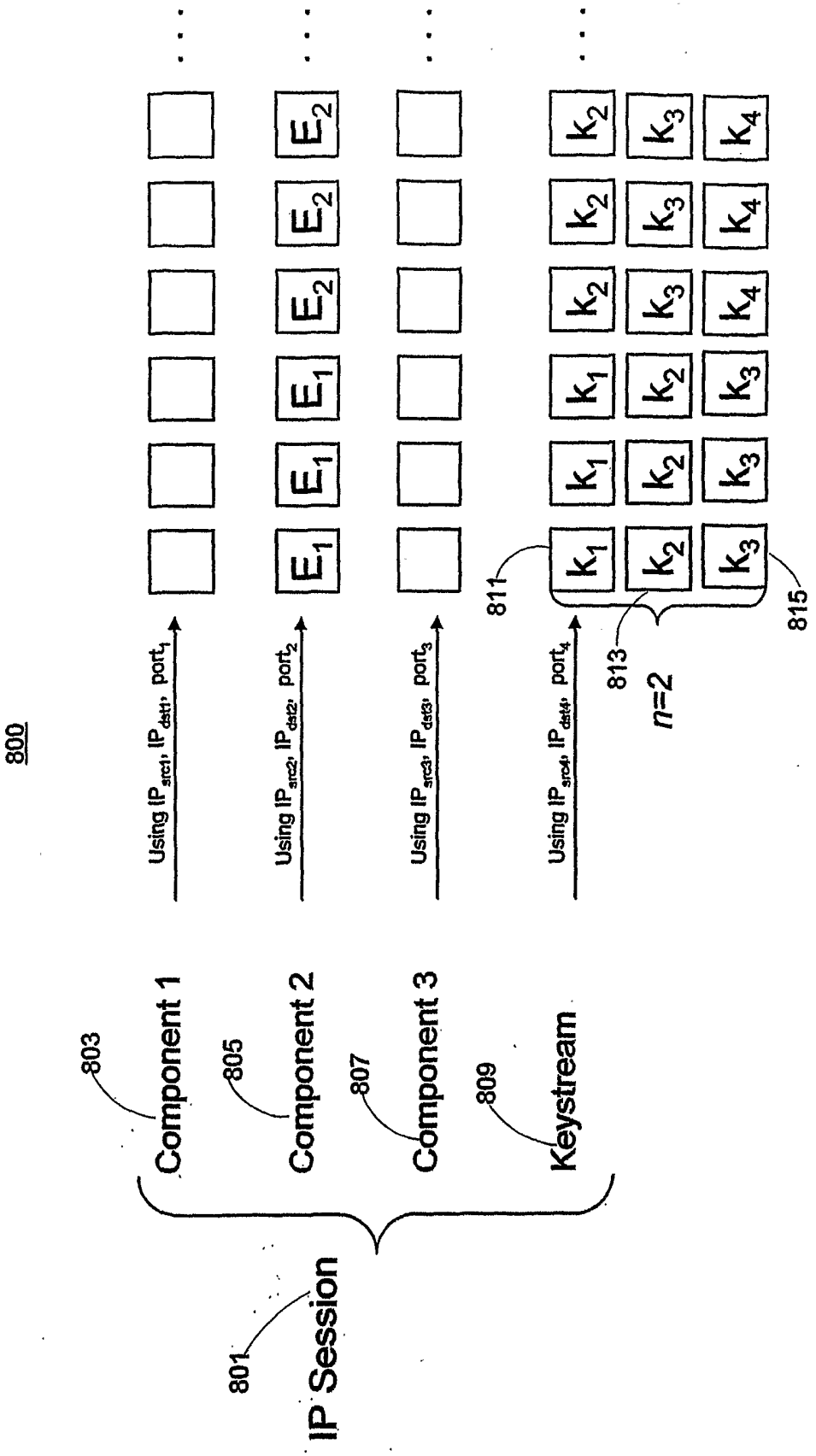

800
IP Session
801
Component 1
803
Component 2
805
Component 3
807
Keystream
809
Using IP_{src1}, IP_{dst1}, $port_1$
Using IP_{src2}, IP_{dst2}, $port_2$
Using IP_{src3}, IP_{dst3}, $port_3$
Using IP_{src4}, IP_{dst4}, $port_4$
E_1
E_2
k_1
k_2
k_3
k_4
811
813
815
n=2

Figure 8

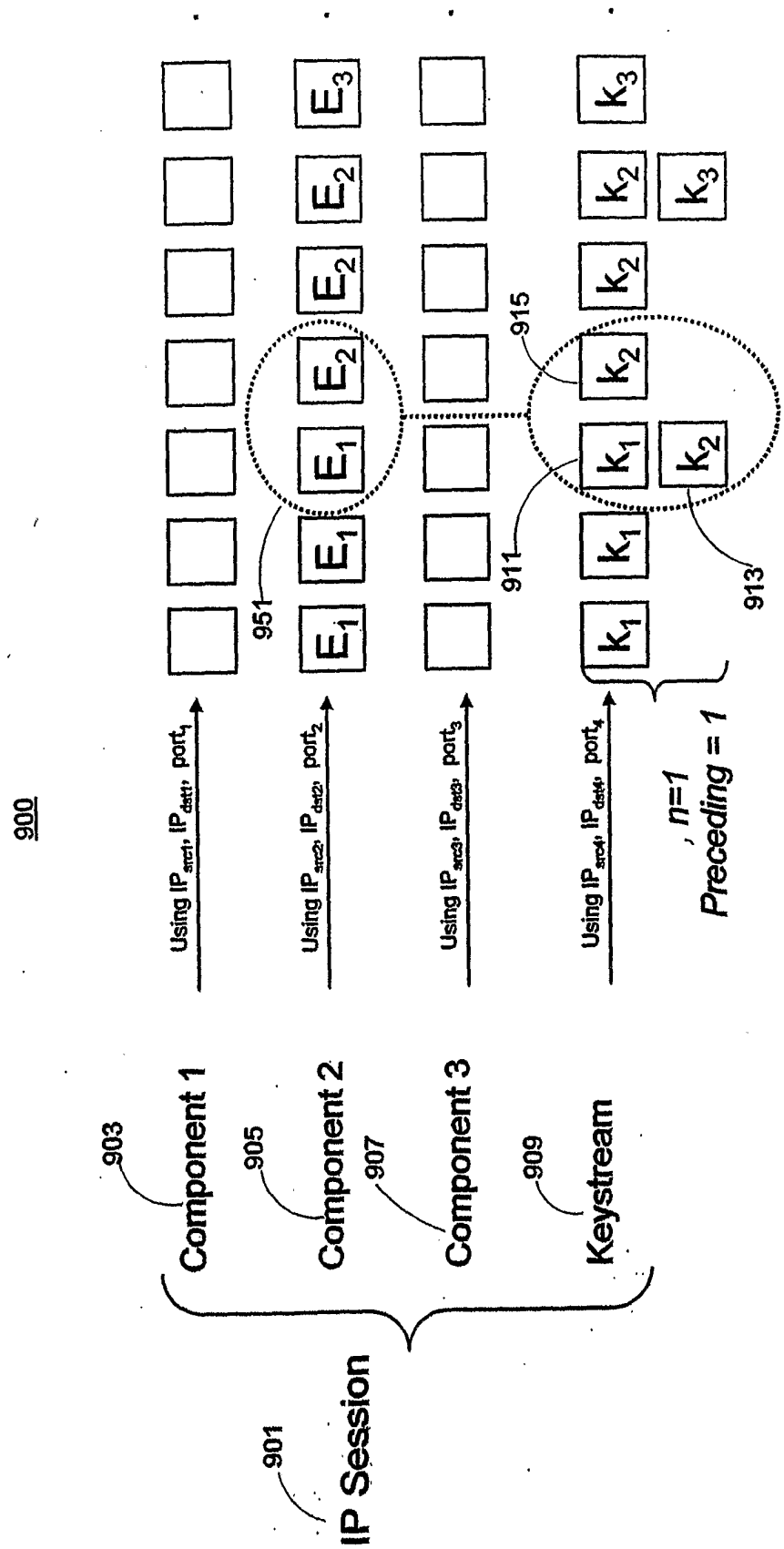

900
IP Session
901
Component 1
903
Component 2
905
Component 3
907
Keystream
909
Using IP_src1, IP_dst1, port_1
Using IP_src2, IP_dst2, port_2
Using IP_src3, IP_dst3, port_3
Using IP_src4, IP_dst4, port_4
951
911
913
915
n=1
Preceding = 1

FIG. 9

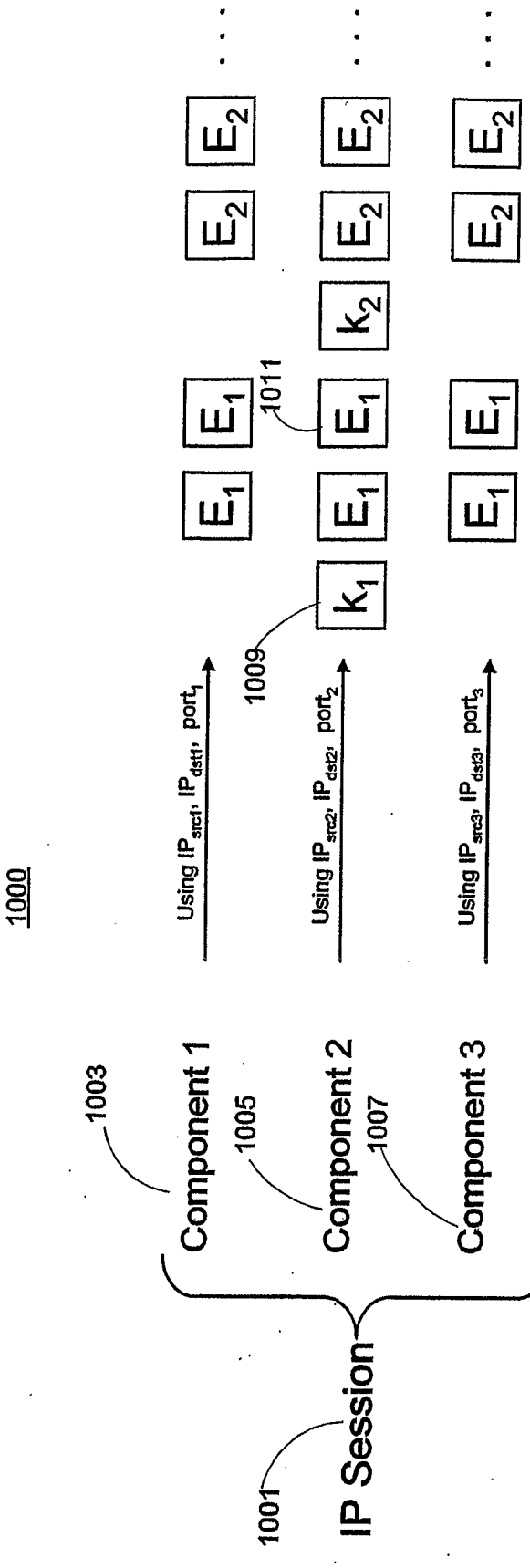

1000
1001
IP Session
1003
Component 1
1005
Component 2
1007
Component 3
Using IP_{src1}, IP_{dst1}, $port_1$
Using IP_{src2}, IP_{dst2}, $port_2$
Using IP_{src3}, IP_{dst3}, $port_3$
1009
1011
k_1
k_2
E_1
E_2

