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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 May 2009 (07.05.2009)

PCT

(10) International Publication Number
WO 2009/057857 A1

(51) International Patent Classification:
H04N 5/44 (2006.01) *H04Q 7/24* (2006.01)

(21) International Application Number:
PCT/KR2008/000616

(22) International Filing Date: 1 February 2008 (01.02.2008)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
10-2007-0110093 31 October 2007 (31.10.2007) KR
10-2008-0005797 18 January 2008 (18.01.2008) KR

(71) Applicant *(for all designated States except US)*: **SK TELECOM CO., LTD.** [KR/KR]; 11, Euljiro 2-ga, Jung-gu, Seoul 100-999 (KR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KIM, Kwang Young** [KR/KR]; 112-1117, Kukdong Apt., Sadang 2-dong, Dongjak-gu, Seoul 156-772 (KR). **KIM, Jong Ho** [KR/KR]; 113-1405, Gwanak Dreamtown Apt., 1712 bunji, Bongcheon-dong, Gwanak-gu, Seoul 151-050 (KR). **KIM, Do Wan** [KR/KR]; 502-401, Haneul Maeul, 1800, Jungsan-dong, Ilsandong-gu, Goyang-si, Gyeonggi-do 410-315 (KR). **PARK, Jae Bum** [KR/KR]; 103-901, Dogok Samsung Raemian Apt., Dogok 2-dong, Gangnam-gu, Seoul 135-537 (KR). **HWANG, Byung Seok** [KR/KR]; 201-903, Chungmu Jugong Apt., 873-2, Geumjeong-dong, Gunpo-si, Gyeonggi-do 435-050 (KR).

(74) Agent: **YOON YANG KIM SHIN & YU**; 11th Floor, Namkang Bldg.1340-6, Seocho-dong, Seocho-gu, Seoul 137-861 (KR).

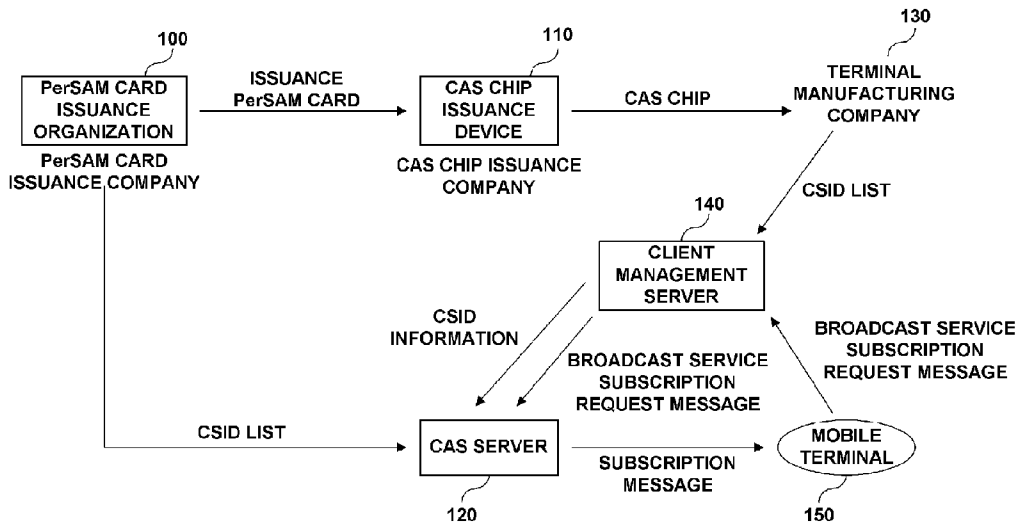
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM,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

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

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR PROVIDING CONDITIONAL ACCESS BROADCASTING SERVICE

[Fig. 1]



(57) Abstract: A method of generating a pre-subscription Conditional Access System (CAS) chip is disclosed. In order for a mobile terminal to receive a conditional-access broadcasting service, a broadcasting service subscription process has been performed on the CAS chip in advance. A CAS Initial Delivery (CID) key is generated using a seed key and an algorithm, stored in an issuance Personalization Secure Application Module (PerSAM) card, and the generated CID key is registered in the CAS chip. A subscriber key is generated using a seed key and an algorithm, stored in a subscription PerSAM card. The generated subscriber key is inserted into a subscription Entitlement Management Message (EMM). A pre-subscription CAS chip is generated by registering the subscription EMM in the CAS chip in which the CID key is registered.

WO 2009/057857 A1

Published:
— *with international search report*

Description

SYSTEM AND METHOD FOR PROVIDING CONDITIONAL ACCESS BROADCASTING SERVICE

Technical Field

[1] The present invention relates, in general, to a system and method for providing a conditional-access broadcasting service, in which a broadcasting service subscription process is performed in advance when a Conditional Access System (CAS) chip is issued, so that a conditional-access broadcasting service can be received using a mobile terminal in which the corresponding CAS chip is installed, and, more particularly, to a system and method for providing a conditional-access broadcasting service, which determines whether access to the broadcasting service of a specific channel is possible by analyzing the subscription Entitlement Management Message (EMM) of an installed CAS chip when a request for access to the broadcasting service of the corresponding channel is made, and which makes a request for subscription to the broadcasting service of the corresponding channel in order to receive the corresponding broadcasting service if it is determined that access to the broadcasting service of the corresponding channel is not possible.

[2]

Background Art

[3] A Digital Multimedia Broadcasting (DMB) service is a broadcasting service that enables subscribers to view or listen to various types of multimedia broadcasts, such as video, audio, and data, in a multichannel environment using personal portable terminals equipped with receiving antennas or mobile terminals for vehicles, even when the subscribers are outdoors or are traveling.

[4] The DMB service has changed the type of broadcast from a conventional analog type to a digital type, thereby providing high-quality Compact Disk (CD)-level sound quality, various data services, bidirectionality, and excellent mobile reception quality, expanding the concept of existing broadcasts from that of watching and listening to broadcasts to that of watching, listening to and participating in broadcasts, and enabling various types of multimedia information, such as news, traffic information, weather information, geographical information, and moving picture information, to be transmitted in the form of text and graphics, in addition to music broadcasts.

[5] Meanwhile, since the above-described DMB service is generally a charged service, a CAS is applied thereto to enforce the conditional access of subscribers.

[6] The CAS performs a conditional-access function by setting viewing levels using a DMB chip installed in each mobile terminal, and performs a security function of

preventing the viewing of a DMB through the illegal use of the DMB chip.

[7] A CAS chip, which is inserted/installed into/in a terminal and is then operated, performs functions of generating a Control Word (CW), necessary to decrypt encrypted broadcasting content, based on an Entitlement Control Message (ECM), and extracting a subscription message and access rights information from an EMM.

[8] A subscription procedure is required in order for the CAS chip to support the normal viewing of a specific program. The subscription procedure is completed by receiving the subscription message.

[9] FIG. 1 is a conceptual diagram showing a method by which a mobile terminal uses a broadcasting service after a conventional CAS chip has been issued.

[10] Referring to FIG. 1, when a CAS chip issuance order is made by a terminal manufacturing company 130, a Personalization Secure Application Module (PerSAM) issuance company 100 issues an issuance PerSAM card, used when important information is issued to a CAS chip, generates a Called Subscriber Identification (CSID) list to be stored in each CAS chip, and then provides the CSID list, together with the issuance PerSAM card, to a CAS chip issuance company 110.

