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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 June 2012 (21.06.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/080972 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/IB2011/055690

(22) International Filing Date:
15 December 2011 (15.12.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2995/DEL/2010 15 December 2010 (15.12.2010) IN

(72) Inventor; and
(71) Applicant : **MOHAN, Taron** [IN/IN]; E-46/9, Okhla Industrial Area, Phase II, New Delhi 110020 (IN).

(74) Agent: **SREEDHARAN, Sunita K.**; SKS Law Associates, C1/611 Mayfair Tower, Charmwood Village, Surajkund, Faridabad, Haryana 121009 (IN).

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

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

**Declarations under Rule 4.17**:

— *as to the identity of the inventor (Rule 4.17(i))*

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

— *of inventorship (Rule 4.17(iv))*

*[Continued on next page]*

(54) Title: STORAGE MEDIA

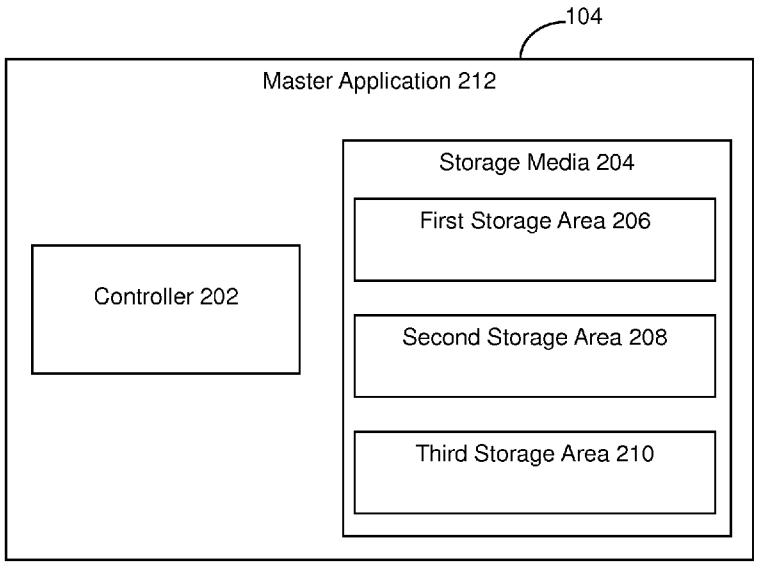


FIG. 2

(57) Abstract: A storage media, a communication device with the storage media and a method for generating a master access key on the storage media is provided. The storage media includes a first storage area with pre-loaded content, a second storage area hosting at least one master access key, and a third storage area that includes an application programming interface that processes a transit access key such that the application programming interface converts the transit access key to the master access key.

WO 2012/080972 A2

**Published**:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

## Title

Storage Media

## Field of the invention

The present invention relates to storage media and more specifically, to a storage media with secure content access management systems.

## Background

Electronic devices like mobile phones, mp3 players etc are increasingly being used for downloading, storage and playback of content especially music / video / games and applications. The content can be downloaded via data networks like general packet radio service (GPRS) or using 3rd Generation (3G) technology or any other wireless / data packet communication technology. In either case, a good quality connection is required to avoid frequent disconnections or failure during download. Further, based upon the user subscription, there may be a cap on the content size or usage period or the number of files etc. that can be downloaded and used through the data pipe. Also, the content to be downloaded may be protected via an encryption algorithm like digital rights management (DRM) technology. DRM technology enables content owners to specify and control the access rights they want to give consumers and the conditions under which it is given.

The content can be unlocked using existing DRM solutions like –

- Mobile device based DRM solutions. Such solutions are limited and lock content to the device / storage media.

- Personal Computer based DRM solutions. These are cumbersome to install, and again lock content to the system.

- Web based DRM solutions. These are difficult to use and need an online connection to authorize access.

Moreover, there may be constraints on the storage capacity of the device for the content downloaded after being unlocked. Thus, there is a need for a solution that securely enables content access on an electronic device without concerns on security and download speed.

**Summary**

The present invention obviates the aforesaid drawbacks and provides a storage media that includes a first storage area with pre-loaded content, a second storage area hosting at least one master access key, and a third storage area that includes an application programming interface (API) that processes a transit access key such that the application programming interface converts the transit access key to the master access key.