FIG. 10

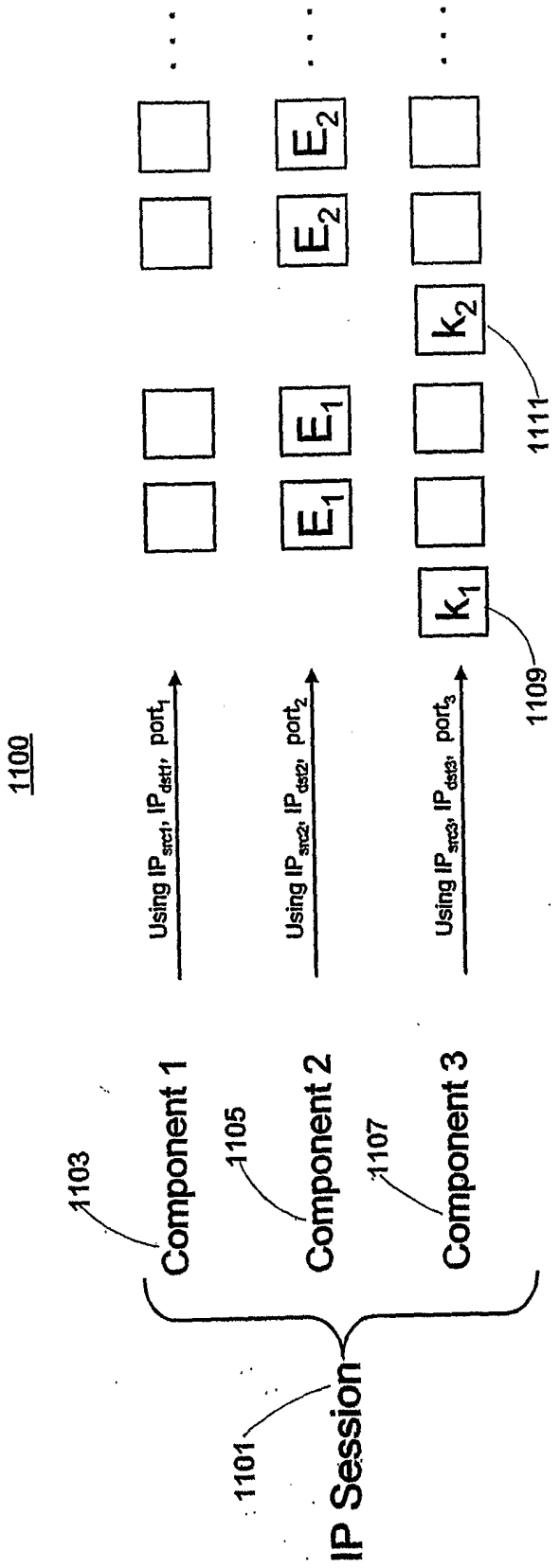

1100
IP Session
1101
Component 1
1103
Component 2
1105
Component 3
1107
Using IP$_{src1}$, IP$_{dst1}$, port$_1$
Using IP$_{src2}$, IP$_{dst2}$, port$_2$
Using IP$_{src3}$, IP$_{dst3}$, port$_3$
k_1
1109
k_2
1111
E_1
E_2

FIG. 11

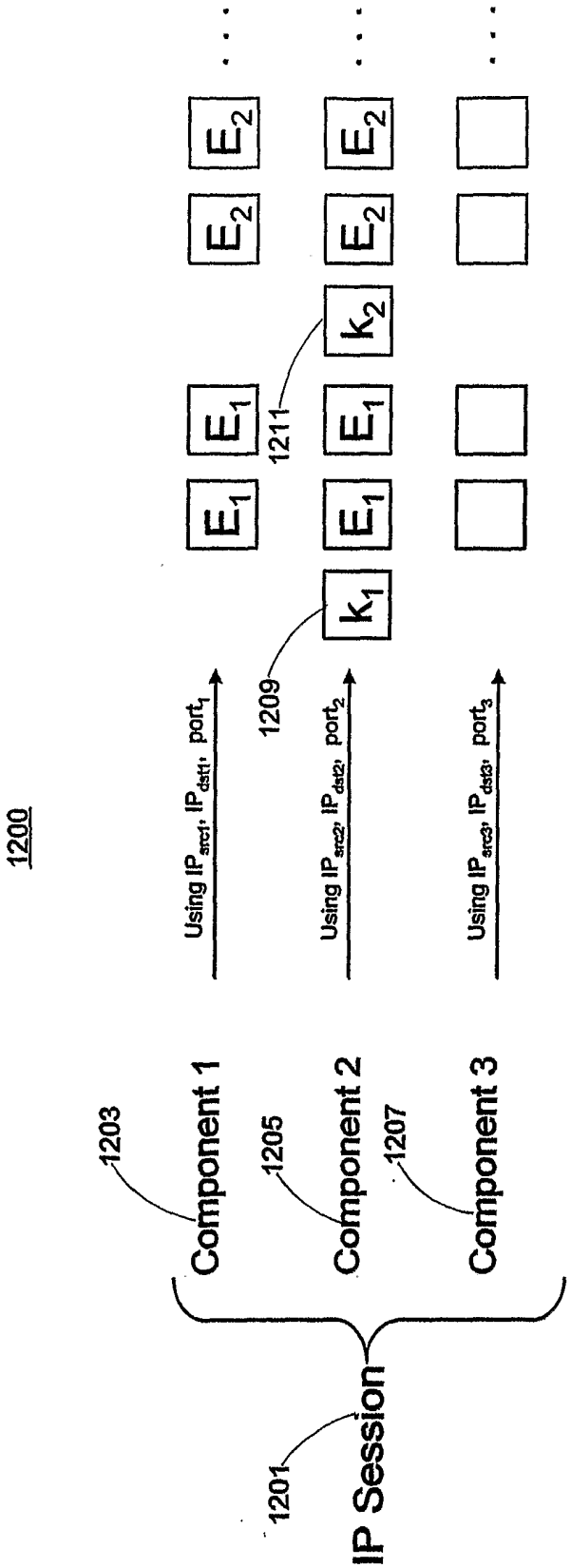

1200
IP Session
1201
Component 1
1203
Component 2
1205
Component 3
1207
Using IP_src1, IP_dst1, port_1
Using IP_src2, IP_dst2, port_2
Using IP_src3, IP_dst3, port_3
1209
1211
E_1
E_2
k_1
k_2

FIG. 12

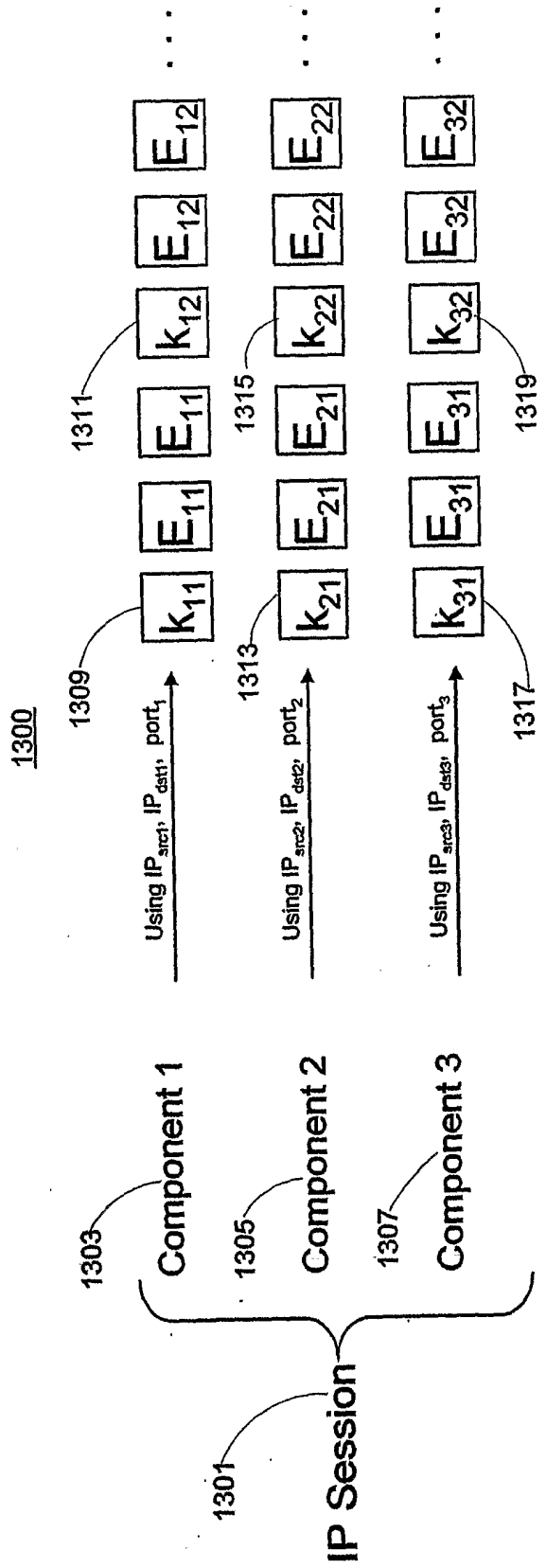

1300
IP Session
1301
Component 1
1303
Component 2
1305
Component 3
1307
1309
1311
1313
1315
1317
1319
Using IP_src1, IP_dst1, port_1
Using IP_src2, IP_dst2, port_2
Using IP_src3, IP_dst3, port_3
k11
k21
k31
k12
k22
k32
E11
E21
E31
E12
E22
E32