[11] The CAS chip issuance company 110 generates a CAS Initial Delivery (CID) key to be included in the CAS chip using a seed key and an algorithm stored in the issuance PerSAM card, received from the PerSAM issuance company 100, and then inputs the generated CID key to the CAS chip.

[12] Thereafter, the generation of the CAS chip is completed, and the CAS chip issuance company 110 transmits the generated CAS chip to the terminal manufacturing company 130.

[13] The terminal manufacturing company 130 installs the CAS chip in a mobile terminal 150, and transmits the results of the installation to a client management server 140.

[14] Thereafter, the client management server 140 transmits the CSID information of the CAS chip, installed in the mobile terminal 150, to a CAS server 120.

[15] Through the above-described processes, the mobile terminal 150, in which the CAS chip is installed, is manufactured.

[16] In order to use a broadcasting service using the mobile terminal 150, manufactured as described above, a user transmits a broadcasting service subscription request message, used to make a request for subscription to the broadcasting service from the client management server 140. The broadcasting service subscription request message includes the CSID information of the CAS chip installed in the mobile terminal 150.

[17] The client management server 140 transmits the broadcasting service subscription request message to the CAS server 120.

[18] Then, the CAS server 120 approves subscription for the CSID included in the broadcasting service subscription request message, and then transmits a subscription

message to the mobile terminal 150. Consequently, the mobile terminal 150 can use the broadcasting service.

[19] As described above, in order to view a specific program using a mobile terminal in which a conventional CAS chip is installed, there is inconvenience in that an additional subscription procedure must be performed.

[20] Furthermore, there is a disadvantage in that a significantly large amount of bandwidth is required when a subscription message is transmitted in compliance with a broadcasting service subscription procedure.

[21] Moreover, in order to receive a broadcasting service, an additional subscription procedure must be performed after a terminal has been purchased, so that there is a disadvantage in that the procedure for receiving the broadcasting service is complicated.

[22]

Disclosure of Invention

Technical Problem

[23] Accordingly, the present invention has been made keeping in mind the above problems occurring in the prior art, and an object of the present invention is to provide a system and method for providing a conditional-access broadcasting service in which a broadcasting service subscription process is performed in advance when a CAS chip is issued, so that bandwidth consumed by subscription messages is reduced, thereby increasing the number of subscribers.

[24] Another object of the present invention is to provide a system and method for providing a conditional-access broadcasting service which can receive a conditional-access broadcasting service, even though an additional subscription procedure has not been performed after a mobile terminal has been purchased.

[25] A further object of the present invention is to provide a system and method for providing a conditional-access broadcasting service which includes product rights information together with a subscription message when a CAS chip is issued, so that a corresponding program can be immediately viewed without performing a purchase procedure for the product.

[26]

Technical Solution

[27] According to an aspect of the present invention in order to accomplish the above objects, the present invention provides a method of generating a pre-subscription Conditional Access System (CAS) chip, for which a broadcasting service subscription process has been performed in advance, in order for a mobile terminal to receive a conditional-access broadcasting service, the method including: a step of generating a CAS Initial Delivery (CID) key using a seed key and an algorithm, stored in an

issuance Personalization Secure Application Module (PerSAM) card, and registering the generated CID key in the CAS chip; and a step of generating a subscriber key using a seed key and an algorithm, stored in a subscription PerSAM card, inserting the generated subscriber key into a subscription Entitlement Management Message (EMM), and generating a pre-subscription CAS chip by registering the subscription EMM in the CAS chip in which the CID key is registered.

[28] According to another aspect of the present invention, the present invention provides a method of generating pre-subscription CAS chips, for which a broadcasting service subscription process has been performed in advance, in order for a mobile terminal to receive a conditional-access broadcasting service, the method including a step of a PerSAM card issuance device for issuing a PerSAM card functioning as a device for authenticating a card and loading a key value, generating a Called Subscriber Identification (CSID) list, and providing the CSID list to a CAS server and a CAS chip issuance device; a step of the CAS server generating a subscription EMM for the CSID list, and providing the subscription EMM to the CAS chip subscription device; a step of the CAS chip issuance device generating a CID key using a seed key and an algorithm, stored in an issuance PerSAM card, and registering the generated CID key in the CAS chip; and a step of the CAS chip subscription device generating a subscriber key using a seed key and an algorithm, stored in a subscription PerSAM card, inserting the generated subscriber key into the subscription EMM provided from the CAS server, and then generating a subscription-completed CAS chip by registering the subscription EMM in the CAS chip, issuance of which is completed by the CAS chip issuance device.

[29] According to another aspect of the present invention, the present invention provides a method of at least one mobile terminal receiving a broadcasting service through a client management server for storing subscriber information, and a CAS server, the method including a step (a) of, when a request for access to the broadcasting service of a specific channel has been made, determining whether the access to the broadcasting service of the corresponding channel is possible by analyzing the subscription EMM of an installed CAS chip; a step (b) of, if, as the result of the determination at the step (a), it is determined that the access to the broadcasting service of the corresponding channel is not possible, displaying a message inquiring about whether a request for viewing rights has been made to access the broadcasting service of the corresponding channel; a step (c) of, if a request command is selected using the displayed message inquiring about whether the request for viewing rights has been made, transmitting a viewing rights request message to the CAS server through the client management server; and a step (d) of, if a viewing rights investment message is received from the CAS server, receiving the broadcasting service of the corresponding channel.

[30] The step (a) step includes determining whether the access to the broadcasting service of the corresponding channel is possible by checking information about channel viewing qualification and about a charged channel viewing level included in the subscription EMM of the CAS chip.

[31] After the step (c), the CAS server affiliates the mobile terminal with the broadcast service of the corresponding channel, and then transmits a viewing rights investment message to the mobile terminal.

[32] According to another aspect of the present invention, the present invention provides a system for providing a conditional-access broadcasting service, including one or more mobile terminals, each configured to include a CAS chip, in which a CID key and a subscription EMM are registered, determine whether access to the broadcasting service of a specific channel is possible using the subscription EMM if the corresponding channel is selected for the access to the broadcasting service, and display a message inquiring about whether a request for viewing rights has been made if it is determined that the access to the broadcasting service of the corresponding channel is not possible; a client management server configured to manage subscriber information, including a CSID list, in which a broadcasting service subscription process has been performed in advance when a CAS chip is issued, and transmit a viewing rights request message when the viewing rights request message is received from one of the mobile terminals; and a CAS server configured to, when the viewing rights request message is received from the client management server, perform subscription to the broadcast service of a channel included in the viewing rights request message, and then transmit a viewing rights investment message to the mobile terminal.

[33] The mobile terminal, when a request command is selected using the message inquiring about whether the request for viewing rights has been made, generates the viewing rights request message, including the identification information of the mobile terminal and information about the corresponding channel, and then transmits the viewing rights request message to the client management server.

