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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 March 2009 (19.03.2009)

PCT

(10) International Publication Number
WO 2009/036394 A1

(51) International Patent Classification:
H04N 7/16 (2006.01) *H04N 5/00* (2006.01)

(21) International Application Number:
PCT/US2008/076318

(22) International Filing Date:
12 September 2008 (12.09.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/971,813 12 September 2007 (12.09.2007) US

(71) Applicant *(for all designated States except US)*: **DEVICEFIDELITY, INC.** [US/US]; 1701 N. Greenville Avenue, Suite 1110, Richardson, TX 75081 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **JAIN, Deepak** [US/US]; 7534 Spicewood Drive, Garland, TX 75044 (US).

(74) Agents: **COX, Michael, E.** et al.; Fish & Richardson P.C., P.O. Box 1022, Minneapolis, MN 55440-1022 (US).

(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, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, 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).

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*

(54) Title: WIRELESSLY RECEIVING BROADCAST SIGNALS USING INTELLIGENT CARDS

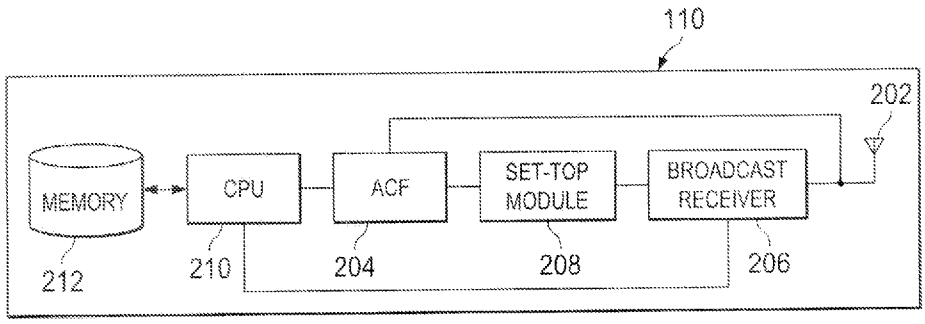


FIG. 2

(57) Abstract: The present disclosure is directed to a system and method for wirelessly receiving broadcast signals using intelligent cards. In some implementations, a service card includes a physical interface, a communication module, memory, and a service module. The physical interface connects to a port of a mobile host device. The mobile host device includes a Graphical User Interface (GUI). The communication module wirelessly receives broadcast signals encoding content. The memory stores user information used to decrypt the encoded content independent of the mobile host device. The stored information is associated with a content provider. The service module decrypts the encoded content in response to at least an event and presents the content through the GUI of the mobile host device.

WO 2009/036394 A1

Wirelessly Receiving Broadcast Signals Using Intelligent Cards

CLAIM OF PRIORITY

This application claims priority to U.S. Patent Application Serial No. 60/971,813, filed on September 12, 2007, the entire contents of which are hereby incorporated by reference.

TECHNICAL FIELD

This invention relates to network communications and, more particularly, to wirelessly receiving broadcast signals using intelligent cards.

BACKGROUND

Portable electronic devices and tokens have become an integrated part of the regular day to day user experience. There is a wide variety of common portable and handheld devices that users have in their possession including communication, business and entertaining devices such as cell phones, music players, digital cameras, smart cards, memory token and variety of possible combinations of the aforementioned devices and tokens. All of these devices share the commonality that consumer are accustomed to carrying them with them most of the time and to most places. This is true across the various demographics and age groups regardless of the level of the sophistication of the consumer, their age group, their technical level or background.

These common handheld devices offer options for expandable memory. Micro Secure Digital (microSD) is the popular interface across high-end cellphones while SD and MultiMediaCard (MMC) interfaces are also available in limited models. MicroSD is the least common denominator supported by the majority of these devices and tokens (in terms of size). In addition, adaptors are available to convert a MicroSD into MiniSD, SD, MMC and USB Although most popular MP3 player (iPOD) offer's a proprietary interface, competing designs do offer standard interfaces. Digital cameras offer mostly SD and MMC while extreme Digital (xD) is another option. Micro and Mini versions of these interfaces are also available in several models. Mini-USB is increasingly available across cellphones, digital cameras and MP3 players for synchronization with laptops.

Various content providers and service providers are developing digital broadcast networks that will be able to provide TV like viewing channels on mobile devices. Several new mobile handset models are also being developed that embed a miniature broadcast receiver that can receive these digital broadcast signals and use a media player software to offer channel viewing to the consumer. In order to secure access and provide access to premium content like movies, subscription based pay-TV content and music albums, the service provider uses a specially designed conditional access system (CAS) which is able to verify the user's subscription and unscramble premium content before rendering it for viewing.

Such capability can be added to the PC, by adding a hardware transceiver that can be added to the PC using peripheral interfaces such as USB, PCMCIA, PCIA or mini-PCI (and others). To control access, the conditional access system is implemented in the same hardware and comprises of a smart card that securely stores the user's identity and his subscription privileges. In addition, the service provider provides an Electronic Service Guide that the user can use to select the channels that he wishes to view. This software is typically installed on the PC together with the access driver for the hardware. In some options, the default channel guide provided by the operating system of the PC (such as Windows Vista / MacOS etc.) can be used.

There are other consumer devices such as smartphones, MP3 players, game players and portable vides players that may make use of broadcast content connection for useful applications. Since the hardware for the broadcast receiver and the conditional access system is specialized and requires a dedicated processor to receive and unscramble content, many of these devices may not be upgraded with an embedded broadcast reception capability. In addition, these devices also lack PCMCIA or USB type expansion slots where broadcast receiver and CAS hardware could be inserted. These devices also typically lack the slot for a hardware security token such as a smart card in order to provide secure access to a fee based premium TV content. These devices also need memory for the users to record content captured through these devices. The need for such memory is growing at a rapid rate.

SUMMARY

The present disclosure is directed to a system and method for wirelessly receiving broadcast signals using intelligent cards. In some implementations, a service card includes a physical interface, a communication module, memory, and a service module. The physical interface connects to a port of a mobile host device. The mobile host device includes a Graphical User Interface (GUI). The communication module wirelessly receives broadcast signals encoding content. The memory stores user information used to decrypt the encoded content independent of the mobile host device. The stored information is associated with a content provider. The service module decrypts the encoded content in response to at least an event and presents the content through the GUI of the mobile host device.

The details of one or more embodiments of the invention are set forth in the accompanying drawings and the description below. Other features, objects, and advantages of the invention will be apparent from the description and drawings, and from the claims.

DESCRIPTION OF DRAWINGS

FIGURE 1 is an example service system in accordance with some implementations of the present disclosure;

FIGURE 2 is an example service card of FIGURE 1 in accordance with some implementations of the present disclosure;

FIGURE 3 is an example Central Processing Unit (CPU) of the service card of FIGURE 2;

FIGURE 4 is a schematic diagram illustrating personalization processes of intelligent cards;

FIGURES 5A and 5B are flow charts illustrating an example method for initialize an intelligent card;

FIGURE 6 is a flow chart illustrating an example method for activating a service card;

FIGURES 7A to 7C are examples of call flow illustrating call sessions with an intelligent card;

FIGURE 8 is a flow chart illustrating an example method for synchronizing local and remote memory; and

FIGURE 9 is a flow chart illustrating an example method for receiving content.

Like reference symbols in the various drawings indicate like elements.

DETAILED DESCRIPTION

FIGURE 1 is a block diagram illustrating an example service system 100 for receiving broadcast signals using an intelligent card. For example, the system 100 may include a SecureDigital (SD) card that receives broadcast signals (e.g., terrestial digital video broadcast) and presents content through a mobile host device based, at least in part, on the received broadcast signals. Broadcast signals may include terrestrial and/or satellite signals that encode images, audio, video, and/or other content. For example, the broadcast signals may be Digital Video Broadcasting - Handheld (DVB-H), DVB-H2, Digital Video Broadcasting - Satellite services to Handhelds (DVB-SH), Forward Link Only (FLO), Digital Multimedia Broadcasting (DMB), Multimedia Broadcast Multicast Service (MBMS), satellite radio, and/or others. Aside from SD, the system 100 may include other interfaces that connect an intelligent card to the host device such as, for example, MultiMediaCard (MMC), miniSD, microSD, Universal Serial Bus (USB), Apple iDock, Firewire, and/or others. An intelligent card may be a device configured to insert into or otherwise attach to a mobile host device and access or otherwise receiving broadcast signals (e.g., e.g., satellite radio) independent of the mobile host device. In some implementations, the intelligent card may be shaped as a microSD card, miniSD card, or microSD card including, for example, notches, raised portions and/or other features. In some implementations, the system 100 may modify, translate, or otherwise convert received broadcast signals to a form processable by or otherwise native to the mobile host device 102. In converting the signal protocols, the system 100 may present media content otherwise foreign to the mobile device 102. Foreign, as used herein, means any component, object, value, variable, content and/or data and/or data schema that is not directly processable, accessible, receivable or otherwise capable of communicating with the mobile devices 102. In some implementations, the conversion of the foreign content to compatible forms may be transparent to the user of the mobile device 102. By providing an intelligent card, the system 100 may access foreign content without

either requiring additional hardware, software, and/or firmware in the mobile host device.