FIG. 13

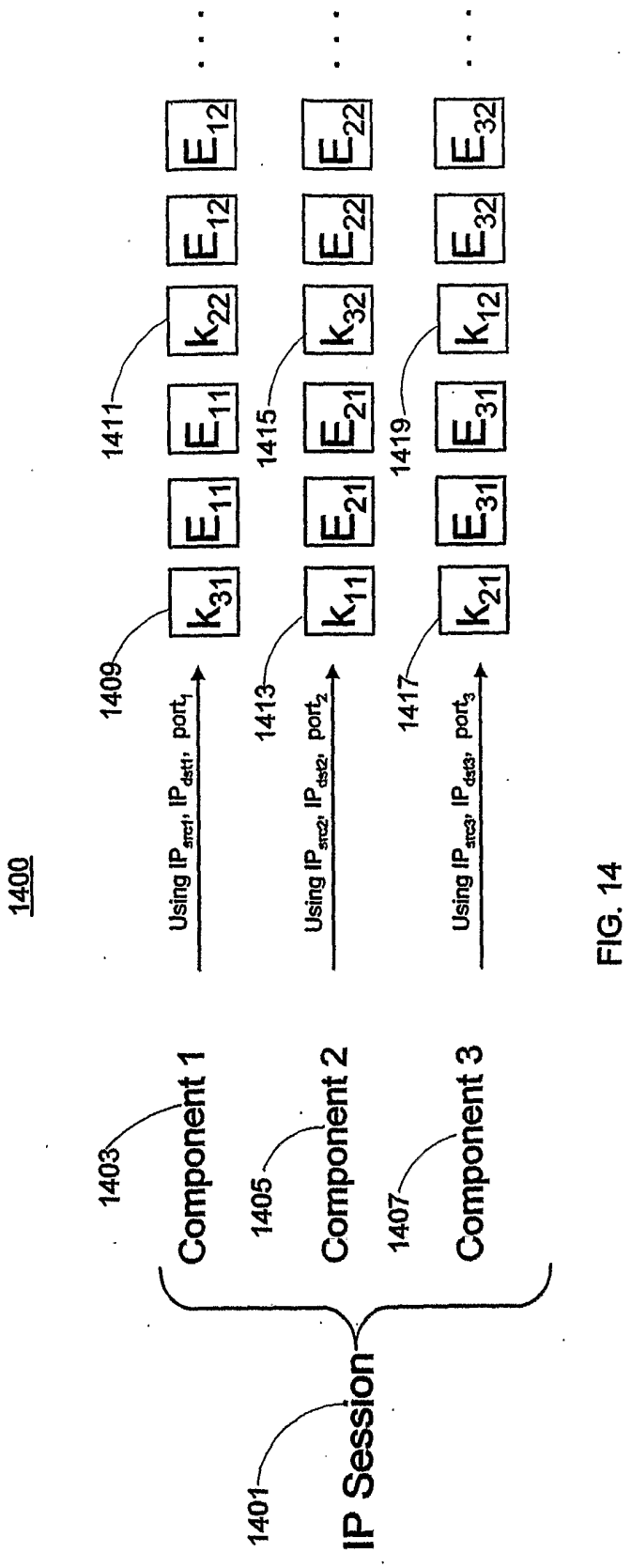

1400
IP Session
1401
Component 1
1403
Component 2
1405
Component 3
1407
Using IP_{src1}, IP_{dst1}, $port_1$
1409
Using IP_{src2}, IP_{dst2}, $port_2$
1413
Using IP_{src3}, IP_{dst3}, $port_3$
1417
k_{31}
E_{11}
E_{12}
k_{22}
1411
k_{11}
E_{21}
E_{22}
k_{32}
1415
k_{21}
E_{31}
E_{32}
k_{12}
1419

FIG. 14

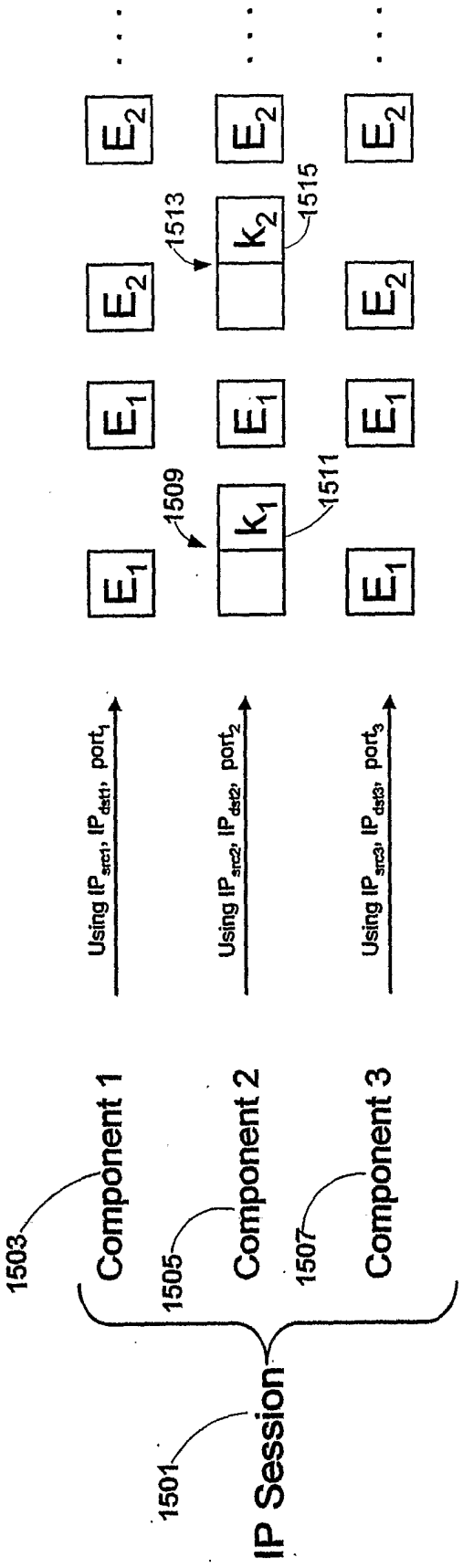

1500
IP Session
1501
Component 1
1503
Component 2
1505
Component 3
1507
Using IP_{src1}, IP_{dst1}, $port_1$
Using IP_{src2}, IP_{dst2}, $port_2$
Using IP_{src3}, IP_{dst3}, $port_3$
E_1
E_2
k_1
k_2
1509
1511
1513
1515

FIG. 15

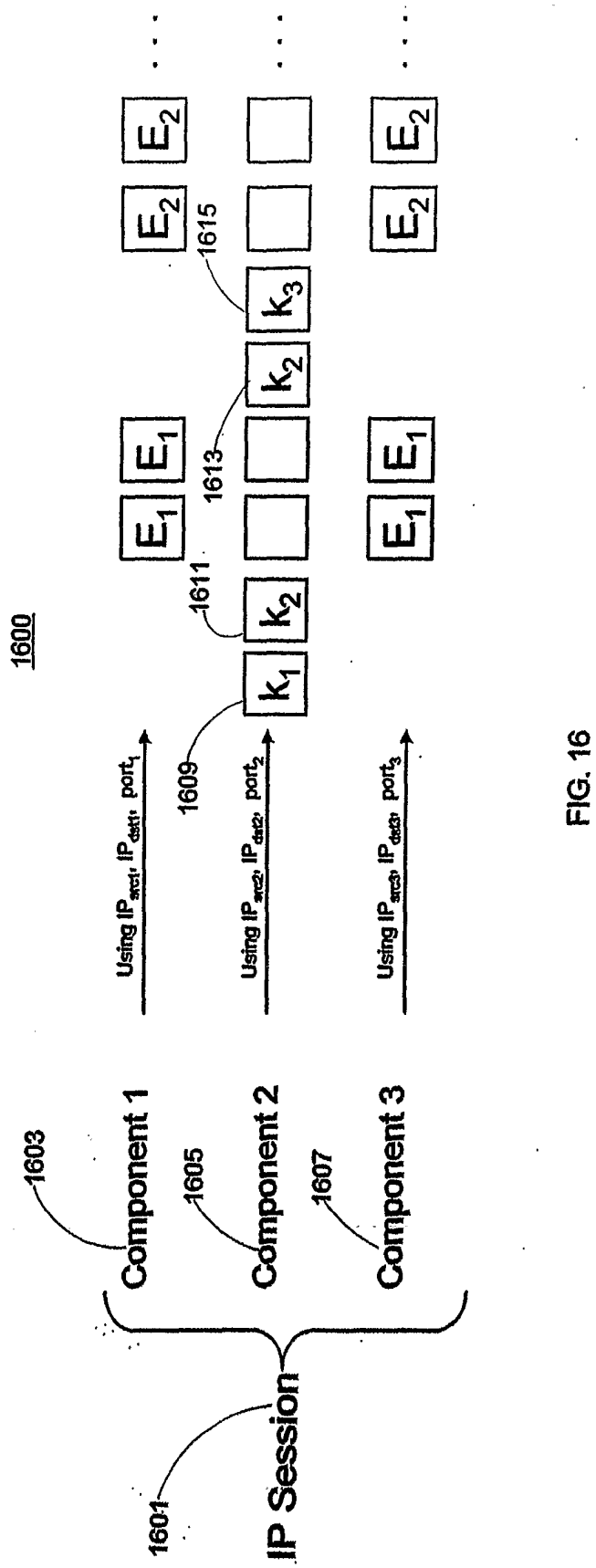

1600
1601
IP Session
1603
Component 1
1605
Component 2
1607
Component 3
Using IP_{src1}, IP_{dst1}, $port_1$
Using IP_{src2}, IP_{dst2}, $port_2$
Using IP_{src3}, IP_{dst3}, $port_3$
1609
1611
1613
1615
k_1
k_2
k_3
E_1
E_2