In another embodiment, the present invention provides a processing system that includes a controller and a storage device. The storage media includes a first storage area with pre-loaded content, a second storage area hosting at least one master access key, and a third storage area that includes an application programming interface that processes a transit access key such that the application programming interface converts the transit access key to the master access key.

In yet another embodiment, the present invention provides an application server that includes a subscriber profile management system, a content ID management system that stores the content details, a billing / authorization key delivery system that permits delivery of the transit access key upon authorization and a transit key management system that generates a transit access key based upon the subscriber profile, the content details and authorization from billing / authorization key delivery system.

In another embodiment, the present invention provides a method for generating a master access key on a storage media to access encrypted content. The method includes the step of sending a transit access key request for the accessed encrypted content to an application server. Thereafter, the method receives a transit access key and processes the transit access key to obtain a master access key required to decrypt the encrypted content.

The transit access key and the master access key is unique for each content that is accessed.

**Brief Description of Drawings**

FIG. 1 illustrates the environment in which the present invention is implemented.

FIG. 2 illustrates a communication device 104 held by a subscriber 102 in accordance with an embodiment of the present invention.

FIG. 3 illustrates an application server 114 in accordance with an embodiment of the present invention.

FIG. 4 illustrates a method of generating master access key in accordance with an embodiment of the present invention.

**Detailed Description**

As required, detailed embodiments of the present invention are disclosed herein; however, it is to be understood that the disclosed embodiments are merely exemplary of the invention, which can be embodied in various forms. Therefore, specific structural and functional details disclosed herein are not to be interpreted as limiting, but merely as a basis for the claims and as a representative basis for teaching one skilled in the art to variously employ the present invention in virtually any appropriately detailed structure. Further, the terms and phrases used herein are not intended to be limiting; but rather, to provide an understandable description of the invention.

The terms "a" or "an", as used herein, are defined as one or more than one. The term plurality, as used herein, is defined as two or more than two. The terms including and/or containing, as used herein, are defined as comprising (i.e., open language). The term coupled / communicates, as used herein, is defined as connected, although not necessarily directly, and not necessarily mechanically.

FIG. 1 illustrates the environment in which the present invention is implemented. It includes a subscriber 102 who is associated with one or more communication devices 104 to 110 for accessing content stored in the storage media of the communication devices 104 to 110. For example, the device 104 may be a Global System for Mobile Communications (GSM), or Code Division Multiple Access (CDMA) or Wideband Code Division Multiple Access (WCDMA) mobile telephone with an internal / external storage media which can be used to conduct wireless / wired telephone calls and to send Short Messaging Service (SMS) messages. The device 106 may be a desktop workstation with internal and / or external storage media which operates an email client for sending and receiving emails. The device 108 may be a business phone with internal storage media for conducting telephone calls over wired telephone network such as the Public Switched Telephone Network (PSTN). The device 110 may be a laptop computer with internal / external storage media which can be used to send and receive emails via a Wireless Local Area Network (WLAN). It may be seen from the examples that a communication device can be any device capable of communication with a wired / wireless network and with a provision of internal and / or external storage media. Further, the devices 104 to 110 can use the same internal/ external storage media.

The devices 104 to 110 are connected to a communications network 112, either through a wired or a wireless connection. The communications network 112 may be a telecommunications network or a data network which is adapted to transmit packet based and circuit based communication data. For example, the communications network 112 may be used to transmit text and/or video and/or audio and/or multimedia content.

The subscriber 102 communicates with an application server 114 via the communications network 112 using one or more of the communication devices 104 to 110. The application server 114 includes a subscriber profile management system 116, a content ID management system 118 that stores the content details, a transit key management system 120 that communicates with subscriber profile management system 116 and the content ID management system 118, and a billing / authorization key delivery system 122. In an embodiment, the application server 114 is composed of one or several interlinked computers that mean a hardware platform, a software platform based on the

hardware platform and several application programs executed by the system platform formed by the software and hardware platform. The functionalities of the application server 114 are provided by the execution of these application programs which are stored on a storage medium on the application server 114.

FIG. 2 illustrates a communication device 104 held by subscriber 102 in accordance with an embodiment of the present invention. The communication device includes a controller 202 and a storage media 204. For simplicity other components of the communication device 104 are not shown in the diagram. The functioning of such components is known in the art.