[34] According to another aspect of the present invention, the present invention provides a mobile terminal including a wireless transmission/reception unit, an input unit, a display unit, and an audio unit, and receiving a conditional-access broadcasting service, the mobile terminal including a CAS chip including a subscription EMM configured to include a subscriber key, and a CID key; a channel viewing qualification determination unit configured to, when a broadcasting service access request command is received through the input unit, determine whether access to the broadcasting service of a specific channel is possible using the subscription EMM included in the CAS chip, and if, as the result of the determination, it is determined that the access to the broadcasting service of the corresponding channel is not possible, display a message

inquiring about whether a request for viewing rights has been made for the corresponding channel on the display unit; and a viewing rights request unit configured to, if the request command is input through the displayed message inquiring about whether the request for viewing rights has been made, generate and transmit a viewing rights request message including the identification information of the mobile terminal and information about the corresponding channel.

[35] The channel viewing qualification determination unit receives the broadcasting service of the corresponding channel through the wireless transmission/reception unit if it is determined that the access to the broadcasting service of the corresponding channel is possible.

[36] The channel viewing qualification determination unit determines whether the access to the broadcasting service of the corresponding channel is possible by checking information about channel viewing qualification and about a charged channel viewing level included in the subscription EMM of the CAS chip.

[37] According to another aspect of the present invention, the present invention provides a pre-subscription CAS chip enabling a conditional-access broadcasting service to be received without performing a subscription procedure when the broadcasting service is initially used, wherein a subscription EMM including a subscriber key is registered in a CAS chip in which a CID key is registered.

[38] The CID key is generated using a seed key and an algorithm stored in an issuance PerSAM card, and the subscriber key is generated using a seed key and an algorithm stored in a subscription PerSAM card.

[39]

Advantageous Effects

[40] As described above, the present invention can provide a system and method for providing a conditional-access broadcasting service in which a broadcasting service subscription process is performed in advance when a CAS chip is issued, so that bandwidth consumed by subscription messages is reduced, thereby increasing the number of subscribers.

[41] Further, the present invention can provide a system and method for providing a conditional-access broadcasting service which can receive a conditional-access broadcasting service, even though an additional subscription procedure has not been performed after a mobile terminal has been purchased.

[42] Moreover, the present invention can provide a system and method for providing a conditional-access broadcasting service which includes product rights information together with a subscription message when a CAS chip is issued, so that a corresponding program can be immediately viewed without performing a purchase

procedure for the product.

[43]

Brief Description of the Drawings

[44] FIG. 1 is a conceptual diagram showing a method by which a mobile terminal uses a broadcasting service after a conventional CAS chip has been issued;

[45] FIG. 2 is a diagram showing a system for issuing a CAS chip and providing a conditional-access broadcasting service according to the present invention;

[46] FIG. 3 is a flowchart showing a method of generating a pre-subscription CAS chip according to the present invention;

[47] FIG. 4 is a block diagram schematically showing the configuration of a mobile terminal in which the pre-subscription CAS chip is installed according to the present invention; and

[48] FIG. 5 is a flow chart showing a method of providing a broadcasting service using the mobile terminal in which a subscription-completed CAS chip is installed according to the present invention.

[49]

Best Mode for Carrying Out the Invention

[50] The above-described objects, technical configuration, and consequent effect of the present invention will be clearly understood through the embodiments of the present invention below, with reference to the drawings attached to the patent specification for the present invention.

[51] Although the devices and organizations (companies) for managing the devices, which will be described below, are the same, they will be described as devices or organizations (companies) for convenience of explanation.

[52] FIG. 2 is a diagram showing a system for issuing a CAS chip and providing a conditional-access broadcasting service according to the present invention.

[53] Referring to FIG. 2, the system for issuing a CAS chip and providing a conditional-access broadcasting service includes a PerSAM card issuance device 200 for generating a CSID list to be stored in each CAS chip, a CAS server 220 for generating a subscription EMM for the CSID list, a CAS chip issuance device 210 for generating a CID key using the issuance PerSAM card, issued from the PerSAM card issuance company 200, and inputting the generated CID key to the CAS chip, a CAS chip subscription device 230 for generating a subscription-completed CAS chip by registering the subscription EMM, generated by the CAS server 220, in the CAS chip, the issuance of which is completed by the CAS chip issuance device 210, a terminal manufacturing company 240 for installing the subscription-completed CAS chip in a mobile terminal 260 and providing the CSID list to a client management server 250, and the

client management server 250 for transmitting a viewing rights request message to the CAS server 220 when viewing rights for a specific channel is requested by the mobile terminal 260.

[54] The PerSAM card issuance company 200 issues an issuance PerSAM card and a subscription PerSAM card, used for a broadcasting service pre-subscription process, and then provides the issuance PerSAM card to the CAS chip issuance device 210 and provides the subscription PerSAM card to the CAS chip subscription device 230.

[55] Further, the PerSAM card issuance device 200 generates the CSID list to be stored in the CAS chip, and then transmits the CSID list to the CAS chip issuance device 210 and the CAS server 220.

[56] When the CSID list is received from the PerSAM card issuance company 200, the CAS server 220 generates a subscription EMM for the CSID list, and then transmits the subscription EMM to the CAS chip subscription device 230. The subscription EMM includes information about the channel viewing qualification of the user of the mobile terminal and about a charged channel viewing level.

[57] The CAS chip issuance device 210 generates a CID key using a seed key and an algorithm stored in the issuance PerSAM card, and then completes the issuance of the CAS chip by registering the CID key in the CAS chip. Thereafter, the CAS chip issuance company 210 provides the issuance-completed CAS chip to the CAS chip subscription device 230.

[58] The CAS chip subscription device 230 generates a subscriber key using a seed key and an algorithm stored in the subscription PerSAM card, inserts the subscriber key into the subscription EMM transmitted from the CAS server 220, and then registers the subscription EMM, including the subscriber key, in the issuance-completed CAS chip. That is, the CAS chip subscription device 230 generates a CAS chip, the pre-subscription for a broadcasting service of which is completed, by registering the subscription EMM in the issuance-completed CAS chip.

[59] The terminal manufacturing company 240 installs the CAS chip, the subscription of which is completed by the CAS chip subscription device 230, in the mobile terminal, and provides a CSID list for a terminal, which operates normally, to the client management server 250.

[60] The client management server 250 transmits the pre-subscription CSID list, transmitted from the terminal manufacturing company 240, to the CAS server 220.

[61] Therefore, the client management server 250 and the CAS server 220 function to manage subscriber information corresponding to the pre-subscription CSID of a broadcasting service.

[62] A user who purchased the mobile terminal 260, in which the CAS chip generated by the above-described process is installed, can receive a conditional-access broadcasting

service without performing an additional subscription procedure. That is, the mobile terminal 260, in which the generated CAS chip is installed, can receive a broadcasting service corresponding to a specific channel based on information about channel viewing qualification and about a charged channel viewing level, included in the corresponding subscription EMM, without performing an additional subscription procedure.

[63] Whether access to the broadcast of a corresponding channel is possible is determined by analyzing the subscription EMM of the installed CAS chip, and then, if, as the results of the determination, it is determined that the access to the broadcast of the corresponding channel is not possible, the mobile terminal 260 outputs a message inquiring about whether a request for viewing rights has been made to access the broadcast of the corresponding channel. If a request command is selected using the displayed message inquiring about whether a request for viewing rights has been made, the mobile terminal 260 requests the viewing rights for the corresponding channel from the CAS server 220 through the client management server 250.

[64] Thereafter, the CAS server 220 invests the viewing rights such that the mobile terminal 260 can receive a broadcast for the corresponding channel, and then transmits a viewing rights investment message to the mobile terminal 260.