FIG. 16

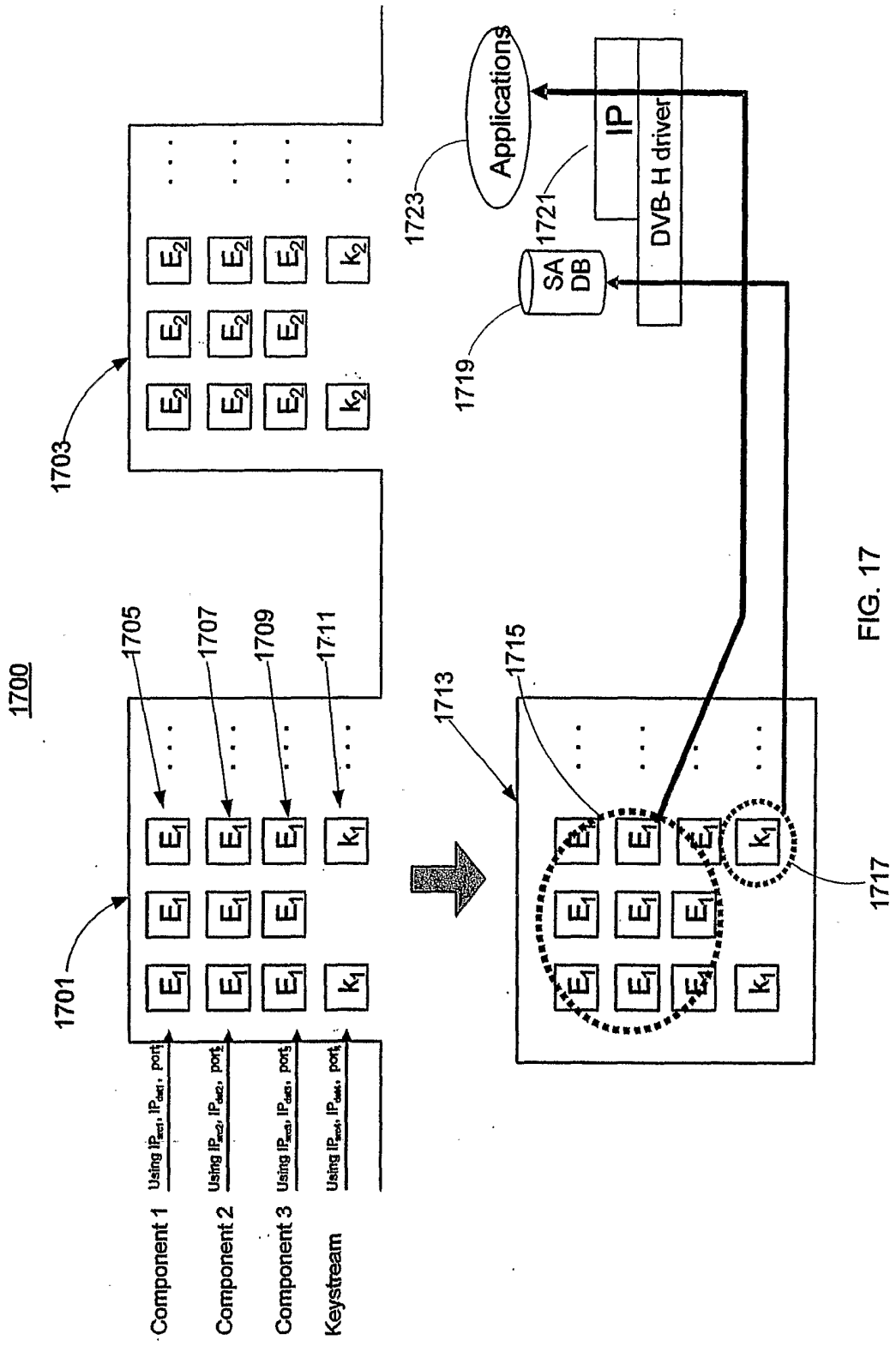

1700
1701
1703
1705
1707
1709
1711
1713
1715
1717
1719
1721
1723
Component 1
Component 2
Component 3
Keystream
Applications
IP
DVB-H driver
SA DB

FIG. 17

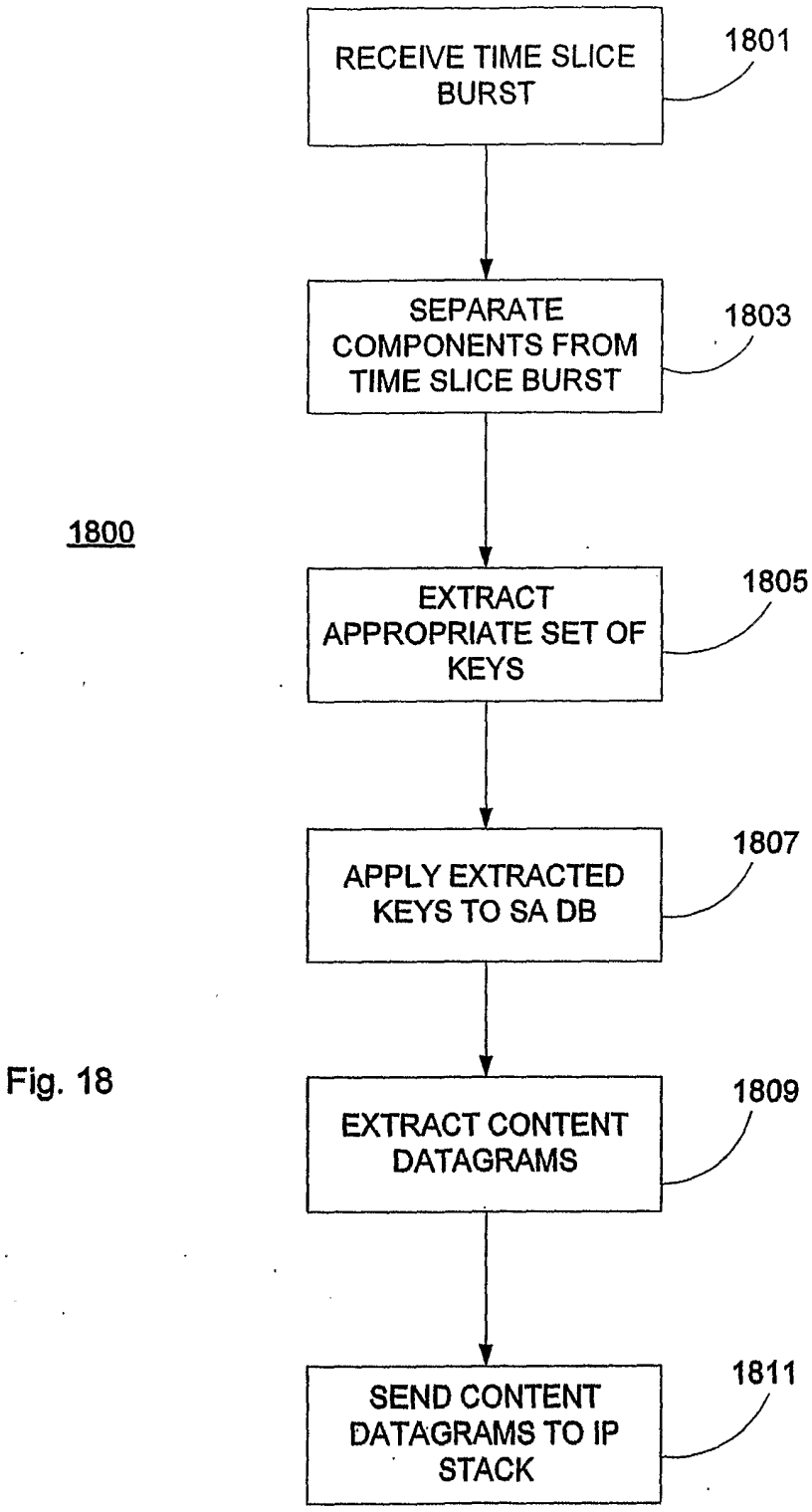

1800
RECEIVE TIME SLICE BURST
1801
SEPARATE COMPONENTS FROM TIME SLICE BURST
1803
EXTRACT APPROPRIATE SET OF KEYS
1805
APPLY EXTRACTED KEYS TO SA DB
1807
EXTRACT CONTENT DATAGRAMS
1809
SEND CONTENT DATAGRAMS TO IP STACK
1811

Fig. 18

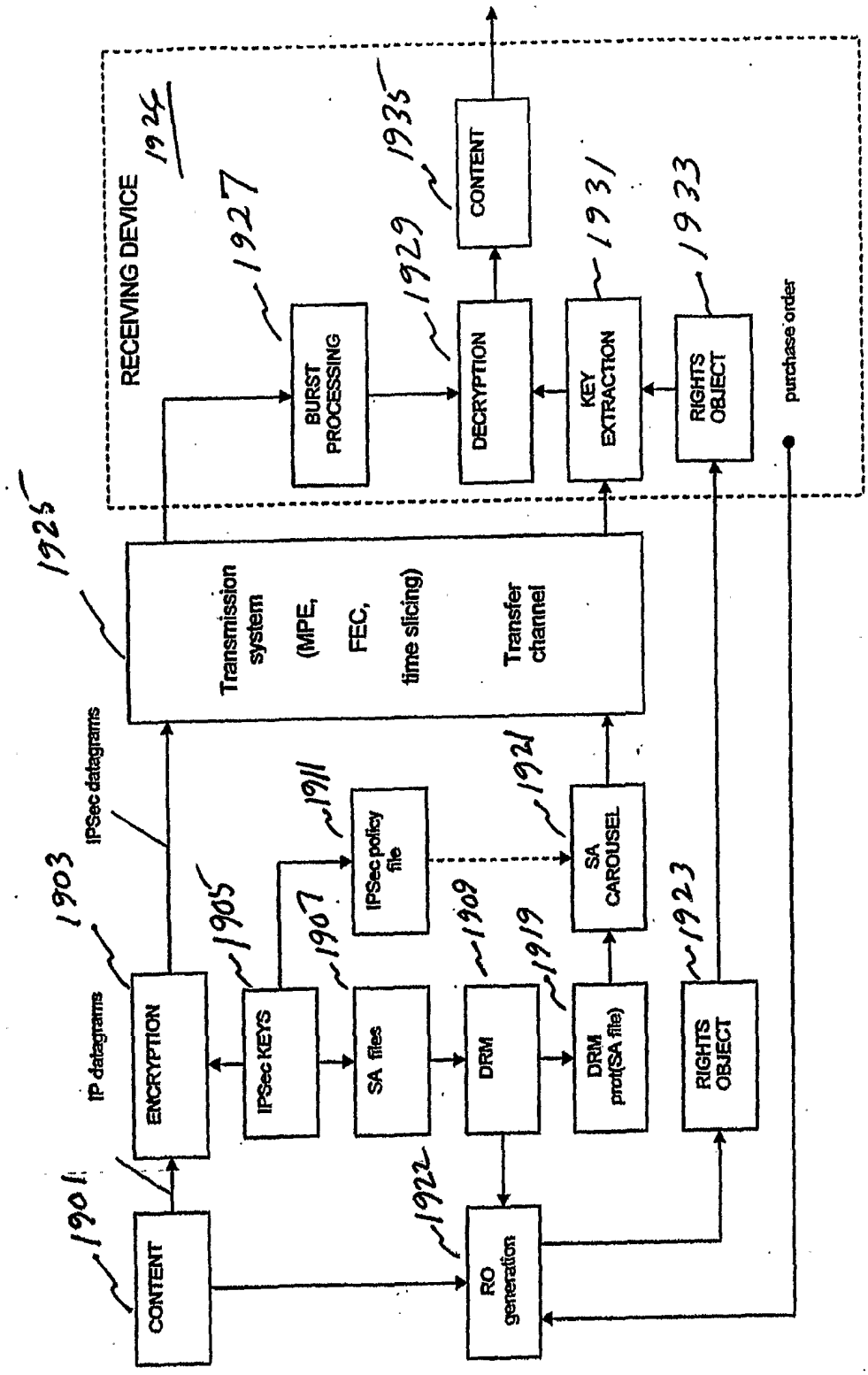


FIG. 19 (Prior Art)