The storage media 204 has a first storage area 206, a second storage area 208 and a third storage area 210. The first storage area 206 stores pre-loaded content. The pre-loaded content may be loaded by a vendor from whom the storage media is purchased or pre-loaded by the subscriber 102 via for example, a file transfer protocol or any known technology. Alternately, the content may be pre-loaded by downloading the content over wireless / wired internet connections. The storage media 204, as explained using exemplary devices 104 to 110, can be an internal storage media or an external storage media to the communication device. The internal storage media includes without limitation memory cards / internal memory / flash memory, etc while the external storage media includes without limitation memory cards, flash cards, universal serial bus (USB) drives etc.. The pre-loaded content is wrapped with an encryption mechanism, for example, digital rights management (DRM) or 16 / 128 / 256 bit or more encryption algorithm and needs proper authorization keys to allow usage. Unless the pre-loaded content is unwrapped and authorized for use, it can not be used for playback. Pre-loaded content in the context of the present invention refers to content that is stored in the first storage area of the storage media and is required to be unwrapped /authorized prior to its usage. The pre-loaded content includes audio files, video files, multimedia files, games, applications, or service initiation links.

The second storage area 208 is relatively smaller in size when compared to first storage area 206. For example, the second storage area 208 maybe about 5 MB while the first

storage area 206 maybe about 995 MB in a 1 GB storage media 204. The second storage area 208 is a secure area as it hosts master access key. In an embodiment where the pre-loaded content is wrapped with DRM, the content master access keys are DRM activation keys, which are used to unwrap and authorize the DRM protected content. The master access key maybe codes used to open the wrapped pre-loaded content. The wrapped pre-loaded content is stored in the first storage area 206 on the storage media 204 and cannot be accessed by anyone as the master access keys are not available in the first storage area 206.

The third storage area 210 stores one or more application programming interfaces. The application programming interfaces process a transit access key received from the application server 114 and converts the transit access key to the master access key.

The controller 202 stores the transit access key in the first storage area 206 and the master access key in the second storage area 208. The controller 202 controls / executes the functionalities / applications stored on the storage media 204. It should be noted that each content that is loaded on the first storage area 206 has a unique transit access key / master access key associated to it and may be wrapped for a separate delivery capability (for example, open mobile alliance (OMA) 2.0 compatible). Further, the transit access key / master access key for same content but different subscribers will be different too.

The controller 202 executes the APIs that process the transit access key / authorization keys corresponding to the content to be unwrapped. The transit access keys are stored in the first storage area 206. The master access key is generated using the transit access key and internal logic stored in the first storage area 206. This master access key is mapped to the content being used and limits the usage as per the rights detailed in the transit and the master access key. The transit access key may be delivered over a short message service (SMS) or a wired / wireless connection or may be pre-stored at the first loading point of the content on the storage media.

When the content is accessed for the first time, the controller 202 executes a master application 212 stored in the first storage area 206. The master application 212 sends a

transit access key request to the application server 114. The transit access key request includes without limitation content ID, subscriber identity requesting the key, price point, activation key details for time / duration / access rights and the like. The transit access keys are delivered to the master application on the storage media 204 over, for example, SMS / http either after being generated by the application server 114 or the transit access key details are accessed by the master application from the first storage area 206. The transit access key is processed by the application API for creating a master access key which is then stored in the second storage area 208. This master access key is different from the transit access key delivered over SMS / http as the transit access keys could be intercepted and used by anyone to access and use the content. This master access key creation capability ensures that the actual activation keys / master access keys are not available to anyone but only to the master application and adequate content usage security is ensured. These master access keys are delivered through the application API. This second storage area 208 has a password access and allows the API to read / write into this secure area 208 once the password is verified.

For example, when any pre-loaded content is requested for usage, the master application seeks the content hosted on the first storage area 206. If the content is present and if it is wrapped, it calls for the master access key stored within the second storage area 208 on the storage media 204. This check is performed as it is possible that the storage media hosts free content along with encrypted content. The master access key mapped to this content is accessed and is used via the API to unwrap the content on the storage media 204. In case the master access key is not present, the master application requests the application server 114 to deliver the transit access key for the corresponding content. On receipt of the transit access key, the master application allows the API to generate the master access key which is then stored in the second storage area 208.

FIG. 3 illustrates the application server 114 in accordance with an embodiment of the present invention. The application server 114 includes a subscriber profile management system 116, a content ID management system 118, a transit key management system 120, and a billing / authorization key delivery system 122. While the subscriber profile management system 116 and the content ID management system 118 are separate

databases hosted at the application server 114, it is possible that the two databases are hosted as a common database.