At a high level, the system 100 includes the mobile devices 102a and 102b and the content provider 104 coupled to the network 106. The mobile device 102 includes a GUI 108 for providing presenting content and a service card 110 for independently converting foreign content to forms compatible with the mobile device 102. In some implementations, the service card 110 may selectively switch antenna on and off in response to an event such as a selection of a graphical element using the GUI 108. The network 108 includes a content distribution stations 112a and 112b (*e.g.*, broadcast tower, satellite, IP broadcast tower) for broadcasting content to the service cards 110.

Each mobile device 102 comprises an electronic device operable to interface with the service card 110. For example, the mobile device 102 may receive and transmit wireless and/or wireless communication with the system 100. As used in this disclosure, the mobile devices 102 are intended to encompass cellular phones, data phones, pagers, portable computers, SIP phones, smart phones, personal data assistants (PDAs), digital cameras, MP3 players, camcorders, video player, game player, one or more processors within these or other devices, or any other suitable processing devices capable of communicating information with the service card 110. In some implementations, the mobile devices 102 may be based on a cellular radio technology. For example, the mobile device 102 may be a PDA operable to wirelessly connect with an external or unsecured network. In another example, the mobile device 102 may comprise a smartphone that includes an input device, such as a keypad, touch screen, mouse, or other device that can accept information, and an output device that conveys information associated with a transaction with the offline store 102, including digital data, visual information, or GUI 108.

The GUI 108 comprises a graphical user interface operable to allow the user of the mobile device 102 to interface with at least a portion of the system 100 for any suitable purpose, such as viewing content channels and/or displaying the Electronic Service Guide (ESG). Generally, the GUI 108 provides the particular user with an efficient and user-friendly presentation of data provided by or communicated within the system 100 and/or also an efficient and user-friendly means for the user to self-manage settings and access channels offered by the content provider 104. The GUI 108 may comprise a plurality of customizable frames or views having interactive

fields, pull-down lists, and/or buttons operated by the user. The term graphical user interface may be used in the singular or in the plural to describe one or more graphical user interfaces and each of the displays of a particular graphical user interface. The GUI 108 can include any graphical user interface, such as a generic media player or touch screen, that processes information in the system 100 and presents the results to the user.

The service card 110 can include any software, hardware, and/or firmware configured to receive broadcast signals from the distribution stations 112. For example, the service card 110 may receive content broadcasted by the content provider 104 and translate, map or otherwise convert the received content to forms viewable with the mobile device 102. In some implementations, the service card 110 can present received content through the GUI 108. In some implementations, the service card 110 may include one or more chipsets that execute an operating system and security processes to receive broadcast signals independent of the mobile host device 102. In doing so, the mobile device 102 may not require additional hardware, software, and/or firmware to present foreign content such as digital TV, IP-TV, satellite radio, satellite TV, and/or other broadcast services. In some implementations, the service card 110 may execute one or more of the following: wirelessly receive signals broadcasted by the distribution stations 112; determine subscription levels of the card 110 based, at least in part, on locally-stored user information; descramble content available to the user in accordance with the subscription levels; translate between broadcast protocols (*e.g.*, DVB, FLO, MBMS, DMB) and protocols compatible with the service card 110; translate between service-card protocols and protocols compatible with mobile device 102; present broadcasted content for viewing through the GUI 108; execute applications locally stored in the service card 110; selectively switch the antenna on and off based, at least in part, on one or more events; authenticate user based, at least in part, on information locally stored in the service card 110; present the Electronic Service Guide application for the user through the GUI 108 for selection of available channels; present menu options for managing recordable content and configuring options for the personal video recorder application via GUI 108; present the personal video recorder application for viewing of recorded content via GUI 108; and/or others. In some implementations, the service card 110 may receive a broadcast signal in response to at least a user selecting a graphical

element in the GUI 108. In some implementations, the service card 110 may selectively switch the antenna between an on and off state in response to one or more events (e.g., user request, completion of broadcast, change of host device, change of network connection of the host device, change of location). The service card 110 may include a communication module with a protocol translation module, antenna tuning circuit, power circuit and a miniature antenna tuned to receive broadcast signals.

In some implementations, the service card 110 may initiate receiving to a broadcast signal in response to at least a user selecting a graphical element in the GUI 108. In some implementations, the service card 110 may selectively switch the antenna between an on and off state in response to one or more events. The one or more events may include a user request, completion of broadcasted content, insertion of card 110 in a different mobile device, location change, timer events, detection of incorrect user ID and password entered by the user, message received from the content provider 104 using a broadcast/cellular signal, and/or others. For example, the service card 110 may receive one or more commands to switch the antenna off from the distribution tower 112 or from the cellular core network. In some implementations, the service card 110 may request user identification such as a PIN, a user ID and password combination, biometric signature, and/or others.

In regards to translating between protocols, the service card 110 may process information in, for example, ISO 7816, a stand security protocol, and/or others. In this case, the service card 110 may translate between a broadcast protocol and the service-card protocol. Broadcast protocols may include DVB, DMB, FLO and/or MBMS. In some implementations, ISO 7816 commands may be encapsulated within interface commands used to transmit data between the mobile host device 102 and the card 110. In addition, the service card 110 may interface the mobile device 102 through a physical interface such as MicroSD, Mini-SD SD, MMC, miniMMC, microMMC, USB, miniUSB, microUSB, firewire, Apple iDock, and/or others. In regard to security processes, the service card 110 may implement one or more Conditional Access Systems (VideoGuard, Irdeto Access, Nagravision, Conax, Viaccess and Mediaguard (a.k.a. SECA)). The CAS may use encryption algorithms to descramble or otherwise decrypt broadcast signals to determine encoded content. In some implementations, the service card 110 may execute private key (symmetric algorithms) such as Data Encryption Standard (DES), Triple DES (TDES) and/or others or public key

(asymmetric algorithms) such as RSA, elliptic curves, and/or others to implement the chosen CAS system compliant with the service provider. For example, the service card 110 may include one or more encryption keys such as public-private keys. In addition, the service card 110 may include memory (*e.g.*, Flash, EEPROM) including a secured token accessible by the content providers 104 to store access rights of the user. The service card 110 may also store user data, applications, offline Webpages, and/or other information. For example, the service card 110 may include a secure token that identifies content that the user subscribes to or can otherwise access. In addition, the service card 110 may execute or otherwise include digital rights management technology to substantially prevent illegal copying, storing or distributing or other violations of digital rights.

The service card 110 may present content (*e.g.*, audio, video) to the user using the GUI 108. In response to initiating foreign-content access, the service card 110 may automatically present an offline Web page through the GUI 108. In some implementations, the offline Web page can be associated with a content provider 104. In some implementations, the service card 110 can be backward compatible and operate as a mass storage device. For example, if the wireless interface of the service card 110 is not available or deactivated, the service card 110 may operate as a mass storage device enabling users to access data stored in the memory component (*e.g.*, Flash). In some implementations, the service card 110 can execute a set of initialization commands in response to at least insertion into the mobile device 102. These initialization commands may include determining device related information for the mobile device 102 (*e.g.*, device ID, device capabilities), determining user relating information (*e.g.*, user ID and password), incrementing counters, setting flags and activating/deactivating functions according to pre-existing rules and/or algorithms.

In some implementations, the service card 110 may automatically execute one or more fraud control processes. For example, the service card 110 may identify an operational change and automatically deactivate the card 110. The service card 110 may execute two fraud control processes: (1) determine a violation of one or more rules; and (2) automatically execute one or more actions in response to at least the violation. In regards to rules, the service card 110 may locally store rules associated with updates to operational aspects of the service card 110. For example, the service card 110 may store a rule indicating a change in mobile host device 102 is an

operational violation. In some implementations, the service card 110 may store rules based, at least in part, on updates to one or more of the following: device ID; subscription period; registration information; CAS parameters; and/or other aspects. In response to one or more events matching or otherwise violating rules, the service card 110 may execute one or more processes to substantially prevent access to broadcasted content. In some implementations, the service card 110 may execute a command based, at least in part, on an event type. For example, the service card 110 may re-execute an activation process in response to at least a specified event type. In some implementations, the service card 110 may execute a command to disconnect the GUI 108 from the service card 110. The service card 110 may present a disconnection notification through the GUI 108 prior to executing the command. In some implementations, the service card 110 may provide options for the user to configure a rule table (PVR rule table) related to the personal video recorder application. This may allow the user to specify rules according to which content is automatically recorded by the service card.