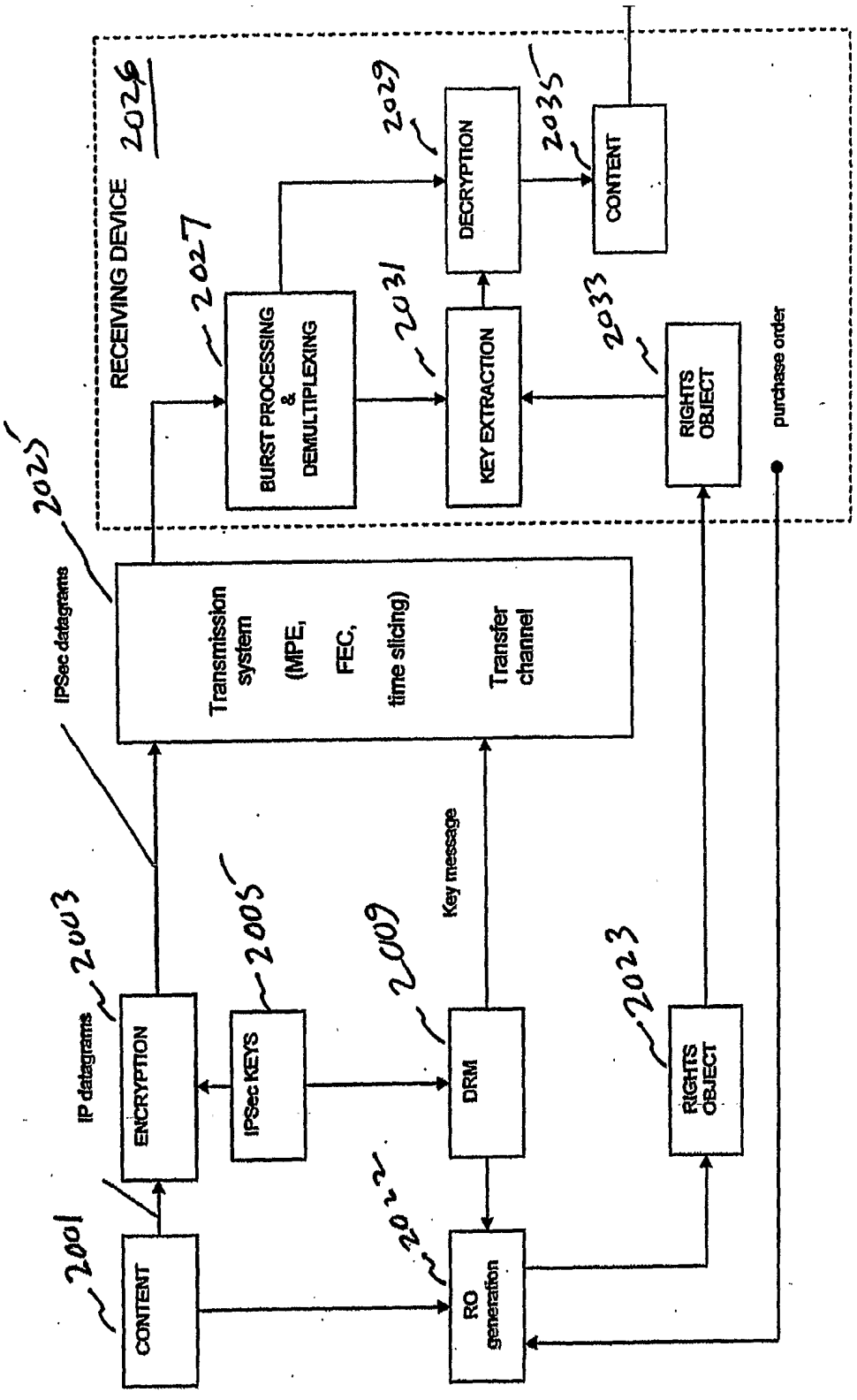

RECEIVING DEVICE
2026
2029
2035
2027
2031
2033
2025
DECRYPTION
CONTENT
BURST PROCESSING & DEMULTIPLEXING
KEY EXTRACTION
RIGHTS OBJECT
purchase order
IPSec datagrams
Transmission system (MPE, FEC, time slicing)
Transfer channel
2003
2005
2009
Key message
2023
IP datagrams
ENCRYPTION
IPSec KEYS
DRM
RIGHTS OBJECT
2001
2007
CONTENT
RO generation
2000

FIG. 20

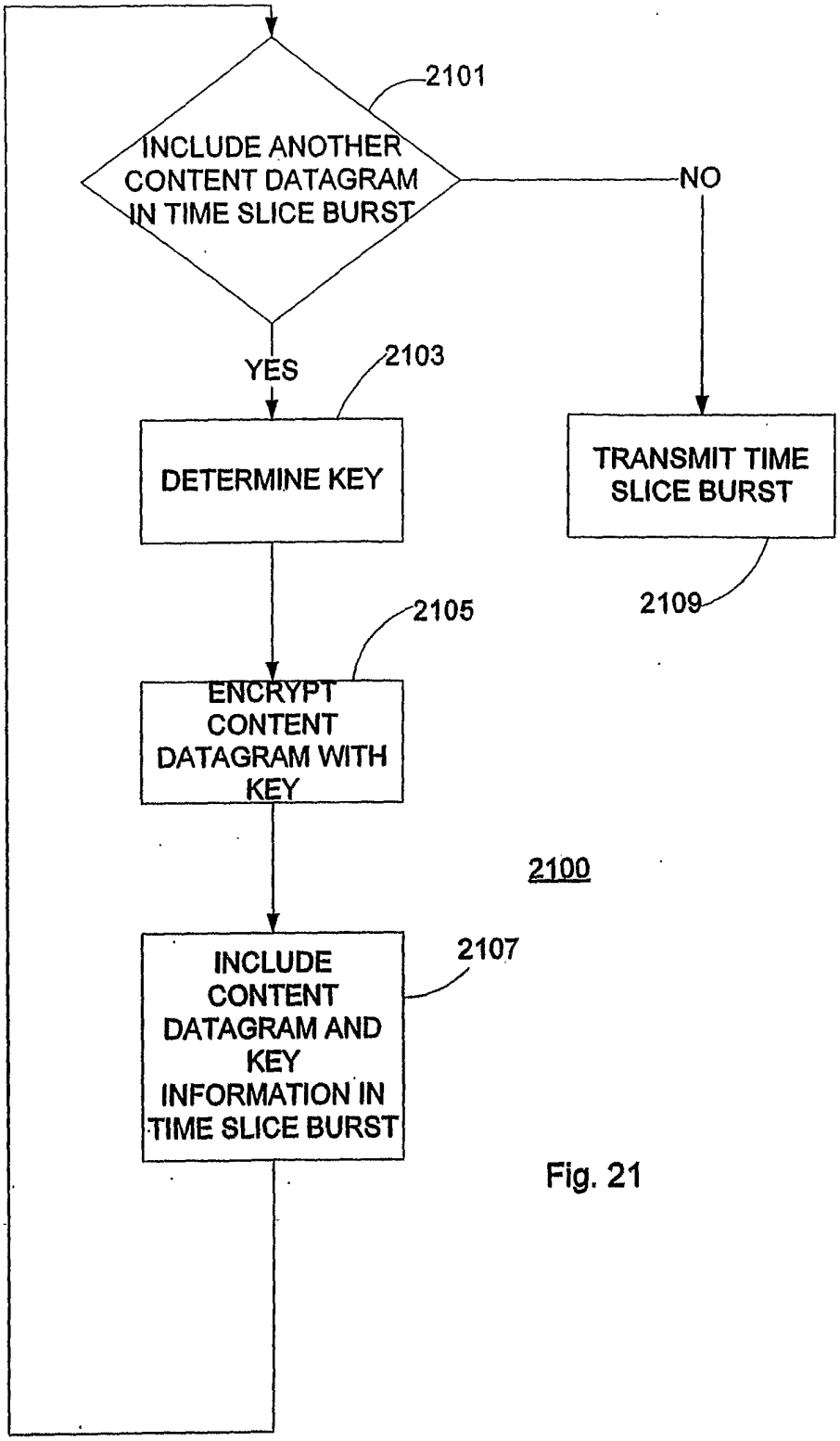

2101
INCLUDE ANOTHER CONTENT DATAGRAM IN TIME SLICE BURST
NO
YES
2103
DETERMINE KEY
TRANSMIT TIME SLICE BURST
2109
2105
ENCRYPT CONTENT DATAGRAM WITH KEY
2100
2107
INCLUDE CONTENT DATAGRAM AND KEY INFORMATION IN TIME SLICE BURST