The subscriber profile management system 116 hosts details of the subscribers like subscriber name/ uniqueID, subscribed content, address, etc while the content ID management system 118 hosts details like content type, content price, content time duration mapped to the pricing, etc.

An application runs on the application server 114 which is designed to handle and service requests from communication devices 104 to 110 received via communications network. In an embodiment, the application may be composed of one or more server applications that are executing on one or more servers corresponding to transit key management system 120 and billing / authorization key delivery system 122. Alternatively, application may coordinate with other software on communication devices 104 to 110 to accomplish its tasks.

The transit key management system 120 receives a transit access key request from the subscriber 102 for delivery of a transit access key mapped to a particular content item stored in the storage media 204. This transit access key request includes without limitation content ID, subscriber identity requesting the key, price point, activation key details for time / duration / access rights and the like. The transit key management system 120 manages the generation and delivery of transit activation. For this purpose, the transit key management system 120 exchanges data with the subscriber profile management system 116, the content ID management system 118 and the billing / authorization key delivery system 122.

The transit key management system 120 communicates the billing price points / delivery requests associated with the received transit access key request with the billing / authorization key delivery system 122. Once the transit key management system 120 obtains an authorization to allow the transit access key delivery to the storage media 204 from system 122, it generates the transit access key. In an embodiment, the authorization may be with any billing associated to the request, for example, the request to authorize

access to a movie XXX for a period of 30 days against a payment of INR 100 or can be free for a week or demo trials. Alternately, it could be a simple authorization against the access rights allowed to the subscriber for the same. Thereafter, the transit key management system 120 delivers the transit access key to the master application hosted on the storage media 204 over for example, SMS / http, mapping the access rights against the content ID.

FIG. 4 illustrates a method of generating master access key in accordance with an embodiment of the present invention. When content in the storage media is accessed, the controller launches the master application at step 402. The master application coordinates the data stored in the first storage area (FSA), second storage area (SSA) and the third storage area (TSA). The master application ascertains whether the content to be accessed from the first storage area 206 is free or encrypted at 404. If the content is free, the master application permits display / playback of the content at 406. If the content is encrypted, the master application checks the second storage area 208 for the master access key for the corresponding content at 408. If the master access key is found, the master application transfers control to the password controlled API to allow display / playback the content at 406. If the master access key is not found, the master application further checks the first storage area if the transit access key is stored in the first storage area at 410. If the transit access key is stored, the master application transfers control to API to allow processing of the transit access key and generation of master access key there from for the requested content at 412. The control is then transferred to step 406.

However, if the master access key and the transit access key are not found, the master application sends transit access key request to the application server at 414. The application server generates the transit access key based upon without limitation, price point, content type etc and sends it to the communication device at 416. The master application transfers the control to password controlled API at step 412 to allow processing of the transit access key and generation of master access key there from for the requested content.

It will be appreciated from the teaching of the present invention described above that the content loaded on the storage media is device independent and once the content is unwrapped, the storage media can be used with any device that may support the storage / display / playback media. Further, issues of slow, frequent disconnections, failure during download, data pipe restrictions (GPRS, 3G) etc are taken care off as the content is provided on the storage media and does not need to be buffered / downloaded during playback. The present invention is more secure than the traditional encryption approaches and doesn't need multiple infrastructure elements to be implemented. Further, the subscriber may have an option to preview the content before purchasing.

**I claim:**

1. A storage media comprising:
   - a first storage area comprising pre-loaded content;
   - a second storage area comprising at least one master access key; and
   - a third storage area comprising application programming interface that processes a transit access key, wherein the application programming interface converts the transit access key to the master access key.

2. The media as claimed in claim 1 wherein the pre-loaded content comprises at least one of digital rights management wrapped content, encryption algorithm wrapped content or transit access key.

3. The media as claimed in claim 1 wherein the pre-loaded content comprises multimedia files, applications, games and service initiation links.

4. The media as claimed in claim 1 wherein the storage media comprises a memory card, a flash memory card, or a device resident / external storage media.

5. The media as claimed in claim 1 wherein the application programming interface is password controlled.

6. The media as claimed in claim 1 wherein the transit access key and the master access key is unique for each content that is accessed.