In regards to accessing broadcasted services, the interface between the service card 110 and the access point 112 or distribution tower 112 may be DVB-H, DMB, MBMS, or FLO for Mobile-TV and Sirius/XM for Satellite Radio or other digital Mobile-TV and/or satellite broadcast interfaces. Based on the PVR Rule Table, the service card 110 may receive content from the broadcast content provider 204 and store the content in real-time to the memory. The content player of the mobile device 102 may then access the stored content using, for example, a media player and access to the GUI 108. The antenna mode of the service card 110 may be set to physical authentication only because the service card 110 may use the mobile device 102 to present video and/or audio. The secure element of the service card 110 may operate as set-top box (CAS token). In this implementation, the secure element my operate in two different roles as illustrated in Table 1 below.

Table 1

DVB-H / MediaFLO or other Mobile-TV Broadcast	**XM / Sirius or other Satellite Radio Broadcast**
Digital TV transmissions are generally scrambled to allow content providers and content providers to offer pay-per-use and tiered subscription services to the end users. In order to perform this capability, there are two types of protection that may be implemented: a) Service Protection: In this case, subscription related access rights are stored on a secure token (such as the smart card in Cable or Satellite Set-top boxes). As and when a user purchases a premium channel / package or pay-per-use event, access right to the same is downloaded to this secure token. The algorithms and method of protection are generally provider dependent and in generally referred to as the CAS (Conditional Access System). The secure element in the plug-in, being a secure token, will host the CAS algorithm compliant with the content provider and the access keys management that are managed dynamically depending on the content subscribed to by the end-user b) Content Protection: In this case, the content download contains digital rights management technology wherein it cannot be illegally copied, stored or distributed. If required by the content provider, the secure element will implement the required DRM scheme of the content provider such that the content downloaded or viewed is used by the end-user according to the restrictions imposed by the content provider	This is a simpler case where the satellite radio content providers may offer service to users who have purchased a particular subscription plan. Only protection applicable here-in is hence the service protection which would be implemented by the secure element. The secure element will store an active subscription for the end-user which will enable the plug-in to securely receive transmission and produce output

The table is for illustration purposes only. The activation of the service card 110 may include some, all, or different aspects of the chart.

In some implementations, the user may acquire the service card 110 when subscribing to a content provider's broadcast content service. The activation process may depend on whether the mobile device 102 includes an interface such as a screen, a keyboard and internet access. In some implementations, the service card 110 may be activated online or offline. Online activation may occur when the device 102 includes an interface such as screen, keyboard and wireless internet access (Cellphone, laptop or Wireless PDA), offline activation may occur when a device 102 does not include internet capability or doesn't have a screen / keyboard (MP3/4 players). These two activation processes are illustrated below in Table 2.

Table 2:

Online Activation	**Offline Activation**
When the device has internet access and has a screen / keyboard, it is assumed to have an internet browser and capable of browsing to any URL. In this case, when the plug-in inserts, it performs the plug-in bootstrap and authentication process. Once successful, the device is able to take the user to a landing page on a browser where the user can perform the registration and activation process.	In this case, the user may cradle his device to the PC that has an internet access and launch the included activation software. This software will take the user to the content provider's landing page to perform the registration and activation process

The table is for illustration purposes only. The activation of the service card 110 may include some, all, or different aspects of the chart.

In some implementations, the service card 110 may operate as a personal video recorded (PVR). For example, the service card 110 may include GBs of flash memory that may store multimedia content. The service card 110 may include a microcontroller sufficiently strong to operate a recording process while streaming the content to the content player on the mobile device 102 at the same time. The service card 110 may include an application residing on a protected area of the memory that would run a PVR and an Electronic Service Guide (ESG) application to enable a user to review the content program and select the programs recording. The DVR and ESG application may enable playing back the recorded content from the memory. In comparison, the service card 110 may include a stronger microcontroller that has an internal clock (*e.g.*, an ARM series processor). The service card 110 may include a special form factor that allows the SD interface to connect to a SD to USB adaptor for

laptop use. In some implementations, the service card 110 includes a secure element OS to enable the functionality described above. The service card 110 may implement a CAS algorithm based on content provider's specification. The secure element OS may structure data in the secure element to enable storage of subscription data for the end user. The microcontroller OS may be capable of personalizing the secure element by loading/updating user subscription parameters. In addition, the microcontroller OS may be capable of presenting the service card 110 as SD mass storage to the mobile device 102. In addition to operating the memory, secure element, the broadcast receiver chipset and the antenna availability, the microcontroller OS may implement a very fast content writing function on the memory in real-time, receive the ESG in real-time from the broadcast content provider 204, and interact with the host device's content player to display the content. The secure element may operate as the CAS and subscription storage token because of cryptographic capabilities. The device application section may be used to store provider specific applications that operate from this segment of the memory or are installed on the mobile device 102 from this segment of the memory.

In some implementations, the service card 110 may include broadcast applications and WAN connectivity. In this case, the user may perform payment to a third party by connecting over the internet and/or performing peer-to-peer payment by connecting to another user with the same functionality. In some implementations, the service card 110 may include broadcast applications and broadcast reception capabilities. In this case, the user may purchase content in real-time and pay for merchandize advertised over the broadcast content in real-time.

The content distribution network 106 facilitates wireless or wired communication between the content providers 104 and any other local or remote computer. The distribution network 106 may be all or a portion of an enterprise or secured network. While illustrated as single network, the distribution network 106 may be a continuous network logically divided into various sub-nets or virtual networks without departing from the scope of this disclosure, so long as at least a portion of distribution network 106 may facilitate communications of transaction information between the content providers 104. In some implementations, the distribution network 106 encompasses any internal or external network, networks, sub-network, or combination thereof operable to facilitate communications between

various computing components in system 100. Network 106 may communicate, for example, Internet Protocol (IP) packets, Frame Relay frames, Asynchronous Transfer Mode (ATM) cells, voice, video, data, and other suitable information between network addresses. Network 106 may include one or more local area networks (LANs), radio access networks (RANs), metropolitan area networks (MANs), wide area networks (WANs), all or a portion of the global computer network known as the Internet, and/or any other communication system or systems at one or more locations. In some implementations, the distribution network 106 include the content providers 104a-c.

Content provider 104a-c comprises an electronic device (e.g., computing device) operable to broadcast content. In some implementation, the content provider 104 can provide broadcast signals that encodes content displayable by the service card 110. The content provider 104 may transmit one or more of the following: serial programs (*e.g.*, television series), movies, news, opinions, education content, training, sports events, Web pages; advanced blogging sites, travel-related content, food and/or cooking content; entertainment; topical movies and/or videos (*e.g.*, surfing, sailing, racing, extreme sports, etc.); political content (*e.g.*, campaigning); adult content; court and/or trail programming; local-government content (*e.g.*, C-SPAN); local programming (*e.g.*, Wayne's World); performing arts (*e.g.*, theater, concerts, music videos, etc.); virtual shopping malls; satellite radio content (audio only channels); and/or other content. The provided content may be in any suitable format such as MPEG, streaming, MP3, realtime, WMV, and/or others. In the illustrated implementation, the content provider 104 includes a conditional access module 124 for authenticating a user and associated privileges prior to providing access to services. For example, the CAS module 124 may transmit a request for information associated with the user such as subscriber ID, receiver ID, PIN, username and password, and/or other information. Based, at least in part, on information associated with the user information, the CAS module 124 may determine available services, content, level of services, and/or other aspects of the requested foreign service.

In some implementations, the service card 110 may operate in accordance with one or more of the following modes: active receiver; self train; killed; memory; inactive; and/or other modes. The service card 110 may operate active-receiver mode to present the service card 110 as a broadcast receiver. In this mode, the service card 110 may execute applications access broadcast services through the broadcast network

108. After the antenna of the service card 110 is activated in this mode, the network 108 may detect the presence of the service card 110. In this implementation, the mobile device 102 may not require additional software to access the services.

In regards to the self-train mode, the service card 110 may receive personalization information from another receiver. In some implementations, the self-train mode can be activated by a special action (e.g., a needle point press to a small switch, entry of an administrative password via the GUI 108). In response to at least activating this mode, the service card 110 may be configured to receive personalization data over, for example, the short range wireless interface from another peer service card or a wired connection with the home broadcast receiver. Personalization data received in this mode may include encrypted information that is stored in secured memory of the service card 110. In some implementations, the service card 110 in this mode may receive the information through a wireless interface of a transmitter and/or others. The service card 110 may then synthesize the information that corresponds to the user account and personalize an internal security module that includes, for example, service applications for accessing services from the provider 104 and associated user credentials. The self-train mode may be used to re-personalize the service card 110 in the field. In some implementations, all previous data can be deleted if the self-train mode is activated. The self-train mode may be a peer-to-peer personalization mode where the card 110 may receive personalization information from another service card 110. This mode may represent an additional personalization mode as compared with factory, store and/or Over-The-Air (OTA) personalization scenarios which may be server to client personalization scenarios. In some implementations, the self-train mode may be a peer-to-peer personalization mode where the service card 110 receives personalization information from another service card. Since two service cards 110 are used in this mode, this mode may be different from a server-to-client personalization scenario as with a factory, store, and OTA personalization.