Fig. 21

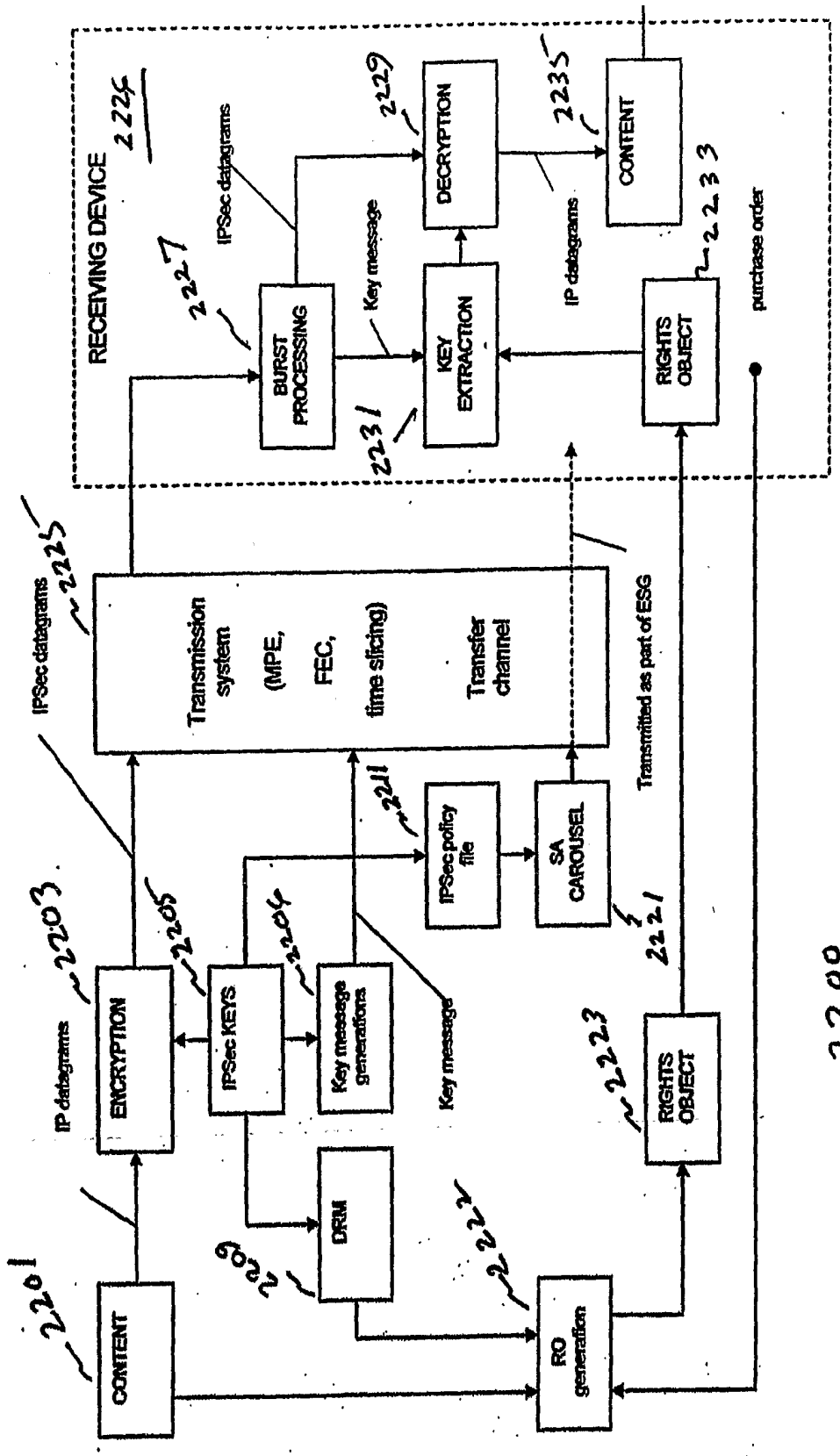

RECEIVING DEVICE
2226
BURST PROCESSING
2227
KEY EXTRACTION
2231
DECRYPTION
2229
CONTENT
2235
RIGHTS OBJECT
2233
IPSec datagrams
Key message
IP datagrams
purchase order
Transmission system
(MPE,
FEC,
time slicing)
Transfer channel
IPSec datagrams
2225
Transmitted as part of ESG
IPSec policy file
2211
SA CAROUSEL
2221
ENCRYPTION
2203
IPSec KEYS
2205
Key message generations
2206
IP datagrams
Key message
DRM
2209
RO generation
2207
RIGHTS OBJECT
2223
CONTENT
2201
2200

FIG. 22

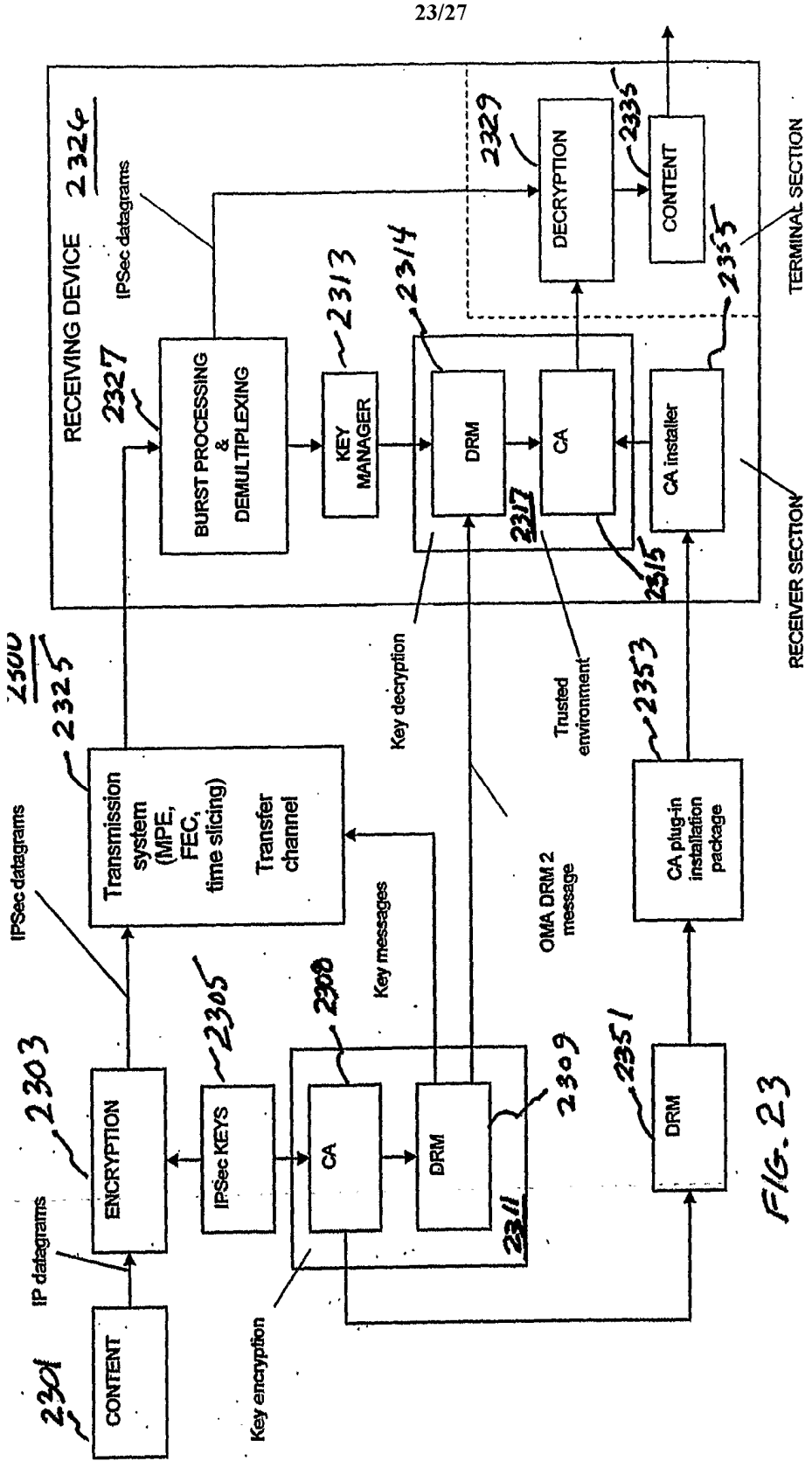

2300
2301
CONTENT
IP datagrams
2303
ENCRYPTION
IPSec datagrams
2305
IPSec KEYS
Key encryption
2307
CA
2309
DRM
2311
Key messages
2325
Transmission system (MPE, FEC, time slicing)
Transfer channel
IPSec datagrams
RECEIVING DEVICE 2326
2327
BURST PROCESSING & DEMULTIPLEXING
IPSec datagrams
2313
KEY MANAGER
2314
DRM
Key decryption
2317
CA
Trusted environment
2315
CA installer
2329
DECRYPTION
2335
CONTENT
2355
TERMINAL SECTION
RECEIVER SECTION
2353
CA plug-in installation package
OMA DRM 2 message
2351
DRM

FIG. 23

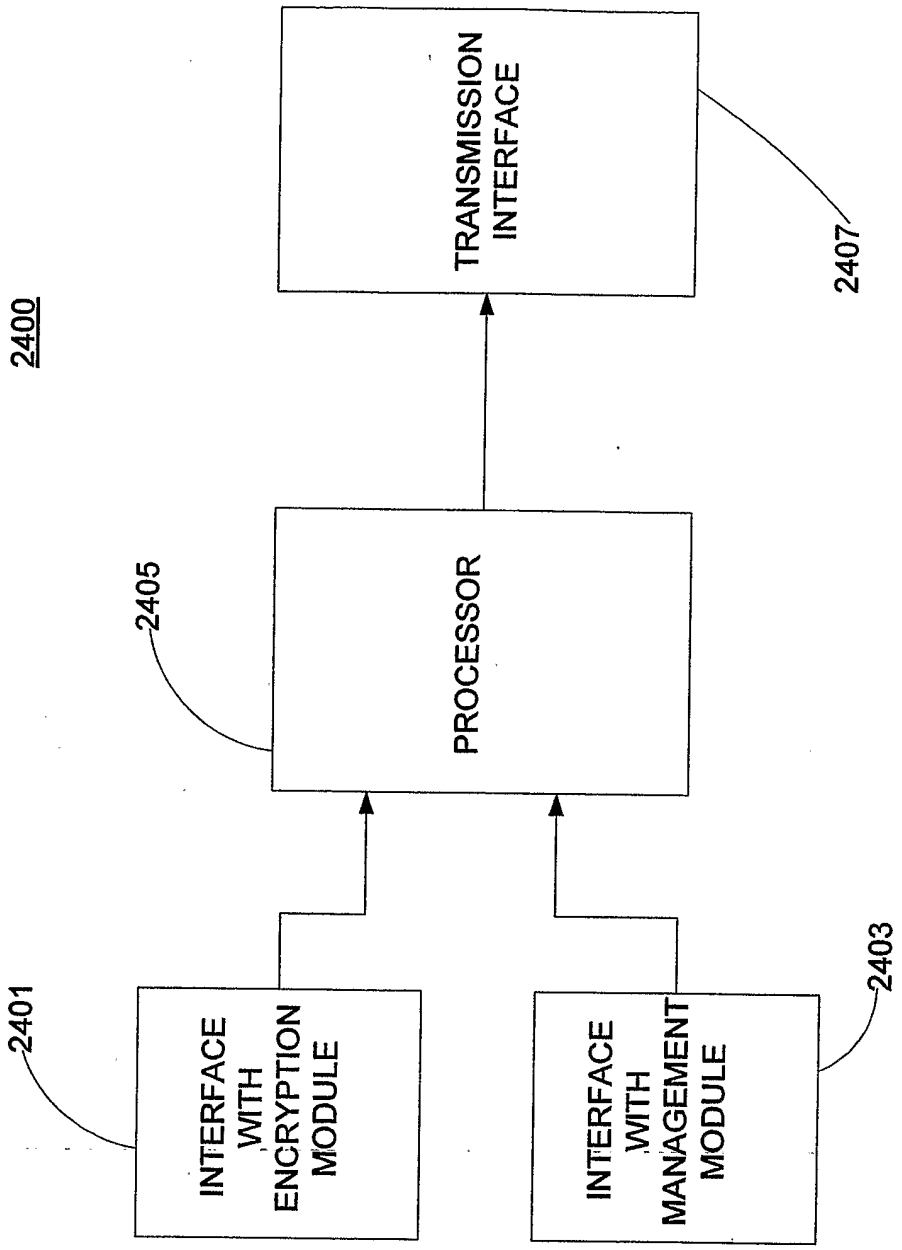

2400
TRANSMISSION INTERFACE
2407
PROCESSOR
2405
INTERFACE WITH ENCRYPTION MODULE
2401
INTERFACE WITH MANAGEMENT MODULE
2403