7. A communication device comprising:
   - a controller; and
   - a storage media comprising a first storage area comprising pre-loaded content, a second storage area comprising at least one master access key, and a third storage area comprising application programming interface that

processes a transit access key to convert the transit access key to the master access key.

8. The communication device as claimed in claim 7 wherein the controller receives the transit access key over one of Internet, file transfer protocol or messaging service.

9. The communication device as claimed in claim 7 wherein the controller stores the transit access key in the first storage area and the master access key in the second storage area.

10. The communication device as claimed in claim 7 wherein the pre-loaded content comprises at least one of digital rights management wrapped content, encryption algorithm wrapped content or transit access key.

11. The communication device as claimed in claim 7 wherein the pre-loaded content comprises multimedia files, applications, games and service initiation links.

12. The communication device as claimed in claim 7 wherein the storage media comprises a memory card, a flash memory card, or a device resident / external storage media.

13. The communication device as claimed in claim 7 wherein the application programming interface is password controlled.

14. The communication device as claimed in claim 7 wherein the transit access key and the master access key is unique for each content that is accessed.

15. An application server comprising:

- a subscriber profile management system;
- a content ID management system that stores the content details;

- a billing / authorization key delivery system that permits delivery of the transit access key upon authorization; and
- a transit key management system that generates a transit access key based upon the subscriber profile, the content details and authorization from billing / authorization key delivery system.

16. A method for generating a master access key on a storage media to access encrypted content, the method comprising:
    - sending a transit access key request for the accessed encrypted content to an application server;
    - receiving a transit access key; and
    - processing the transit access key to obtain a master access key required to decrypt the encrypted content, wherein the transit access key and the master access key is unique for each content that is accessed .

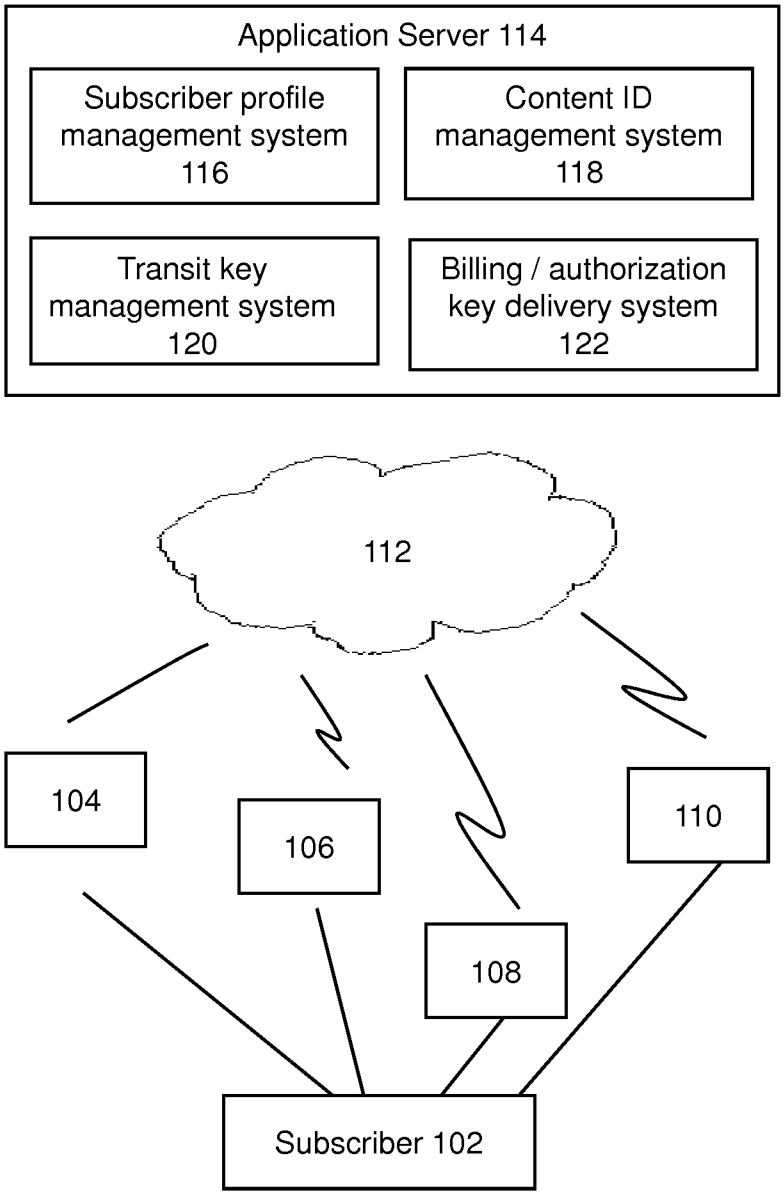
Application Server 114
Subscriber profile management system 116
Content ID management system 118
Transit key management system 120
Billing / authorization key delivery system 122
112
104
106
108
110
Subscriber 102