In regards to the inactive mode, the service card 110 may temporarily deactivate the wireless interface. In some implementations, the inactive mode can be activated through the physical interface with the mobile device 102 such as a SD interface. In response to at least the activation of the inactive mode, the service card 110 may temporarily behave as only a mass-memory card. In some implementations,

the card 110 may also enter this state when the reset needle point is pressed. In this mode, the service card 110 may preserve locally-stored information including user information. In this mode, the service card 110 may execute the activation process and if successful may return to the active mode. The content provider 104 may use this mode to temporarily prevent usage in response to at least identifying at least potentially fraudulent activity.

In regards to the killed mode, the service card 110 may permanently deactivate the wireless interface. In some implementations, the killed mode is activated through the physical interface with the mobile device 102 such as a SD interface. In response to at least the activation of the killed mode, the service card 110 may permanently behaves as a mass memory stick. In the event that the reset needle point is pressed, the service card 110 may, in some implementations, not be made to enter any other modes. In addition, the service card 110 may delete user information in memory in response to at least this mode being activated. In some implementations, the providers 104 may use this mode to delete data from a service card 110 that is physically lost but still connected to the broadcast network 108.

In regards to the memory mode, the service card 110 may operate as a mass memory stick such that the memory is accessible through conventional methods. In some implementations, the service card 110 may automatically activate this mode in response to at least being removed from the host device, inserted into a non-authorized host device, and/or other events. The service card 110 may be switched to active mode from the memory mode by, for example, inserting the card 110 into an authorized device or may be switched from this mode into the self-train mode to re-personalize the device for a new host device or a new user account. In some implementations, the memory mode may operate substantially same as the inactive mode.

In some implementations, the service card 110 may be re-personalized/updated such as using software device management process and/or a hardware reset. For example, the user may want to re-personalize the service card 110 to change host devices, to have multiple host devices, and/or other reasons. In regards to the software device management, the user may need to cradle the new host device with the service card 110 inserted to launch the software device management application. In some implementations, the software management application can be an application directly

installed on a client, integrated as a plug-in to a normal synchronization application such as ActiveSync, available via a browser plug-in running on the plug-in provider's website, and/or other sources. The user may log into the application and verify their identity, and in response to verification, the application may allow access to a devices section in the device management application. The device management application may read the service card 110 and display the MAC addresses, signatures of the devices that he has inserted his plug-in to, and/or other device specific information. The mobile device 102 may be marked as active and the host device may be shown as disallowed or inactive. The application may enable the user to update the status of the new host device, and in response to at least the selection, the device management application may install the signature on the new host device and mark update the status as allowable in secure memory of the service card 110. The user may be able to also update the status of the mobile device 102 to disallowed. Otherwise, both devices may be active and the service card 110 may be switched between the two devices. In regards to the hardware reset process, the use may use the reset needle point press on the physical service card 110 to activate the self-train mode. In this mode, the user data may be deleted and have to be reloaded. When the service card 110 is inserted into the new host device, the provisioning process may begin as discussed above.

In some aspects of operation, the content provider 104 may transmit information to the mobile host device 102 using the service card 110 in response to at least an event. The information may include, for example, service information (e.g., access history), scripts, applications, Web pages, and/or other information associated with the content provider 104. The event may include completing access to a service, determining a service card 110 is outside the operating range of a broadcast network 108, receiving a request from a user of the mobile host device, and/or others. For example, the content provider 104 may identify a mobile host device 102 associated with a card 110 that accessed a service and transmit service information to the service card 110 using the broadcast or cellular core network 108. In addition or alternatively, the content provider 104 may request information from the mobile host device 102, the service card 110 and/or the user using the broadcast or cellular core network 108. For example, the content provider 104 may transmit a request to update the Electronic Service Guide to the card 110 through the broadcast or cellular core network 108.

FIGURE 2 is a block diagram illustrating an example service card 110 in accordance with some implementations of the present disclosure. In general, the service card 110 may independently receive broadcast signals to present through the GUI 108 of the mobile host device 102. The service card 110 is for illustration purposes only and may include some, all, or different elements without departing from the scope of the disclosure.

As illustrated, the service card 110 includes an antenna 202, an Antenna Control Function (ACF) module 204, a broadcast receiver 206, a set-top module 208, a CPU 210 and memory 212. The antenna 202 receives wireless broadcast signals such as satellite radio and/or TV. In some implementations, the AFC module 204 can selectively switch the antenna 202 between an active state and an inactive state in response to at least an event. A switching event may include a user selection through the GUI 108. In some implementations, the switching event may be based, at least in part, on operational aspects of the mobile host device 102 such as completion of presentation of multimedia. In addition, the ACF module 204 may dynamically adjust the impedance of the antenna 202 to tune the receive frequency. The ACF module 204 may selectively switch the antenna 202 on and off in response to at least a command from the CPU 210. In some implementations, the antenna 202 can be connected through a logic gate to allow for code from the CPU 210 to turn the antenna 202 on and off through the ACF module 204.

The receiver 206 can include any software, hardware, and/or firmware configured to receive broadcast signals using the antenna 202. For example, the receiver 206 may convert broadcast signals to set top module processable signals. In some implementations, the receiver 206 may translate a broadcast protocol to a security protocol. For example, the receiver 206 may translate to ISO 7816, a stand security protocol, and/or others. Broadcast signals may include DVB, DMB, FLO and/or MBMS. In some implementations, ISO 7816 commands may be encapsulated within interface commands used to transmit data between the mobile host device 102 and the card 110.

The set-top module 208 can include any software, hardware, and/or firmware configured to unscramble broadcast signals to a form displayable through the GUI 110. For example, the set-top module 208 may launch the CAS application to unscramble the broadcast signal to determine encoded content and decrypt the encoded content to a

presentable form (*e.g.*, MPEG 4). In some implementations, the set-top module 208 may authenticate one or more aspects of the mobile host device, user, and/or card 110. In some implementations, the set-top module 208 may authenticate a user by verifying a physical connection with a user using user information such as user ID and password, biometric information (*e.g.*, fingerprint), a PIN entered by the user, a x.509 type certificate that is unique to the user and stored on the host device 110, and/or other processes. For example, the set-top module 208 may compare user information provided through the GUI 108 with user information stored in the local memory 212. Alternatively or in addition, the set-top module 208 may authenticate the mobile host device 102 by comparing a device signature with a locally-stored certificate. In some implementations, the user can select a user-id and password or PIN or certificate at provisioning time. If this case, the CPU 210 may instantiate a software plug-in on the host device. For example, a software plug-in may request the user for his user-id and password or PIN in real time, read a user certificate installed on the device (*e.g.*, x.509), and/or others. The operation of the software plug-in may be customized by the provider. Regardless, the returned user data may be compared with user data stored in the memory 212. In case of a successful match, the ACF module 204 may activate the antenna 202. In case of an unsuccessful match of a certificate and/or user information, the card 110 is deactivated. In case of unsuccessful user ID and password match, the user may be requested to repeat user-id and password attempts until a successful match or the number of attempts exceeds a threshold. The card provider may customize the attempt threshold.

In some implementations, the set-top module 208 may implement one or more Conditional Access Systems with accompanying encryption algorithms to decode broadcast signals. For example, the set-top module 208 may include or otherwise identify a one or more keys for decoding broadcast content. In some implementations, the service card 110 may execute private key (symmetric algorithms) such as Data Encryption Standard (DES), Triple DES (TDES) and/or others or public key (asymmetric algorithms) such as RSA, elliptic curves, and/or others. For example, the service card 110 may include one or more encryption keys such as public-private keys. In connection with decoding signals, the CAS in the set-top module 208 may identify a subscription profile identifying content available to the user. For example, the CAS in the set-top module 208 may determine one or more broadcast channels available to the

user and decode one of the available broadcast channels for presenting through the GUI. The set top box 208 may present the Electronic Service Guide to the user through the GUI. The Electronic Service Guide may not only present the choice of channels available to the user but may also make available a detailed listing of programming content available on each channel. The Electronic Service Guide may also interface to the Personal Video Recorder application in the card and provide options to the user to set up timers to record certain programs. The Electronic Service Guide may also be periodically updated by the service provider through the set top box.