[65] Therefore, the mobile terminal 260 can receive the broadcast of the corresponding channel.

[66] FIG. 3 is a flowchart showing a method of generating the pre-subscription CAS chip according to the present invention.

[67] Referring to FIG. 3, the PerSAM card issuance device generates a CSID list to be stored in a CAS chip at step S300, and then transmits the CSID list to the CAS server and the CAS chip issuance device at step S302.

[68] Here, the PerSAM card issuance device issues an issuance PerSAM card and a subscription PerSAM card, used for pre-subscription to a broadcasting service.

[69] The CAS server generates a subscription EMM file for a CSID list, transmitted from the PerSAM card issuance device, at step S304, and then transmits the subscription EMM file to the CAS chip subscription device at step S306.

[70] Thereafter, the CAS chip issuance device generates a CID key using a seed key and an algorithm, stored in the issuance PerSAM card, issued by the PerSAM card issuance device, at step S308, completes the issuance of the CAS chip by registering the generated CID key in the CAS chip at step S310, and then provides the issuance-completed CAS chip to the CAS chip subscription device at step S312.

[71] The process of the CAS server generating the subscription EMM and the process of the CAS chip issuance device generating the issuance-completed CAS chip can be simultaneously realized.

[72] The CAS chip subscription device generates a subscriber key using a seed key and an algorithm stored in the subscription PerSAM card at step S314, and inserts the generated subscriber key into the subscription EMM, transmitted from the CAS server, at step S216.

[73] Thereafter, the CAS chip subscription device generates a subscription-completed CAS chip by inputting the subscription EMM to the issuance-completed CAS chip, transmitted from the CAS chip issuance device, at step S318. Consequently, the CAS chip includes the subscription EMM, which includes the subscriber key generated by the subscription PerSAM card and the CID key generated by the issuance PerSAM card. Here, the subscription-completed CAS chip is a CAS chip in which subscription to a broadcasting service is performed before the CAS chip is issued.

[74] FIG. 4 is a block diagram schematically showing the configuration of a mobile terminal in which a pre-subscription CAS chip is installed according to the present invention.

[75] Referring to FIG. 4, the mobile terminal, in which the pre-subscription CAS chip is installed, includes a wireless transmission/reception unit 300 for performing wireless communication, an input unit 310 for receiving user commands, a storage unit 320 for storing various types of data, a display unit 330 for displaying the current state of the mobile terminal or the processing state of an event requested by the user, and an audio unit 340 for outputting voice signals, a CAS chip 350 for storing subscription EMM information, a channel viewing rights determination unit 360, and a viewing rights request unit 370.

[76] The CAS chip 350 includes the subscription EMM, including the subscriber key generated by the subscription PerSAM card and the CID key generated by the issuance PerSAM card. The subscription EMM includes information about the channel viewing qualification of the user of the mobile terminal and about a charged channel viewing level.

[77] Here, the CAS chip 350 of the mobile terminal includes a unique CID key. The CID key is issued to the CAS chip 350 through the issuance PerSAM card, and a seed key and an algorithm, used to generate the CID key, are included in the issuance PerSAM card. The CID key is a key used for encryption/decryption when a broadcasting service provider transmits a subscription EMM, including a subscriber key, to a mobile terminal.

[78] That is, the subscription EMM is encrypted using the CID key, and then the encrypted subscription EMM is transmitted to the mobile terminal. The mobile terminal decrypts the encrypted subscription EMM using its own CID key, and then extracts a subscriber key.

[79] Thereafter, a message, transmitted to the mobile terminal, is basically encrypted

using a subscriber key or a key generated based on the subscriber key, and is then transmitted. Accordingly, in order to interpret a message transmitted to the mobile terminal, a subscriber key is necessary.

[80] Conventionally, the subscriber key is included in a subscription EMM, is encrypted using a CID key, and is then transmitted. However, the subscription EMM is installed in the CAS chip in advance using the subscription PerSAM card in the present invention. Therefore, a seed key and an algorithm are included in the subscription PerSAM card so as to generate a subscriber key.

[81] Briefly, in order to view a broadcast using a mobile terminal, the CAS chip 350 must include a CID key and a subscriber key. Therefore, the subscriber key is included in the CAS chip 350, along with the CID key.

[82] When a broadcasting service is initially used, the CAS chip 350 enables a conditional-access broadcasting service to be received without performing a subscription procedure. The CAS chip 350 is called a pre-subscription CAS chip.

[83] When a broadcasting-service-viewing request command for a specific channel is input by a user through the input unit 310, the channel viewing rights determination unit 360 determines whether it is possible to view the corresponding channel using the subscription EMM included in the CAS chip 350.

[84] If, as the results of the determination, it is determined that it is possible to view the corresponding channel, the channel viewing rights determination unit 360 receives the broadcasting service corresponding to the channel through the wireless transmission/reception unit 300.

[85] If, as the results of the determination, it is determined that it is not possible to view the corresponding channel, the channel viewing rights determination unit 360 displays a message inquiring about whether a request for viewing rights has been made to access the broadcast of the corresponding channel.

[86] The user of the mobile terminal checks the displayed message inquiring about whether the request for viewing rights has been made. If the user wants to access the broadcast of the corresponding channel, the user can select a request command.

[87] When the request command is selected through the input unit 310, the viewing rights request unit 370 generates a viewing rights request message including the identification information of the mobile terminal and about the corresponding channel, and then transmits the viewing rights request message to the client management server and the CAS server through the wireless transmission/reception unit 300.

[88] Thereafter, the CAS server invests viewing rights for a channel included in the viewing rights request message, generates a viewing rights investment message, and then transmits the viewing rights investment message to the mobile terminal.

[89] FIG. 5 is a flow chart showing a method of providing a broadcasting service using

the mobile terminal in which a subscription-completed CAS chip is installed according to the present invention.

[90] Referring to FIG. 5, when the user of a mobile terminal makes a request for access to the broadcast service of a specific channel using a menu at step of S400, the mobile terminal determines whether access to the broadcast service of the corresponding channel is possible by analyzing the subscription EMM of a CAS chip installed in the mobile terminal at step S402.

[91] That is, if a broadcasting service viewing request command is input, the mobile terminal determines whether access to the broadcast service of the corresponding channel is possible by checking information about channel viewing qualification of the subscription EMM of the CAS chip and about a charged channel viewing level.

[92] If, as the results of the determination at step S402, it is determined that access to the broadcast service of the corresponding channel is not possible, the mobile terminal displays a message inquiring about whether a request for viewing rights has been made to access the broadcast of the corresponding channel at step S404.

[93] If a user, who checked the displayed message inquiring about whether the request for viewing rights has been made, wants to access the broadcast service of the corresponding channel and selects a request command at step S406, the mobile terminal transmits a viewing rights request message to the CAS server through the client management server at step S408. Here, the viewing rights request message includes the identification information of a mobile terminal and information about a channel for which it is desired to access a broadcast service.

[94] The CAS server affiliates the mobile terminal with the broadcast service of the corresponding channel, and then transmits a viewing rights investment message to the mobile terminal at step S410.

[95] Consequently, the mobile terminal can receive the broadcast service of the corresponding channel.