FIG. 1

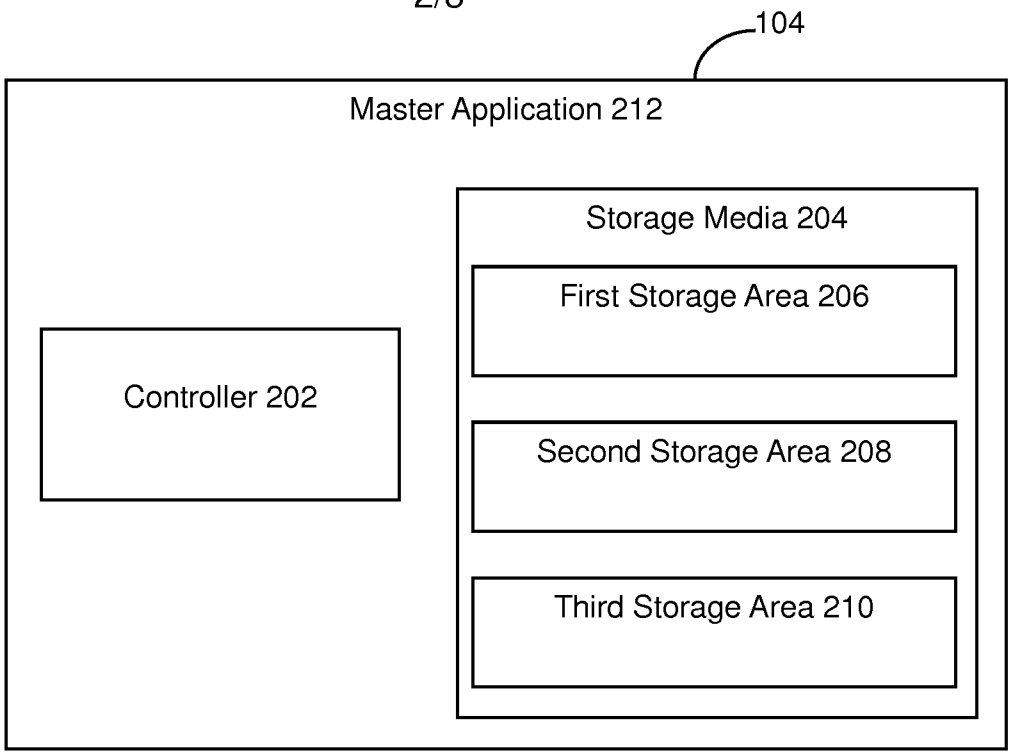
104
Master Application 212
Storage Media 204
First Storage Area 206
Controller 202
Second Storage Area 208
Third Storage Area 210

**FIG. 2**

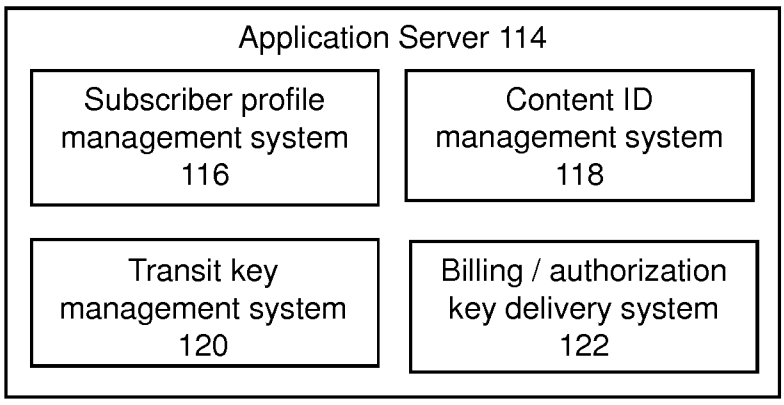
Application Server 114
Subscriber profile management system 116
Content ID management system 118
Transit key management system 120
Billing / authorization key delivery system 122