The CPU 210 can include any software, hardware, and/or firmware that manages operational aspects of the card 110 independent of the mobile host device 102. For example, the CPU 210 may include a runtime environment for executing broadcast applications for accessing foreign content encoded in broadcast signals. In some implementations, the CPU 210 may execute one or more of the following: interfacing the mobile host device 102 such as translating between protocols; determining operational aspects of the mobile host device 102; transmitting commands to the mobile host device 102 to substantially control one or more hardware components (*e.g.*, GUI 108, memory); identifying events associated with activating and deactivating the antenna 202; executing broadcast applications that present foreign content from the provider 104; executing media protocol conversion to adapt the content according to the capabilities of the media player accessible through the GUI, execute the PVR application to record content on the flash memory of the card, provide access to stored content on the flash memory, manage the set top box using ISO 7816 interface, mange the broadcast chipset using a high-speed IP interface, manage the memory using a standard memory controller interface; and/or others. In some implementations, the CPU 210 may transmit to the ACF module 204 switching commands in response to an event such as a user request, completion of a transaction, and/or others. In some implementations, the CPU 210 may switch the antenna 202 between active and inactivate mode using the ACF module 204 based, at least in part, on a personalization parameter defined by, for example, a user, distributor (*e.g.*, content provider), and/or others. For example, the CPU 210 may activate the antenna 202 when the service card 110 is physically connected to a host device and when a handshake with the host device is successfully executed. In some implementations,

the CPU 210 may automatically deactivate the antenna 202 when the service card 110 is removed from the host device. In regards to the handshaking process, the CPU 210 may execute one or more authentication processes prior to activating the service card 110 and/or antenna 202 as illustrated in FIGURE 7. For example, the CPU 210 may execute a physical authentication, a device authentication, and/or a user authentication. For example, the CPU 210 may activate the antenna 202 in response to at least detecting a connection to the physical interface with the host device (e.g., SD interface) and successful installation of the device driver for mass memory access (e.g., SD device driver) on the host device. In some implementations, device authentication may include physical authentication in addition to a signature comparison of a device signature stored in memory 212 that was created during first-use (provisioning) to a run-time signature calculated using, for example, a unique parameter of the host device 102. In the event no host device signature exists in the memory 212, the CPU 210 may bind with the first compatible host device 102 that the card 110 is inserted into. A compatible host device 102 may be a device that can successfully accomplish physical authentication successfully. If a host-device signature is present in the memory 212, the CPU 210 may compare the stored signature with the real-time signature of the current host device 102. If the signatures match, the CPU 210 may proceed to complete the bootstrap operation. If the signatures do not match, host device 102 may be rejected, bootstrap is aborted and the card 110 may be returned to the mode it was before being inserted into the device.

The memory 212 may include a secure and non-secured section. In this implementation, the secure memory 212 may store one or more user credentials that are not accessible by the user. In addition, the memory 212 may store offline Web pages, applications, service history, and/or other data. In some implementations, the memory 212 may include Flash memory from 64 MB to 32GB. In addition, the memory 212 may be partitioned into user memory and device application memory. The memory 212 may store signatures of allowed host devices and/or antenna modes. In some implementations, the memory 212 may include secure portions designed to be accessible only by the content provider.

FIGURE 3 illustrates is a block diagram illustrating an example CPU 210 of FIGURE 2 in accordance with some implementations of the present disclosure. In general, the CPU 210 includes personalized modules that receive foreign content

independent of the mobile device 102. The illustrated CPU 210 is for example purposes only, and the CPU 210 may include some, all or different modules without departing from the scope of this disclosure.

In some implementations, the service card 110 can include a host controller 302, a real-time framework 304, a broadcast application 306, a real-time OS 308, a high speed IP interface 310, a memory controller 312, and a security module driver 314. In some implementations, the host controller 302 includes an interface layer, an API/UI layer, a Web server, and/or other elements associated with the mobile host device 102. The host controller 302 includes interfaces to the host device, *i.e.*, physical connection. In regards to the physical interface, the host controller 302 may physically interface the mobile device 102 using an SD protocol such as MicroSD, Mini-SD or SD (full-size). In some implementations, the physical interface may include a converter/adapter to convert between two different protocols based, at least in part, on the mobile device 102. In some implementations, the mobile device 102 may communicate using protocols such as USB, MMC, Firewire, iPhone proprietary interface, and/or others. In addition, the host controller 302 may include any software, hardware, and/or firmware that operates as an API between the mobile device 102 and the service card 110. Prior to accessing services, the service card 110 may automatically install drivers in the mobile device 102 in response to at least insertion. For example, the service card 110 may automatically install a microSD device driver in the device 102 to enable the service card 110 to interface the mobile device 102. In some implementations, the service card 110 may install an enhanced device driver such as a Mass Memory with Radio (MMR) API. In this implementation, the interface can drive a class of plug-ins that contain mass memory as well as a radio interface. The MMR API may execute one or more of the following: connect/disconnect to/from the MMR controller (Microcontroller in the plug-in); transfer data using MM protocol (*e.g.*, SD, MMC, XD, USB, Firewire); send encrypted data to the MMR controller; receive Acknowledgement of Success or Error; received status word indicating description of error; turn radio on/off; send instruction to the service card 110 to turn the antenna on with specifying the mode of operation (e.g., sending mode, listening mode); transmit data such as send instruction to controller to transmit data via the radio; listen for data such as send instruction to controller to listen for data; read data such as send instruction to controller to send the data received by the listening radio;

and/or others. In some implementations, MMR can be compliant with TCP/IP. In some implementations, API encapsulated ISO 7816 commands may be processed by the security module in addition to other commands.

In some implementations, host controller 302 can operate in accordance with the two processes: (1) the service card 110 as the master and the mobile device 102 as the slave; and (2) the card UI as the master. In the first process, the host controller 302 may pass one or more commands to the mobile device 102 in response to, for example, insertion of the service card 110 into a slot in the mobile device 102, a request from the GUI 108, and/or other events. In some implementations, the host controller 302 can request the mobile device 102 to execute one or more of following functions: Get User Input; Get Signature; Display Data; Send Data; Receive Data; and/or others. The Get User Input command may present a request through the GUI 108 for data from the user. In some implementations, the Get User Input may present a request for multiple data inputs. The data inputs may be any suitable format such as numeric, alphanumeric, and/or other strings of characters. The Get Signature command may request the mobile device 102 to return identification data such as, for example, a phone number, a device ID like an IMEI code or a MAC address, a network code, a subscription ID like the SIM card number, a connection status, location information, Wi-Fi beacons, GPS data, and/or other device specific information. The Display Data command may present a dialog to the user through the GUI 108. In some implementations, the dialog can disappear after a period of time, a user selection, and/or other event. The Send Data command may request the mobile device 102 to transmit packet data using its own connection to the external world (*e.g.*, SMS, cellular, Wi-Fi). The Receive Data command may request the mobile device 102 to open a connection channel with certain parameters and identify data received through the connection. In some implementations, the command can request the mobile device 102 to forward any data (*e.g.*, SMS) satisfying certain criteria to be forwarded to the service card 110.

In regards to the UI as master, the host controller 302 may execute one or more of the following commands: security module Command/Response; Activate/Deactivate; Flash Memory Read/Write; Send Data with or without encryption; Receive Data with or without decryption; URL Get Data / URL Post Data; and/or others. The security module commands may relate to security functions

provided by the card and are directed towards the security module within the service card 110 (*e.g.*, standard ISO 7816 command, proprietary commands). In some implementations, the commands may include encryption, authentication, provisioning of data, creation of security domains, update of security domain, update of user credentials after verification of key, and/or others. In some implementations, the commands may include non security related smart card commands such as, for example, read service history commands. The read service guide command may perform a read of the Electronic Service Guide data stored in the memory 212 of the service card 110. In some implementations, certain flags or areas of the memory 212 may be written to after security verification. The Activate/Deactivate command may activate or deactivate certain functions of the service card 110. The Flash Memory Read/Write command may execute a read/write operation on a specified area of the memory 212. The Read command may be used by the Media Player to receive the streaming content selected by the user for viewing. The Send Data with or without encryption command may instruct the mobile device 102 to transmit data using a wireless connection. In addition, the data may be encrypted by the service card 110 prior to transmission using, for example, keys and encryption capability stored within the set-top module 208. The Receive Data with or without decryption command may instruct the service card 110 to switch to listening mode to receive data from its wireless connection with the cellular core network 108. In some implementations, data decryption can be requested by the security module using, for example, keys and decryption algorithms available on the security module, *i.e.*, on-board decryption. The URL Get Data/URL Post Data command may instruct the host controller 302 to return pages as per offline get or post instructions using, for example, offline URLs.

In some implementations, the host controller 302 may assign or otherwise associate URL style addressing to certain files stored in the memory 212 (*e.g.*, flash) of the service card 110. In some implementations, the host controller 302 can locate a file using the URL and returns the file to the GUI 108 using standard HTTP, HTTPS style transfer. In some implementations, the definition of the files can be formatted using standard HTML, XHTML, WML and/or XML style languages. The file may include links that point to additional offline storage locations in the memory 212 and/or Internet sites that the mobile device 102 may access. In some implementations, the host controller 302 may support security protocols such as SSL. The host

controller 302 may transfer an application in memory 212 to the mobile device 102 for installation and execution. The host controller 302 may request the capabilities of the browser on the device 102 using, for example, the browser user agent profile, in order to customize the offline Web page according to the supported capabilities of the device and the browser, such as, for example, supported markup language, screen size, resolution, colors and such.