FIG. 24

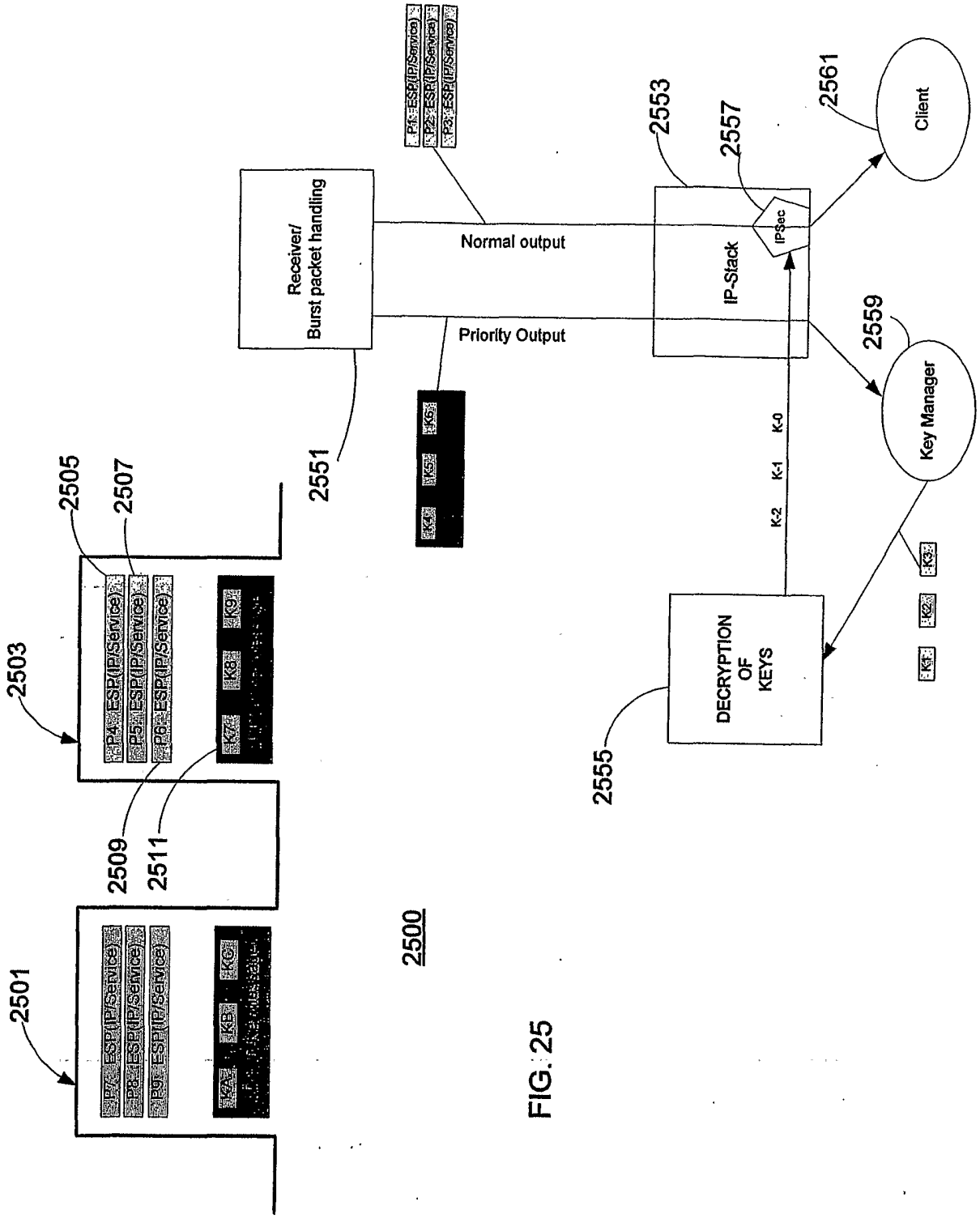

2500
2501
2503
2505
2507
2509
2511
2551
2553
2555
2557
2559
2561
P1: ESP(IP/Service)
P2: ESP(IP/Service)
P3: ESP(IP/Service)
P4: ESP(IP/Service)
P5: ESP(IP/Service)
P6: ESP(IP/Service)
P7: ESP(IP/Service)
P8: ESP(IP/Service)
P9: ESP(IP/Service)
K1
K2
K3
K4
K5
K6
K7
K8
K9
K-0
K-1
K-2
Receiver/
Burst packet handling
Normal output
Priority Output
IP-Stack
IPSec
Client
Key Manager
DECRYPTION
OF
KEYS

FIG. 25

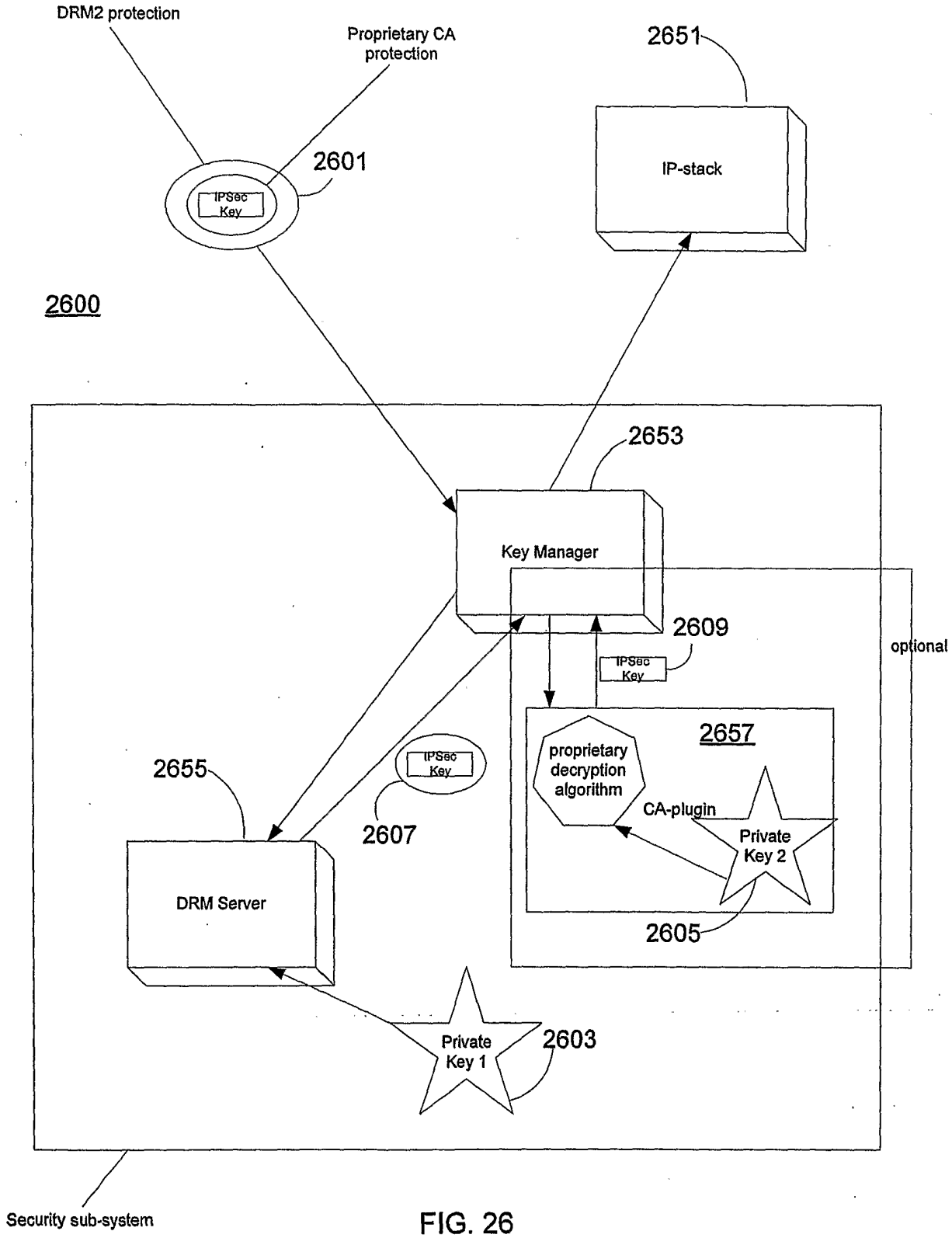

DRM2 protection
Proprietary CA protection
2651
IP-stack
2601
IPSec Key
2600
2653
Key Manager
2609
optional
IPSec Key
2657
proprietary decryption algorithm
CA-plugin
Private Key 2
2655
IPSec Key
2607
DRM Server
2605
Private Key 1
2603
Security sub-system