[96] If, as the results of the determination at step S402, it is determined that access to the broadcast service of the corresponding channel is possible, the mobile terminal receives the broadcast service of the corresponding channel at step S412.

[97] It will be apparent to those skilled in the art, to which the present invention, described above, belongs, that the present invention can be realized using other preferred embodiments without departing from the technical scope or essential features of the present invention. Therefore, it should be understood that the above-described embodiment has been described for illustrative purposes only, and is not intended to limit the present invention. The range of the present invention is described by the accompanying claims, which will be set forth below, rather than the preferred embodiment, and it should be understood that the meaning and range of the claims, all

modifications deduced from equivalent concepts thereof, and modified embodiments are included in the range of the present invention.

Industrial Applicability

[98] As described above, a system and method for providing a conditional-access broadcasting service according to the present invention uses a mobile terminal in which a pre-subscription CAS chip, in which a broadcasting service subscription process is performed in advance when the CAS chip is issued, is installed, so that it is suitable for receiving a conditional-access broadcasting service without performing an additional subscription procedure.

Claims

[1] A method of generating a pre-subscription Conditional Access System (CAS) chip, for which a broadcasting service subscription process has been performed in advance, in order for a mobile terminal to receive a conditional-access broadcasting service, the method comprising:
a step of generating a CAS Initial Delivery (CID) key using a seed key and an algorithm, stored in an issuance Personalization Secure Application Module (PerSAM) card, and registering the generated CID key in the CAS chip; and
a step of generating a subscriber key using a seed key and an algorithm, stored in a subscription PerSAM card, inserting the generated subscriber key into a subscription Entitlement Management Message (EMM), and generating a pre-subscription CAS chip by registering the subscription EMM in the CAS chip in which the CID key is registered.

[2] A method of generating pre-subscription CAS chips, for which a broadcasting service subscription process has been performed in advance, in order for a mobile terminal to receive a conditional-access broadcasting service, the method comprising:
a step of a PerSAM card issuance device for issuing a PerSAM card functioning as a device for authenticating a card and loading a key value, generating a Called Subscriber Identification (CSID) list, and providing the CSID list to a CAS server and a CAS chip issuance device;
a step of the CAS server generating a subscription EMM for the CSID list, and providing the subscription EMM to the CAS chip subscription device;
a step of the CAS chip issuance device generating a CID key using a seed key and an algorithm, stored in an issuance PerSAM card, and registering the generated CID key in the CAS chip; and
a step of the CAS chip subscription device generating a subscriber key using a seed key and an algorithm, stored in a subscription PerSAM card, inserting the generated subscriber key into the subscription EMM provided from the CAS server, and then generating a subscription-completed CAS chip by registering the subscription EMM in the CAS chip, issuance of which is completed by the CAS chip issuance device.

[3] The method according to claim 2, wherein the PerSAM card issuance device issues the issuance PerSAM card and the subscription PerSAM card.

[4] A method of at least one mobile terminal receiving a broadcasting service through a client management server for storing subscriber information, and a CAS server, the method comprising:

a step (a) of, when a request for access to a broadcasting service of a specific channel has been made, determining whether the access to the broadcasting service of the corresponding channel is possible by analyzing a subscription EMM of an installed CAS chip;

a step (b) of, if, as a result of the determination at the step (a), it is determined that the access to the broadcasting service of the corresponding channel is not possible, displaying a message inquiring about whether a request for viewing rights has been made to access the broadcasting service of the corresponding channel;

a step (c) of, if a request command is selected using the displayed message inquiring about whether the request for viewing rights has been made, transmitting a viewing rights request message to the CAS server through the client management server; and

a step (d) of, if a viewing rights investment message is received from the CAS server, receiving the broadcasting service of the corresponding channel.

[5] The method according to claim 4, wherein the step (a) step comprises determining whether the access to the broadcasting service of the corresponding channel is possible by checking information about channel viewing qualification and about a charged channel viewing level included in the subscription EMM of the CAS chip.

[6] The method according to claim 4, further comprising, after the step (c), the CAS server affiliating the mobile terminal with the broadcast service of the corresponding channel, and then transmitting a viewing rights investment message to the mobile terminal.

[7] A system for providing a conditional-access broadcasting service, comprising:

one or more mobile terminals, each configured to include a CAS chip, in which a CID key and a subscription EMM are registered, determine whether access to a broadcasting service of a specific channel is possible using the subscription EMM if the corresponding channel is selected for the access to the broadcasting service, and display a message inquiring about whether a request for viewing rights has been made if it is determined that the access to the broadcasting service of the corresponding channel is not possible;

a client management server configured to manage subscriber information, including a CSID list, in which a broadcasting service subscription process has been performed in advance when a CAS chip is issued, and transmit a viewing rights request message when the viewing rights request message is received from one of the mobile terminals; and

a CAS server configured to, when the viewing rights request message is received

from the client management server, perform subscription to a broadcast service of a channel included in the viewing rights request message, and then transmit a viewing rights investment message to the mobile terminal.

[8] The system according to claim 7, wherein the mobile terminal, when a request command is selected using the message inquiring about whether the request for viewing rights has been made, generates the viewing rights request message, including identification information of the mobile terminal and information about the corresponding channel, and then transmits the viewing rights request message to the client management server.

[9] The system according to claim 7, wherein the mobile terminal does not perform an additional subscription procedure for the broadcasting service based on the subscription EMM registered in the CAS chip.

[10] A mobile terminal including a wireless transmission/reception unit, an input unit, a display unit, and an audio unit, and receiving a conditional-access broadcasting service, the mobile terminal comprising:

a CAS chip including a subscription EMM configured to include a subscriber key, and a CID key;

a channel viewing qualification determination unit configured to, when a broadcasting service access request command is received through the input unit, determine whether access to a broadcasting service of a specific channel is possible using the subscription EMM included in the CAS chip, and if, as a result of the determination, it is determined that the access to the broadcasting service of the corresponding channel is not possible, display a message inquiring about whether a request for viewing rights has been made for the corresponding channel on the display unit; and

a viewing rights request unit configured to, if the request command is input through the displayed message inquiring about whether the request for viewing rights has been made, generate and transmit a viewing rights request message including identification information of the mobile terminal and information about the corresponding channel.

[11] The mobile terminal according to claim 10, wherein the channel viewing qualification determination unit receives the broadcasting service of the corresponding channel through the wireless transmission/reception unit if it is determined that the access to the broadcasting service of the corresponding channel is possible.