As part of the Real time OS, the real-time framework 304 may execute one or more functions based, at least in part, on one or more periods of time. For example, the real-time framework 304 may enable an internal clock available on the CPU 210 to provide timestamps in response to at least requested events. The real-time framework 304 may allow certain tasks to be pre-scheduled such that the tasks are executed in response to at least certain time and/or event based triggers. This aspect is used by the Real Time OS to generate triggers to launch the Personal Video Recorder application, Set top box and the broadcast chipset to begin reception and recording of the content if the user set timer for content recording has been met. In some implementations, the real-time framework 304 may allow the CPU 210 to insert delays in certain transactions. In some implementation, a part of WAP standards called WTAI (Wireless Telephoney Application Interface) can be implemented to allow offline browser pages on the card 110 to make use of functions offered by the mobile device 102.

The broadcast application 306 can include any software, hardware, and/or firmware that receive broadcast content. For example, the broadcast application 306 may receive a request for content through the GUI and receive the associated broadcast signal in response to at least the request. In some implementations, the broadcast application 306 may execute one or more of the following: transmit properties of the service card 110; to the broadcast Content Distribution System; download the Electronic Service Guide data from the Broadcast Content Distribution System; tune the antenna to the right frequency based, at least in part, on selection made by the user via the Electronic Service Guide viewed on the GUI; receive the broadcasted content based, at least in part, on the subscription information; transmit user profile and authentication data to the content distribution system, receive instructions and data to update the Electronic Service Guide, receive request from the CPU to begin or end the broadcast reception; and/or other processes. In these case, the broadcast application

310 may present media through the GUI 108 that is otherwise not accessible by the mobile host device 102, *i.e.*, foreign content.

The real-time OS 308 may execute or otherwise include one or more of the following: real-time framework 304; a host process that implements the physical interface between the service-card CPU and the mobile device 102; an interface that implements the physical interface between the service-card CPU and the security module; a memory-management process that implements the ISO 7816 physical interface between the service-card CPU and the memory 212; an application-layer process that implements the API and UI capabilities; the ACF module 204; power management; and/or others. In some implementations, the real-time OS 308 may manage the physical interface between the service-card CPU and the memory 212 that includes memory segmentation to allow certain memory areas to be restricted access and/or data buffers/pipes. In some implementations, the CPU 210 may include a separate memory controller 312 for managing the local memory 212. In some implementations, the real-time OS 308 may include a microcontroller OS configured to personalizing the set-top module 208 such as by, for example, converting raw data (account number, subscription information, user profile, receiver ID, CAS parameters) into secure encrypted information. In addition, the microcontroller OS may present the card 110 as a microSD mass storage to the host device 102. The microcontroller OS may partition the memory 212 into a user section and a protected device application section. In this example, the device application section may be used to store provider specific applications that either operate from this segment of the memory or are installed on the host device 102 from this segment of the memory.

The high speed IP interface 318 may provide the hardware protocol implementation and/or drivers for digital streaming content corresponding to the broadcasting signals received by the broadcast receiver. For example, the through this high speed IP interface, the CPU mayreceive non-encrypted or non-scrambled digital streaming content associated with free or off-air or non-premium channels. In this case, this streaming content is directly made available to the media player of the host device after appropriate media protocol translation if required. For example, through this high speed IP interface, the CPU may receive encrypted or scrambled digital content associated with premium or subscription channels. In this case, the content is

first sent to the set-top box for decoding and unscrambling and then forwarded to the media player after any appropriate media translation.

FIGURE 4 is a schematic diagram 400 of personalization of a intelligent card (*e.g.*, the service card 110). In particular, the intelligent card may be personalized prior to being issued to a user, *i.e.*, pre-issuance, or after being issued to a user, *i.e.*, post-issuance. In regards to pre-issuance, intelligent cards may be personalized in mass batches at, for example, a factory. In this example, each intelligent card may be loaded with user credentials, security framework, applications, offline Web pages, and/or other data. In some implementations, a intelligent card may be personalized individually at, for example, an electronics retailer branch. In this case, a intelligent card may be individually loaded with data associated with a user after, for example, purchasing the card. As for post issuance, the intelligent card may be personalized wirelessly. For example, the service card 110 may be personalized through a cellular connection established using the mobile device 102. In some implementations, an intelligent card may be personalized by synchronizing with a computer such as client 104. The service card 110 may receive from an enterprise at least associated with the service provider 104 that personalization data prior to activation including user credentials, broadcast applications, personal video recorder applications and at least one of operational flags, rule table or user interface. The personalization data present in the card may be updated after activation using at least one of the following methods: wireless or over the air messages containing special and secure update instructions; internet or client application running on a PC connected to the service card 110 via the host device or a card reader; internet application wirelessly connecting to the service card 110 via the host mobile device or user interface application of the service card 110 itself; and/or other methods.

In some implementations, provisioning of the intelligent card can be based, at least in part, on the distribution entity (*e.g.*, service provider, wireless operator, user). For example, the intelligent card may be distributed by a service provider such as a content provider (for example, DirecTV). In the service provider implementation, the intelligent card can be pre-provisioned with user accounts. In this case, the intelligent card may be activated in response to at least initial insertion into a host device. The antenna mode may be set to physical authentication only by default. In some examples, the user may self-select a user-id/password or PIN authentication to prevent

unauthorized use or through a PC cradle and plug-in management software if the host device does not have a screen and keyboard. In the wireless-operator implementation, the intelligent card may require device authentication before activation. In some examples, the user may provision service data (e.g., subscriber profile) using one of several methods. In addition, the user may add user authentication. In the user-provided implementation, the user may acquire the intelligent card from, for example, a retail store or other channels like OEM host device manufacturers. In this case, the user may activate the card in a plurality of different devices with provider selected provisioning.

In regards to activation, the intelligent card may be configured in memory mode when user acquires the card from, for example a content provider, a wireless operator, a third-party provider, and/or others. Activation of the card may include the following two levels: 1) physically, specifying antenna availability under a specific set of circumstances desired by the provider; and b) logically, at the service provider signifying activation of the broadcast application carried on the card. In some implementations, activation may be based, at least in part on device distributor, antenna availability selection, and/or type of host device as illustrated in Table 3 below.

Table 3:

Plug-in Seller and Mode of distribution	**Plug-In Initial State and Antenna Availability Choice**	**Device Has No Screen /Keyboard**	**Device Has Screen & keyboard**
Content provider ships plug-in directly to the subscriber or through participating resellers/ distributors etc.	Plug-in is in Memory Mode. It is fully personalized with user's account information and Antenna mode is set to Physical Authentication	Manual: User has to call provider's number to activate his account, the Device can only work with a single account. User can also access content provider's site on the internet using another PC to activate his account	If the device is capable of wireless access, upon insertion, the plug-in spawns a web page and takes the user to content provider's website. The user self activates his account by entering his account number and matching secret personal information (home phone number for example).

			The user can also optionally select a user-id and password (change Antenna availability to user authentication) at the same time. If Internet connection is not available, the device can automatically dial a voice call to content provider's number for account activation. If wireless connection is not available as well (device is only a PDA), the user has to fallback to manual activation (see left)
WNO: Wireless Network Operator Ships plug-in bundled with host device, User can select his preferred host device and plugin is bundled with it if user would like to avail of this service	Plug-In is in Memory Mode, it is partially personalized (device signature of the host device loaded to prevent user from changing host device) while other information is not loaded. Antenna Availability is set to Device Authentication (plug-in can only used with host device it is shipped with)	Not Applicable	Assumption: Device has a functional wireless connection. Operator offers a bundled broadcast application and subscription. When user clicks the broadcast application, the user is invited to sign-up with operator's partner content provider for a new account and subscription. Once sign-up is successful, account data is downloaded Over the Air or Over the Internet to the plugin and it is activated for use Device can use multiple content providers in this scenario and store multiple channels. User can select

			to enter a user ID and password for a content provider in the broadcast application in order to convert Antenna availability to user and device authentication for that content provider Plug-in is bound to a device signature. When removed from the device, the Antenna turns off and the plug-in turns into a simple mass memory stick. When Plug-in is inserted into another host device, the signature doesn't match and Antenna remains off.
WNO: Wireless Network Operator Ships plug-in as an accessory with an advice for compatible devices, User can select his preferred host device and attempt to operate his plug-in with, to avail of the service	Plug-In is in Memory Mode, it is unpersonalized. Antenna Availability is set to Network authentication is set to On. Plug-In will bind to first device it is inserted in and where network authentication is successful	Not Applicable	Assumption: Device has functional wireless connection. Plug-In will spawn an internet connection to the operator portal and the broadcast application will be downloaded upon user confirmation. User can reject download and choose to manually provision content provider data by going to a third party content provider or directly to the content provider website. Plug-In is bound to the device and to the wireless provider's network. If the same device is unlocked