**FIG. 3**

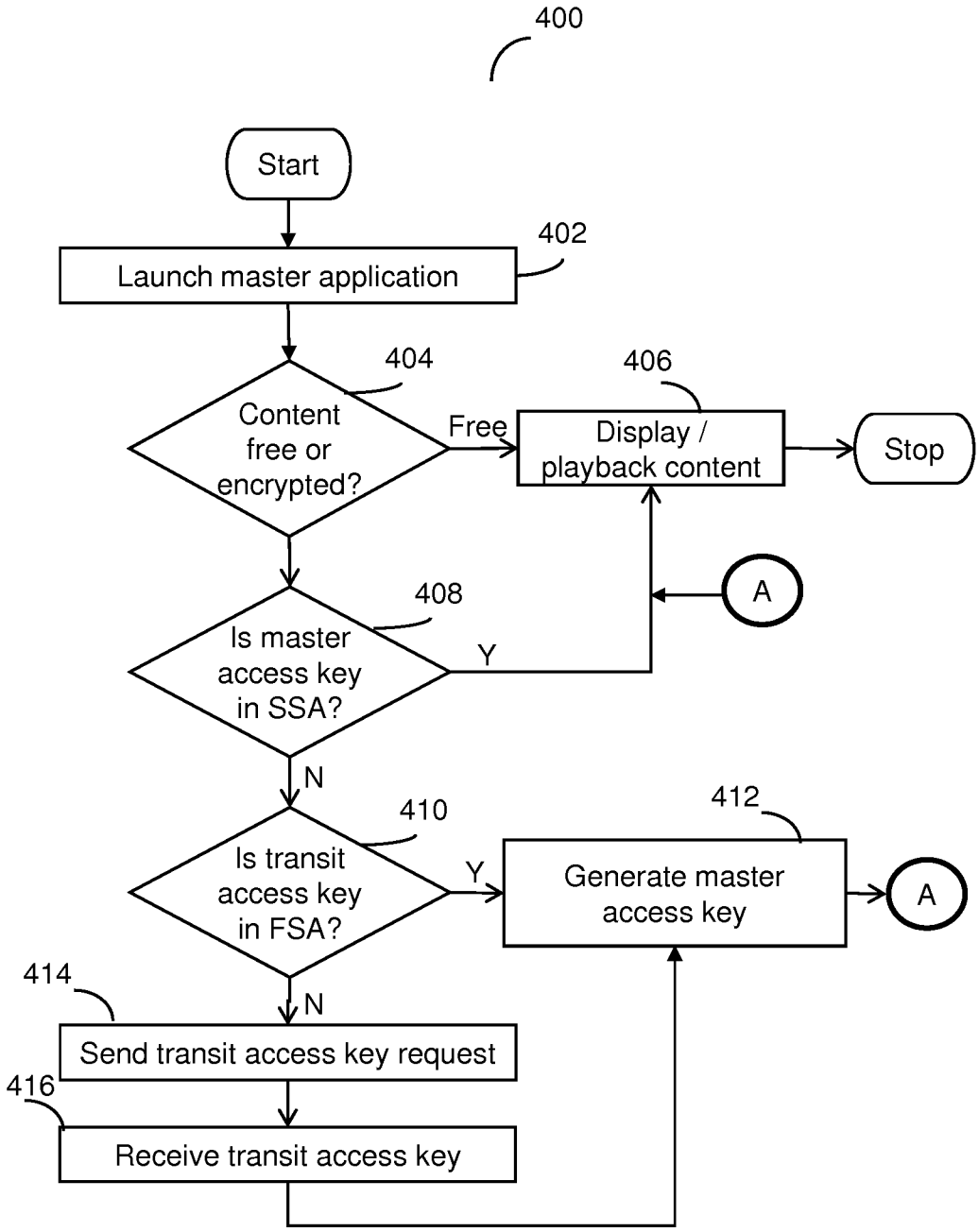
400
Start
Launch master application
402
Content free or encrypted?
404
Free
Display / playback content
406
Stop
A
Is master access key in SSA?
408
Y
N
Is transit access key in FSA?
410
Y
Generate master access key
412
A
N
414
Send transit access key request
416
Receive transit access key

FIG. 4