[12] The mobile terminal according to claim 10, wherein the channel viewing qualification determination unit determines whether the access to the broadcasting service of the corresponding channel is possible by checking information about

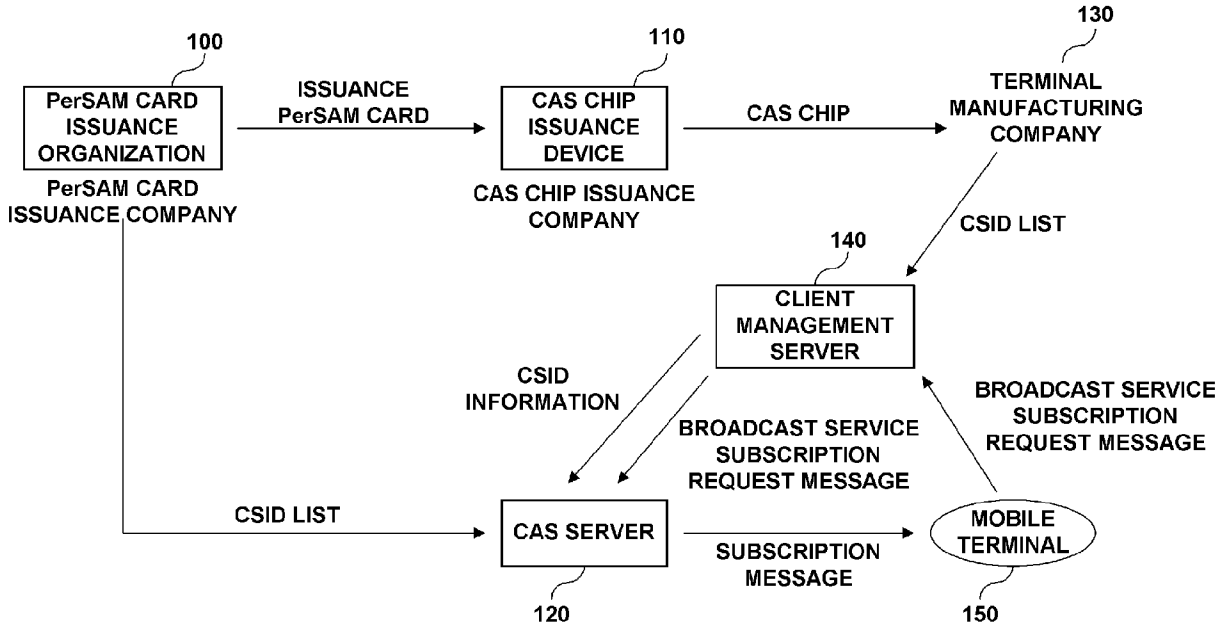
channel viewing qualification and about a charged channel viewing level included in the subscription EMM of the CAS chip.

[13] A pre-subscription CAS chip enabling a conditional-access broadcasting service to be received without performing a subscription procedure when the broadcasting service is initially used, wherein a subscription EMM including a subscriber key is registered in a CAS chip in which a CID key is registered.

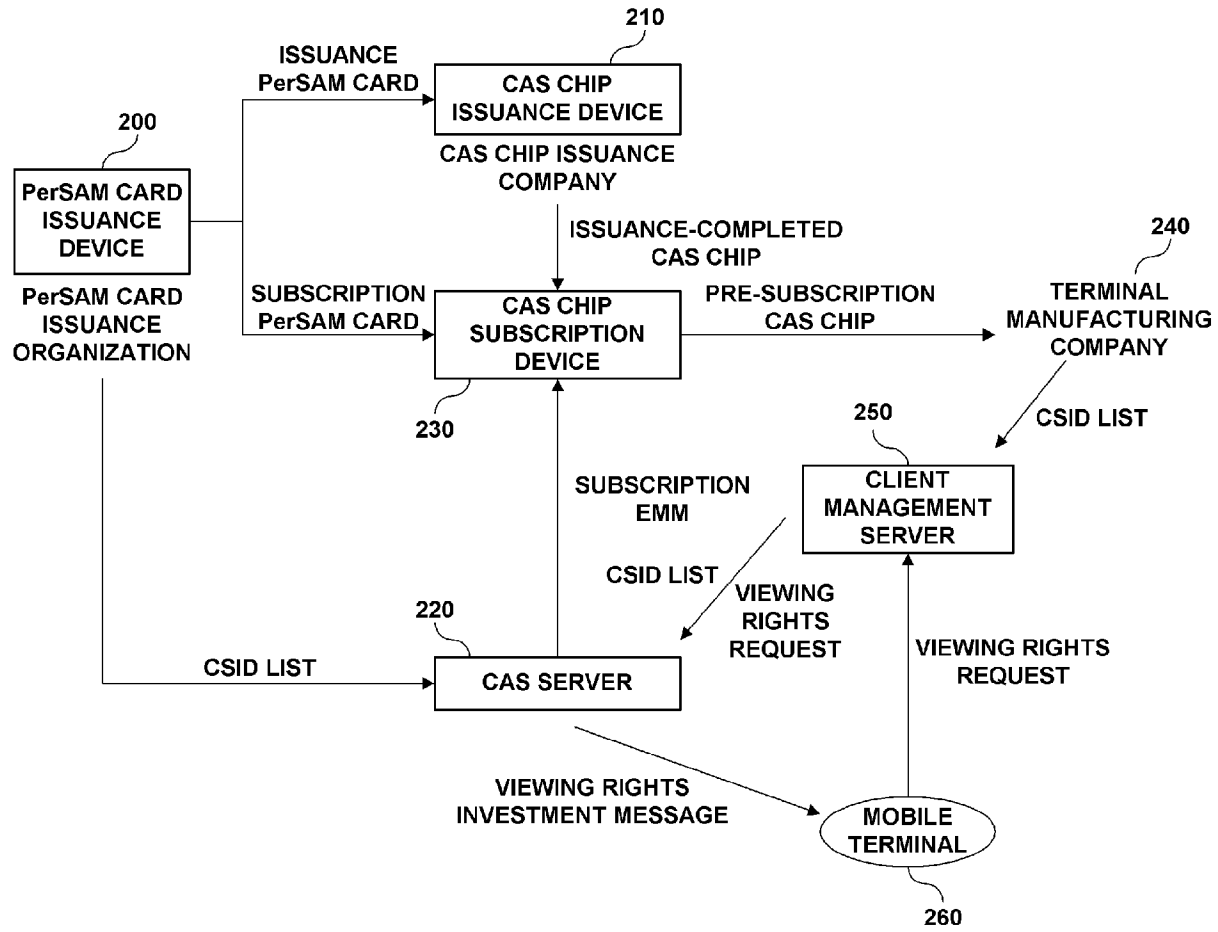
[14] The pre-subscription CAS chip according to claim 13, wherein the CID key is generated using a seed key and an algorithm stored in an issuance PerSAM card.

[15] The pre-subscription CAS chip according to claim 13, wherein the subscriber key is generated using a seed key and an algorithm stored in a subscription PerSAM card.