			and used on another network, the plug-in will cease to operate and will revert back to memory mode. When removed from the device, the plug-in will revert to the memory mode.
OEM 1: Cellphone manufacturer	Device Authentication (device comes bundled with a cellphone)	Not Applicable	Option A: Device Manufacturer offers a broadcast application, rest of the process remains as above Option B: Wireless Operator offers a broadcast application. User goes to the wireless operator portal and downloads this application Over the Air. The rest of the process then remains the same as above Option C: User navigates to a third party broadcast application (example MSN-TV, Mobi-TV). Sign up is offered to participating content provider and applications are personalized on the plug-in Over the Internet Option D: User navigates to content provider's website and activates a new account which is personalized over the Internet on the plug-in
OEM 2: Other manufacturer	Device Authentication	User has to cradle the device to the PC with	If the device has wireless connection (it is a

		an internet connection and sign-up on the PC by going to an content provider's website directly. Account is downloaded over the internet via the cradle and then the device is activated. In this process, the plug-in is bound to the device signature. When removed from the host device, the antenna turns off When plugged into another device, the device signature fails and the device behaves like a mass memory device only	wireless PDA): Same as above if the device has no wireless connection (it is an unconnected PDA): Same as left

The illustrated chart is for example purposes only. The user may activate an intelligent card using the same, some, or different processes without departing from the scope of this disclosure.

FIGURE 5 is a flow chart illustrating an example method 500 for automatically bootstrapping an intelligent card in response to at least insertion into a host device. In general, an intelligent card may execute one or more authentication procedures prior to activation. Many of the steps in this flowchart may take place simultaneously and/or in different orders as shown. System 100 may use methods with additional steps, fewer steps, and/or different steps, so long as the methods remain appropriate.

Method 500 begins at step 502 where insertion into a host device is detected. For example, the service card 110 may detect insertion into the mobile device 102. If authentication is not required for any aspect of the intelligent card at decisional step 504, then execution ends. If authentication is required for at least one aspect, then execution proceeds to decisional step 506. If communication with the host device

includes one or more errors, then, at step 508, a failure is indicated to the user. In the example, the service card 110 may present an indication of a communication error to the user using the GUI 108. If a communication error is not detected at decisional step 506, then execution proceeds to decisional step 510. In some implementations, the intelligent card uploads an SD driver to the host device. If the intelligent card only requires physical authentication, then execution proceeds to decisional step 512. If the network authentication flag is not set to on, then, at step 514, the antenna is turned on and the intelligent card is updated with host-device signature. As for the example, the service card 110 may activate the antenna for wireless transactions and update local memory with the host-device signature. If the network authentication flag is turned on at decisional step 512, then, at step 516, the intelligent card transmits a request for the network ID to the host device. Next, at step 518, the intelligent card retrieves a locally-stored network ID. If the stored network ID and the request network ID match at decisional step 520, then the card is activated at step 514. If the two network ID's do not match, then the antenna is deactivated at step 522.

Returning to decisional step 510, if the authentication is not only physical authentication, then execution proceeds to decisional step 524. If the authentication process includes device authentication, then, at step 526, the intelligent card transmits a request for a network ID to the host device. At step 528, the intelligent card retrieves a locally stored device signatures. If the intelligent card does not include at least one device signature, then execution proceeds to decisional step 534. If the intelligent card includes one or more device signatures, then execution proceeds to decisional step 532. If one of the device signatures matches the request network ID, then execution proceeds to decisional step 534. If the signatures and the request network ID do not match, then execution proceeds to step 522 for deactivation. If user authentication is not included in the authentication process, then execution proceeds to decisional step 512 for physical authentication. If user authentication is included at decisional step 534, then execution proceeds to step 538.

Returning to decisional step 524, if the authentication process does not include device authentication, then execution proceeds to decisional step 536. If user authentication is not included in the process, then, at step 522, the intelligent card is turned off. If user authentication is included, then, at step 538, the intelligent card request a userid and password from the user using the host device. While the user

authentication is described with respect to entering a user id and password through the mobile host device, the user may be authenticated using other information such as a simple PIN and/or biometric information (e.g., fingerprint). Again returning to the example, the service card 110 may present a request for the user to enter a user-id and password through the GUI 108. At step 540, the intelligent card sends the entered information to the service provider using the cellular network or the broadcast network. If at the account information is validated by the service provider at decisional step 542, then execution proceeds to decisional step 512 for physical authentication. If the account information is not validated at decisional step 542, then execution proceeds to decisional step 544. If the number of attempts have not exceeded a specified threshold, then execution returns to step 538. If the number of attempts has exceed to the threshold, then the antenna is deactivated at step 522. In the example, if the event that the service card 110 fails to authorize the device, network and/or user, the service card 110 may wirelessly transmit an indication to the associated service provider using the cellular radio technology of the mobile host device 102. In this case, the illustrated method 500 may be implemented as a fraud control process to substantially prevent unauthorized use of the service card 110.

FIGURE 6 is a flow chart illustrating an example method 600 for activating a wireless transaction system including an intelligent card. In general, an intelligent card may execute one or more activation processes in response to, for example, a selection from a user. Many of the steps in this flowchart may take place simultaneously and/or in different orders as shown. System 100 may use methods with additional steps, fewer steps, and/or different steps, so long as the methods remain appropriate.

Method 600 begins at step 602 where a request to activate a service card is received. For example, the user may select a graphical element displayed through the GUI 108 of a mobile host device 102 in FIGURE 1. If an account activation is included at decisional step 604, then at step 606, a request to activate the associated user account is wirelessly transmitted to service provider using cellular radio technology of the host device. For example, the service card 110 may wireless transmit an activation request to the service provider 104 using the cellular radio technology of the mobile host device 102. If an account activation is not included, then execution proceeds to decisional step 608. If card activation is not included, then

execution ends. If card activation is included, then execution proceeds to decisional step 610. If an activation code is not included, then at step 612, one or more preprogrammed questions are presented to the user using the GUI of the host device. Returning to the initial example, the service card 110 may identify locally stored questions and present the questions to the user using the GUI 108 of the mobile host device 102. At step 614, locally-stored answers to the programmed questions are identified. Returning to decisional step 610, if an activation code is included, then execution proceeds to decisional step 616. If the activation code is manually entered by the user, then at step 618, a request for the activation code is presented to the user through the GUI of the mobile host device. In the initial example, the service card 110 may present a request for an activation code such as a string of characters to the user through the GUI 108 of the mobile host device 102. If the activation code is not manually entered by the user, then at step 620, the service card wirelessly transmits a request for the activation code using the cellular radio technology of the host device. In the cellular example, the service card 110 may transmit a request to the service provider using the cellular core network 108. In either case, the locally-stored activation code is identified at step 622. If the locally stored information matches the provided information at decisional step 624, then at step 626, the service card is activated. For example, the service card 110 may activate in response to at least a user entering a matching activation code through the GUI 108. If the provided information does not match the locally stored information, then execution ends.

FIGURES 7A-C is an example call flow 700 in accordance with some implementations of the present disclosure. As illustrated, the flow 700 includes a network 702, a host device 704, an intelligent card 706, and a cellular network 708. The host device 704 is configured to communicate with the network 702 and includes a slot for insertion of the intelligent card 706. The intelligent card 706 is configured to transmit commands to and receive data from a user interface application 710 executed by the host device 710 and execute access foreign services independent of the host device 710. The card 706 includes a CPU 712 for accessing services and a wireless chipset 714 for communicating with the cellular network 708. The CPU 712 executes a host controller/API interface 716 configured to transmits commands in a form compatible with the host device 704 and convert data from the host device 704 to a form compatible with the CPU 712.

As illustrated, the flow 700 may include multiple sessions 720 between the host device 704 and the card 706 and between the card 706 and the cellular network 708. The session 720a illustrates a session managed by the card 706 using the network capabilities of the host device 710. In this example, the card 706 transmits data for transmission through a network connected to the host device 704, and after receiving the data, the host device 704 transmits the data to the network 802. In response to receiving data from the network 702, the host device 704 may automatically transmit the received data to the card 706. In some implementations, the card 706 may transmit a request for a device signature to the host device 704 as illustrated in session 720b. For example, the card 706 may request the device signature during a bootstrapping process. The session 720c illustrates that a user may submit commands to the card 706 through the interface of the host device 704. For example, the user may request that the card display the user's transaction history through the interface of the host device 704.