FIG. 26

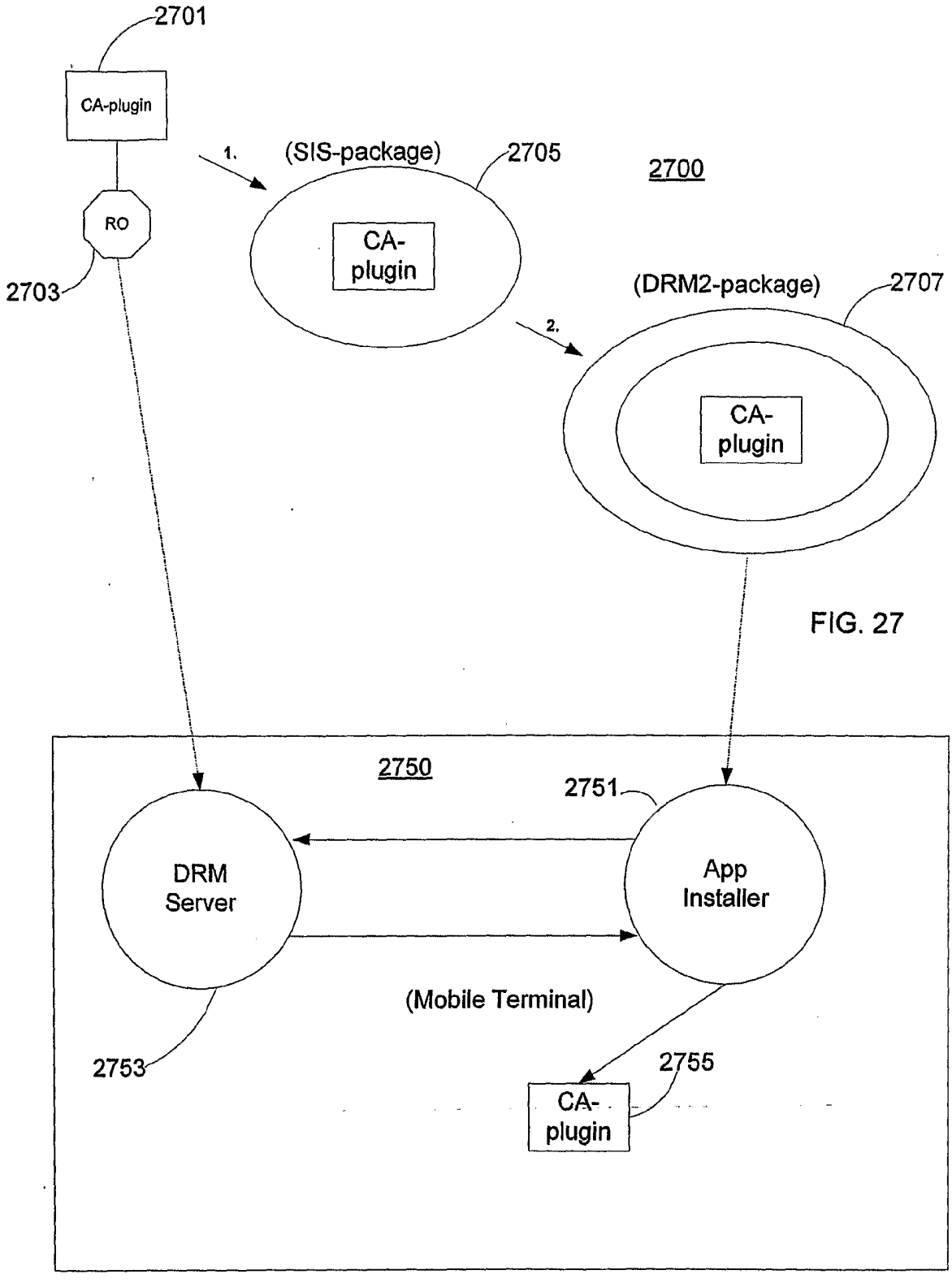

2701
CA-plugin
RO
2703
1.
(SIS-package)
2705
CA-plugin
2700
(DRM2-package)
2707
2.
CA-plugin
2750
2751
DRM Server
App Installer
(Mobile Terminal)
2753
2755
CA-plugin

FIG. 27

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 2005/001899

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 9/00, H04N 7/167
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04N, H04L

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, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 03059039 A2 (SONY ELECTRONICS INC), 24 July 2003 (24.07.2003), page 10, line 7 - line 14, abstract --	1-74
A	US 20020021809 A1 (JUHA SALO ET AL), 21 February 2002 (21.02.2002), claims 1-18, abstract, [0007],[0041] --	1-74
A	WO 03005145 A2 (NOKIA CORPORATION), 16 January 2003 (16.01.2003), figure 10 --	1-74
A	US 5787172 A (TERRY SUTTON ARNOLD), 28 July 1998 (28.07.1998), column 6, line 31 - line 46 --	1-74

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 November 2005	17-11-2005
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 Jesper Bergstrand/MN Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 2005/001899

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 20030081776 A1 (BRANT L. CANDELORE), 1 May 2003 (01.05.2003), see whole document -- US 20040181666 A1 (BRANT L. CANDELORE), 16 Sept 2004 (16.09.2004), see whole document -- US 20050094812 A1 (KARINA TEREKHOVA ET AL), 5 May 2005 (05.05.2005), see whole document -- US 20050100167 A1 (JUKKA ALVE ET AL), 12 May 2005 (12.05.2005), see whole document -- --------	1-74
P,A		
P,A		
P,A		

INTERNATIONAL SEARCH REPORT

Information on patent family members

29/10/2005

International application No.
PCT/IB 2005/001899

WO	03059039	A2	24/07/2003	AU	2002360605	A	00/00/0000
				CN	1623326	A	01/06/2005
				EP	1468561	A	20/10/2004
				JP	2005514886	T	19/05/2005
				CA	2405902	A	26/04/2003
				CA	2413807	A	02/07/2003
				CA	2413880	A	02/07/2003
				CA	2413881	A	02/07/2003
				CA	2413905	A	02/07/2003
				CA	2413955	A	02/07/2003
				CA	2413980	A	02/07/2003
				CA	2437086	A	09/03/2004
				US	20030046686	A	06/03/2003
				US	20030123664	A	03/07/2003
				US	20030133570	A	17/07/2003
				US	20030145329	A	31/07/2003
				US	20030152224	A	14/08/2003
				US	20030156718	A	21/08/2003
				US	20030159139	A	21/08/2003
				US	20030159140	A	21/08/2003
				US	20030174837	A	18/09/2003
				US	20040073917	A	15/04/2004
				US	20050028193	A	03/02/2005
US	20020021809	A1	21/02/2002	AU	7968801	A	14/01/2002
				CN	1190981	C	23/02/2005
				CN	1449632	A,T	15/10/2003
				EP	1300035	A	09/04/2003
				GB	0016245	D	00/00/0000
				GB	2364211	A	16/01/2002
				WO	0203728	A	10/01/2002
WO	03005145	A2	16/01/2003	CN	1554063	A	08/12/2004
				EP	1449132	A	25/08/2004
				US	20040249768	A	09/12/2004
				US	20050004875	A	06/01/2005
				EP	0802926	A	29/10/1997
				JP	10500725	T	20/01/1998

US	5787172	A	28/07/1998	CA	2184679	A	04/03/1998
				EP	0746927	A,B	11/12/1996
				SE	0746927	T3	
				WO	9523468	A	31/08/1995
				AT	189570	T	15/02/2000
				DE	69514908	D,T	20/07/2000
				EP	0907270	A	07/04/1999
				US	6148400	A	14/11/2000
				US	6456716	B	24/09/2002
US	20030081776	A1	01/05/2003	AU	2002357846	A	00/00/0000
				CA	2405865	A	26/04/2003
				CA	2413807	A	02/07/2003
				CA	2413880	A	02/07/2003
				CA	2413881	A	02/07/2003
				CA	2413905	A	02/07/2003
				CA	2413955	A	02/07/2003
				CA	2413980	A	02/07/2003
				CA	2437086	A	09/03/2004
				CN	1633809	A	29/06/2005
				EP	1486071	A	15/12/2004
				JP	2005515694	T	26/05/2005
				US	20030123664	A	03/07/2003
				US	20030133570	A	17/07/2003
				US	20030145329	A	31/07/2003
				US	20030152224	A	14/08/2003
				US	20030156718	A	21/08/2003
				US	20030159139	A	21/08/2003
				US	20030159140	A	21/08/2003
				US	20030174837	A	18/09/2003
				US	20040073917	A	15/04/2004
				US	20050028193	A	03/02/2005
				WO	03061173	A	24/07/2003
				US	20020194613	A	19/12/2002
				US	20020196939	A	26/12/2002
				US	20030021412	A	30/01/2003
				US	20030026423	A	06/02/2003
				US	20030046686	A	06/03/2003
				US	20040181666	A	16/09/2004

INTERNATIONAL SEARCH REPORT

Information on patent family members

29/10/2005

International application No.
PCT/IB 2005/001899

US	20040181666	A1	16/09/2004	US	20030174844	A	18/09/2003
				US	20040158721	A	12/08/2004
				WO	2004082147	A	23/09/2004
				AU	2002357213	A	00/00/0000
				CA	2405899	A	26/04/2003
				CA	2413807	A	02/07/2003
				CA	2413880	A	02/07/2003
				CA	2413881	A	02/07/2003
				CA	2413905	A	02/07/2003
				CA	2413955	A	02/07/2003
				CA	2413980	A	02/07/2003
				CA	2437086	A	09/03/2004
				CN	1623327	A	01/06/2005
				EP	1461952	A	29/09/2004
				JP	2005515725	T	26/05/2005
				US	20030021412	A	30/01/2003
				US	20030123664	A	03/07/2003
				US	20030133570	A	17/07/2003
				US	20030145329	A	31/07/2003
				US	20030152224	A	14/08/2003
				US	20030156718	A	21/08/2003
				US	20030159139	A	21/08/2003
				US	20030159140	A	21/08/2003
				US	20030174837	A	18/09/2003
				US	20040073917	A	15/04/2004
				US	20050028193	A	03/02/2005
				WO	03061288	A	24/07/2003
				CA	2405865	A	26/04/2003
				CA	2405901	A	26/04/2003
				CA	2405902	A	26/04/2003
				CA	2406329	A	26/04/2003
				US	20020194613	A	19/12/2002
				US	20030026423	A	06/02/2003
				US	20030046686	A	06/03/2003
				US	20020196939	A	26/12/2002
				US	20030081776	A	01/05/2003
US	20050094812	A1	05/05/2005	GB	0325846	D	00/00/0000
				GB	2407947	A	11/05/2005
				US	20050090235	A	28/04/2005
				WO	2005045603	A	19/05/2005
US	20050100167	A1	12/05/2005	WO	2005045554	A	19/05/2005
				US	20050100162	A	12/05/2005