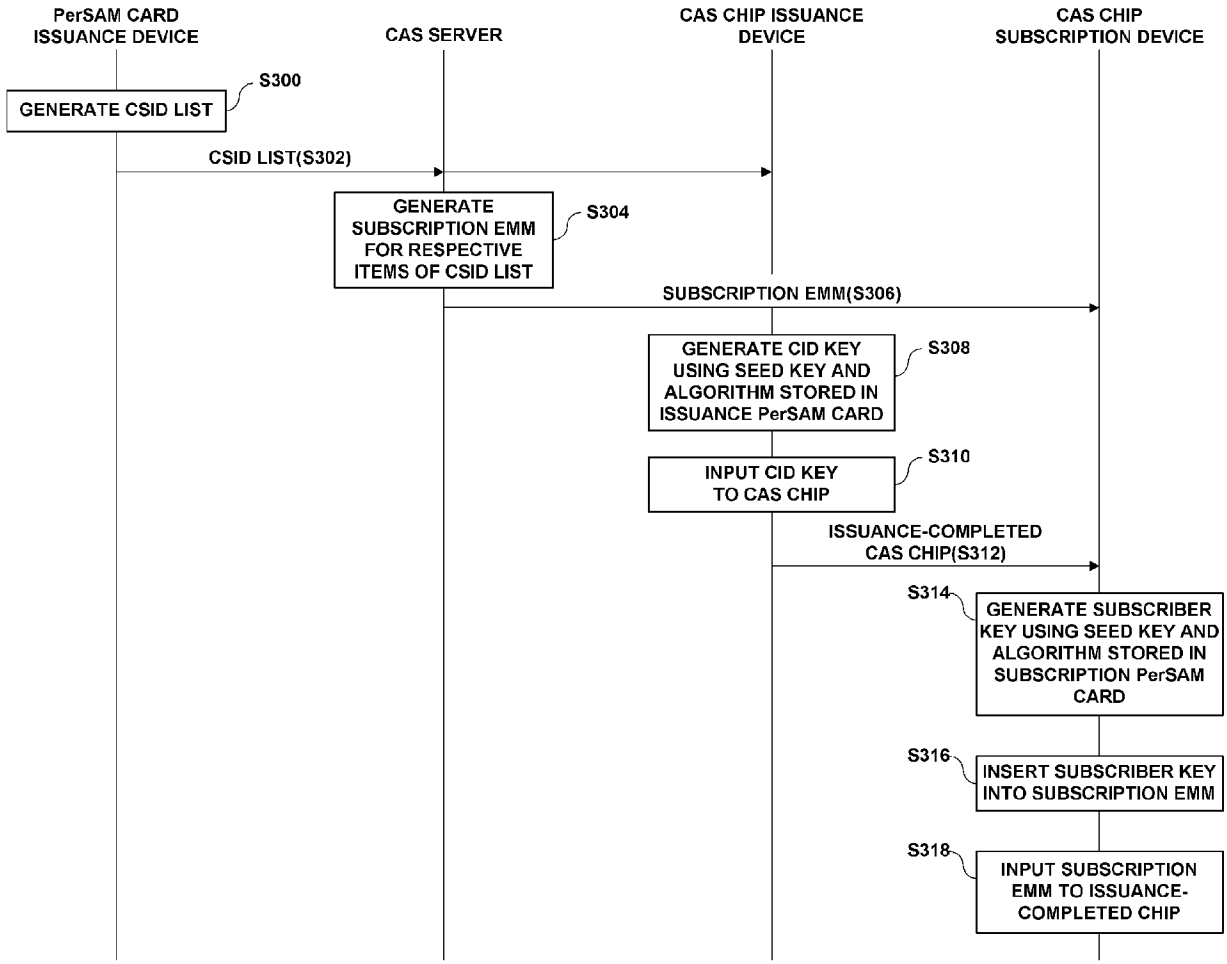
[Fig. 1]


100
PerSAM CARD ISSUANCE ORGANIZATION
PerSAM CARD ISSUANCE COMPANY
ISSUANCE PerSAM CARD
110
CAS CHIP ISSUANCE DEVICE
CAS CHIP ISSUANCE COMPANY
CAS CHIP
130
TERMINAL MANUFACTURING COMPANY
CSID LIST
140
CLIENT MANAGEMENT SERVER
CSID INFORMATION
BROADCAST SERVICE SUBSCRIPTION REQUEST MESSAGE
BROADCAST SERVICE SUBSCRIPTION REQUEST MESSAGE
CSID LIST
CAS SERVER
120
SUBSCRIPTION MESSAGE
MOBILE TERMINAL
150

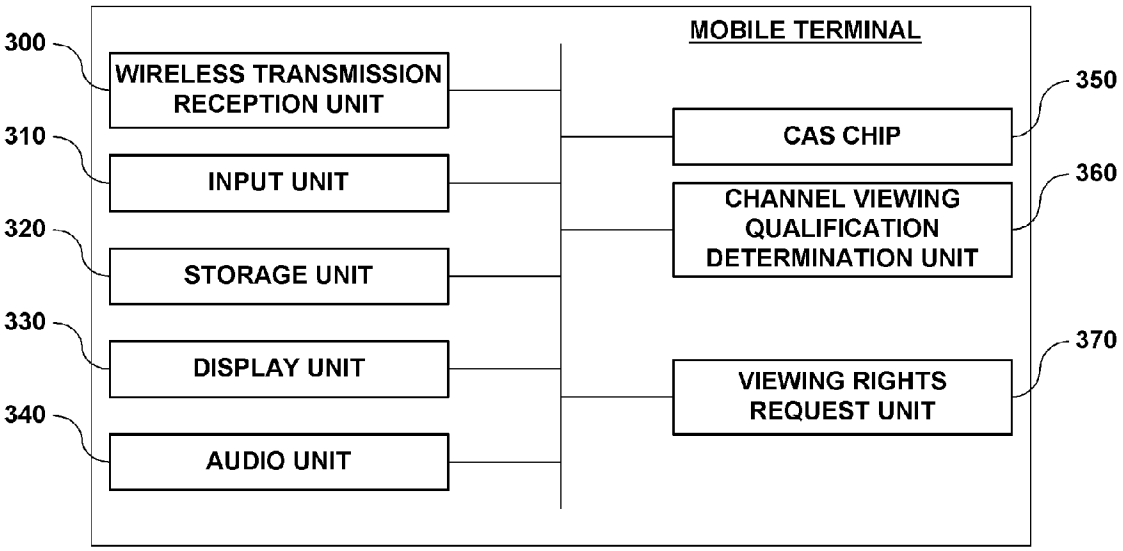
[Fig. 2]


200
PerSAM CARD ISSUANCE DEVICE
PerSAM CARD ISSUANCE ORGANIZATION
ISSUANCE PerSAM CARD
210
CAS CHIP ISSUANCE DEVICE
CAS CHIP ISSUANCE COMPANY
ISSUANCE-COMPLETED CAS CHIP
SUBSCRIPTION PerSAM CARD
CAS CHIP SUBSCRIPTION DEVICE
230
PRE-SUBSCRIPTION CAS CHIP
240
TERMINAL MANUFACTURING COMPANY
CSID LIST
250
CLIENT MANAGEMENT SERVER
SUBSCRIPTION EMM
CSID LIST
VIEWING RIGHTS REQUEST
VIEWING RIGHTS REQUEST
220
CSID LIST
CAS SERVER
VIEWING RIGHTS INVESTMENT MESSAGE
MOBILE TERMINAL
260

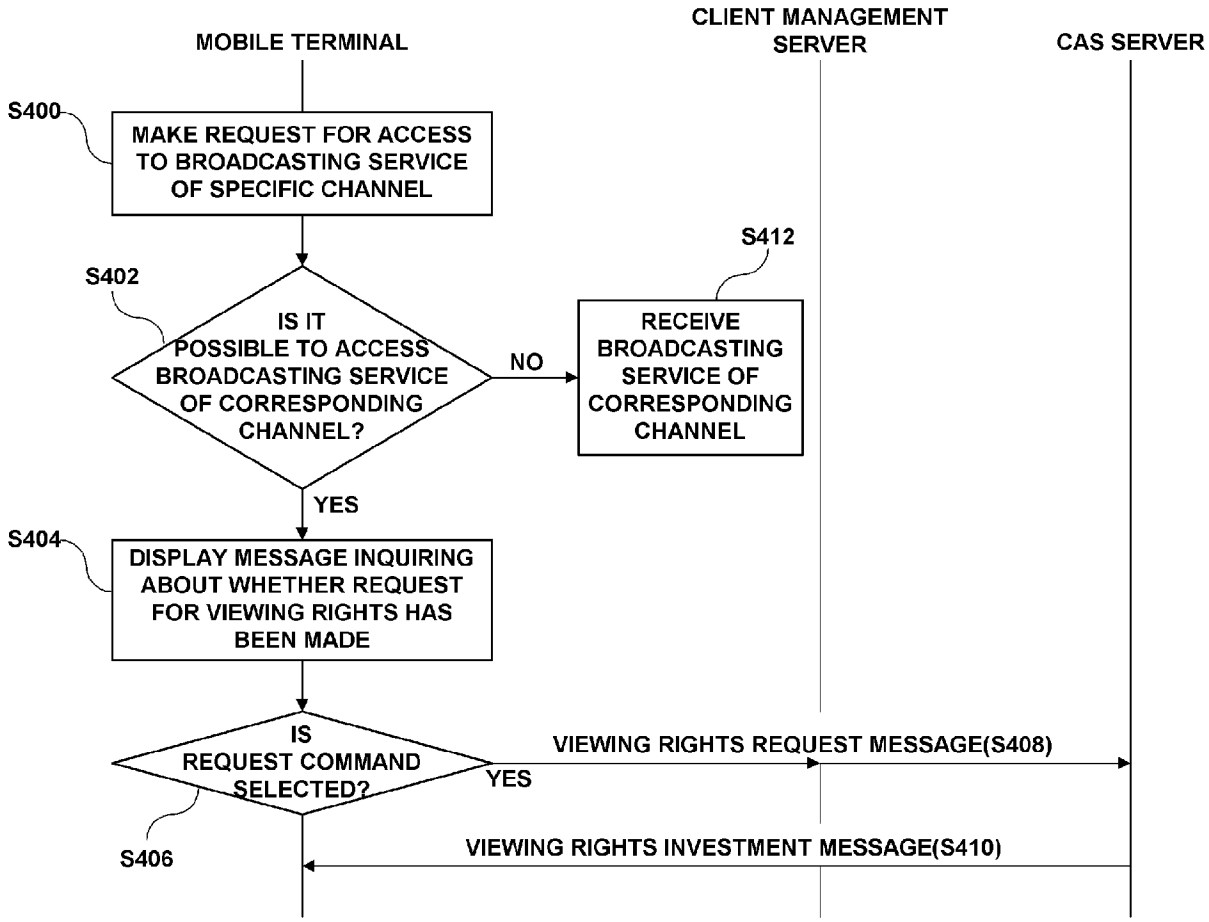
[Fig. 3]


PerSAM CARD ISSUANCE DEVICE
CAS SERVER
CAS CHIP ISSUANCE DEVICE
CAS CHIP SUBSCRIPTION DEVICE
S300
GENERATE CSID LIST
CSID LIST(S302)
GENERATE SUBSCRIPTION EMM FOR RESPECTIVE ITEMS OF CSID LIST
S304
SUBSCRIPTION EMM(S306)
GENERATE CID KEY USING SEED KEY AND ALGORITHM STORED IN ISSUANCE PerSAM CARD
S308
INPUT CID KEY TO CAS CHIP
S310
ISSUANCE-COMPLETED CAS CHIP(S312)
S314
GENERATE SUBSCRIBER KEY USING SEED KEY AND ALGORITHM STORED IN SUBSCRIPTION PerSAM CARD
S316
INSERT SUBSCRIBER KEY INTO SUBSCRIPTION EMM
S318
INPUT SUBSCRIPTION EMM TO ISSUANCE-COMPLETED CHIP

[Fig. 4]


MOBILE TERMINAL
300
WIRELESS TRANSMISSION RECEPTION UNIT
310
INPUT UNIT
320
STORAGE UNIT
330
DISPLAY UNIT
340
AUDIO UNIT
350
CAS CHIP
360
CHANNEL VIEWING QUALIFICATION DETERMINATION UNIT
370
VIEWING RIGHTS REQUEST UNIT

[Fig. 5]


MOBILE TERMINAL
CLIENT MANAGEMENT SERVER
CAS SERVER
S400
MAKE REQUEST FOR ACCESS TO BROADCASTING SERVICE OF SPECIFIC CHANNEL
S402
IS IT POSSIBLE TO ACCESS BROADCASTING SERVICE OF CORRESPONDING CHANNEL?
NO
S412
RECEIVE BROADCASTING SERVICE OF CORRESPONDING CHANNEL
YES
S404
DISPLAY MESSAGE INQUIRING ABOUT WHETHER REQUEST FOR VIEWING RIGHTS HAS BEEN MADE
IS REQUEST COMMAND SELECTED?
YES
S406
VIEWING RIGHTS REQUEST MESSAGE(S408)
VIEWING RIGHTS INVESTMENT MESSAGE(S410)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2008/000616

A. CLASSIFICATION OF SUBJECT MATTER

H04N 5/44(2006.01)i, H04Q 7/24(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 8

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility Models : IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKIPASS(KIPO Internal) : "Conditional Access System"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2006-0041563 A (ONTIMETEK INC.) 12 May 2006 See abstract; claims 1-10; figure 1-3.	1-15
A	KR 10-2004-0056481 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 1 Jul. 2004 See abstract; claims 1-13; figure 1-6.	1-15
A	US 006510515 B1 (RAITH, ALEX KRISTER) 21 Jan. 2003 See abstract; claims 1-88; figure 1-4.	1-15
A	US 005457739 A (CHEVILLER, JEAN-PIERRE LE) 10 Oct. 1995 See abstract; claims 1-17; figure 1-2.	1-15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of 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
29 JULY 2008 (29.07.2008)	**29 JULY 2008 (29.07.2008)**

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea
Facsimile No. 82-42-472-7140

Authorized officer
JUNG, Yun Seok
Telephone No. 82-42-481-8123

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2008/000616

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR 2006041563 A	12.05.2006	None	
KR 2004056481 A	01.07.2004	US 7383562	03.06.2008
		US 2004-123330 A1	24.06.2004
		US 2004-123330 AA	24.06.2004
US 6510515 B1	21.01.2003	AU 1999-48098 A1	05.01.2000
		AU 1999-48098 B2	05.01.2000
		AU 765447 B2	18.09.2003
		BR 9911241 A	06.03.2001
		CA 2335290 AA	23.12.1999
		CN 1190921 C	23.02.2005
		CN 1312990 A	12.09.2001
		JP 2002-518935	25.06.2002
		JP 2002-518935 T2	25.06.2002
		JP 2006-314118 A2	16.11.2006
		KR 10-2001-0052841	25.06.2001
		KR 10-2006-0076327	04.07.2006
		KR 2006076327 A	04.07.2006
		NZ 508561 A	19.12.2003
		US 6510515 B1	21.01.2003
		US 6510515 BA	21.01.2003
		WO 99-66670 A1	23.12.1999
US 5457739 A	10.10.1995	EP 0600067 A1	08.06.1994
		FR 2692740 B1	23.12.1994
		US 5457739 A	10.10.1995
		WO 94-00933 A1	06.01.1994