In some implementations, the card 706 may receive a command to activate or deactivate the antenna through the host device 704 as illustrated in session 720d. For example, a service provider may identify irregular transactions and transmit a command through the network 702 to deactivate the card 706. The card 706 may authorize a user by requesting a user-id and password using the host device 704. As illustrated in session 720e, the user may submit a user-id and password to the card 706 using the interface of the host device 704, and in response to an evaluation of the submitted user-id and password, the card 706 may present through the host device 704 an indication that the user verification is successful or has failed. In some implementations, a user and/or service provider may request a transaction history of the card 706 as illustrated in session 720f. For example, a service provider may transmit a request for the transaction history through the network 702 connected to the host device 704, and in response to at last in the request, the card 706 may transmit the transaction history to the service provider using the network 702 connected to the host device 704. In some implementations, the user may present offline Web pages stored in the card 706 as illustrated in session 720. For example, the card 706 may receive a request to present an offline Web page from the user using the host device 704 and present the offline page using the URL in the request. In some implementations, content data stored in the memory of the card 706 or available via live reception of

streaming content may be presented through, for example, the host device 704 as illustrated in session 720h. For example, the user may request specific information associated with the Electronic Service Guide and the card 706 may retrieve the data and present the data to the user using the host device 704. In addition, the user may write data to the memory in the card 706 as illustrated in session 720i. For example, the user may setup timers for the Personal Video Recorder application on the card 706 and the card 706 may indicate the success and failure of the timer setup

In regards to session between the card 706 and the terminal, the flow 700 illustrates the personalization session 720k and the transaction session 720l. In regards to personalization, a service provider may personalize a card 706 with user credentials, user applications, Web pages, and/or other information as illustrated in session 720k. For example, the cellular network 708 may transmit a provisioning request to the card 706 including associated data. The protocol translation 718 may translate the personalization request to a form compatible with the card 706. In response to at least the request, the CPU 712 transmit an indication whether the personalization was a success or not using the protocol translation 718. Prior to the a broadcast session beginning live reception, the broadcast network 708 may submit a subscription verificationchallenge to the card 706 as illustrated in session 720l. In this case, the card 706 may identify a receiver signature of the receiver 718, present associated data to the user through the host device 704, and transmit the signature to the cellular network 708 using the protocol translation 718.

FIGURE 8 is a flow chart illustrating an example method 800 for managing the Electronic Service Guide application. In general, an intelligent card may receive ESG data from the broadcast network and display it to the user in response to at least an event. Many of the steps in this flowchart may take place simultaneously and/or in different orders as shown.

Method 800 begins at step 802 where ESG data currently stored is identified. For example, the service card 112 may receive ESG data from the broadcast network or the cellular network such as channel lineup, program listing, program information and program ratings. At step 804, previously downloaded ESG content is identified. In the example, the service card 112 may identify content previously downloaded from the content provider to the local memory in the card 112. In some implementations, the service card 112 may identify one or more aspects of memory such as file names,

file sizes, dates, and/or other aspects. If the previously-downloaded content matches the current content at decisional step 806, then execution ends. If the previously-dowloaded content does not match the current content, then, at step 808, at least a portion of the locally-stored content is automatically updated in the local memory. As for the example, the service card 112 may only download content identified as new content or content that was previously not downloaded. In downloading the content, the service card 112 may substantially updates local-stored ESG content according to the latest available ESG from the service provider

FIGURE 9 is a flow chart illustrating an example method 900 for managing the Personal Video Recorder application. In general, an intelligent card may automatically receive data from the broadcast network and record it to the memory (if space is available) in response to at least an event (timer). Many of the steps in this flowchart may take place simultaneously and/or in different orders as shown.

Method 900 begins at step 902 where a timer event triggers the beginning of broadcast reception. For example, the service card 112 may automatically tune the antenna to the channel corresponding to the program that the user has setup to record as associated with the timer. At step 804, available memory space is identified. In the example, the service card 112 may identify free local memory in the card 112. If the available memory is below a certain threshold (configured by the service provider) at decisional step 806, then execution ends. If available memory is above a certain threshold, then, at step 808, broadcast reception is started and content is automatically recorded in the local memory in a newly created program data file. After a specified size of program data is recorded, available memory is checked again and the process is repeated by appending to the program data file until either the program ends or the available memory falls below the threshold. Once the program ends, the program data file is finalized and given a unique identifier so that it can be accessed for viewing.

A number of embodiments of the invention have been described. Nevertheless, it will be understood that various modifications may be made without departing from the spirit and scope of the invention. Accordingly, other embodiments are within the scope of the following claims.

WHAT IS CLAIMED IS:

1. A service card, comprising:

a physical interface that connects to a port of a mobile host device, wherein the mobile host device includes a Graphical User Interface (GUI);

a communication module that wirelessly receives broadcast signals encoding content;

set-top box module that stores user information used to access content independent of the mobile host device,

memory that can store downloaded encoded content in a format viewable by a media player, the stored content associated with a content provider; and

a service module that decrypts the encoded content in response to at least an event and presents the content through the GUI of the mobile host device.

2. The service card of claim 1, wherein the service card comprises a SD card.

3. The service card of claim 1, the broadcast signals comprise at least one of satellite broadcast signals, terrestrial broadcast signals, or IP broadcast signals.

4. The service card of claim 1, wherein the content comprises at least one of video, images, or audio.

5. The service card of claim 1, wherein the service module comprises an operating system with a runtime environment that executes a locally-stored broadcast application for receiving the content independent of the mobile host device.

6. The service card of claim 1, wherein a user-interface module that presents Electronic Service Guide information associated with receiving the content through the GUI of the mobile host device.

7. The service card of claim 6, wherein the user-interface module further presents a request for user identification including at least one of a Personal Identification Number (PIN), user ID and password, or biometric signature through the GUI of the mobile host device, the service module further verifies the submitted user identification prior to accessing foreign services.

8. The service card of claim 7, the service module further deactivates the service module in response to at least a number of user-id and password or PIN entry events exceeding a threshold.

9. The service card of claim 1, wherein the service module selectively switches a broadcast receiver between an active state and an inactivate state in response to at least an event.

10. The service card of claim 9, wherein the switching event includes a selection through a GUI of the mobile host device.

11. The service card of claim 1, wherein the service module further comprises a protocol translation module that translates signals from broadcast content to content viewable by the mobile host device.

12. The service card of claim 1, further comprising an authentication module that authenticates at least one of a network of the mobile host device, the mobile host device, or a user.

13. The service card of claim 12, the authentication module further deactivates the antenna in response to at least a failure to authenticate the at least one of the network of the mobile host device, the mobile host device, or the user.

14. The service card of claim 1, wherein the service card is initialized in response to at least insertion in the port of the mobile host device.

15. The service card of claim 1, further comprising an activation module that activates the service card in response to at least a user request or an initial insertion into the mobile host device.

16. The service card of claim 15, wherein the service card is activated based, at least in part, on a user manually entering an activation code through the GUI of the mobile host device.

17. The service card of claim 1, wherein the service card presents the content through the GUI independent of loading a driver onto the mobile host device.

18. The service card of claim 1, wherein the service card emulates a set-top box when receiving broadcast signals.

19. The service card of claim 1, further comprising a power module that receives power from the mobile host device.

20. The service card of claim 1, wherein an enterprise at least associated with the content provider uploads personalization data prior to activation, wherein the personalization data includes the user information and a broadcast application.

21. The service card of claim 20, the service module further operable to update the personalization data after activation in response to at least one of a wireless signal including secure update instructions or a wired signal through a client connected to the service card.

22. The service card of claim 1, the service module further operable to transmit to deactivate the service card in response to at least an activity violating one or more fraud control rules.

23. The service card of claim 1, wherein the set-top box module further updates Electronic Service Guide (ESG) data and presents stored ESG data in response to a request.

24. The service card of claim 1, further comprising a Personal Video Recorder (PVR) that automatically receives broadcasted content in response to at least an event and records the received content in accordance with available memory.

25. The service card of claim1, further comprising a Channel Associated Signaling (CAS) module that identifies content privileges of the user and decodes scramble content based, at least in part, on the identified privileges.

26. A method, comprising:

interfacing a port of a mobile host device, wherein the mobile host device includes a Graphical User Interface (GUI);

wirelessly receiving broadcast signals encoding content;

storing user information used to decrypt the encoded content independent of the mobile host device, the stored information associated with a content provider;

decrypting the encoded content in response to at least an event; and

presenting the content through the GUI of the mobile host device.

27. The method of claim 26, wherein the service card comprises a microSD card.

28. The method of claim 26, the broadcast signals comprise at least one of satellite broadcast signals or terrestrial broadcast signals.

29. The method of claim 26, wherein the content comprises at least one of video, images, or audio.

30. The method of claim 26, further comprising executing a locally-stored broadcast application for receiving the content independent of the mobile host device.

31. A system, comprising:

a means for interfacing a port of a mobile host device, wherein the mobile host device includes a Graphical User Interface (GUI);

a means for wirelessly receiving broadcast signals encoding content;

a means for storing user information used to decrypt the encoded content independent of the mobile host device, the stored information associated with a content provider;

a means for decrypting the encoded content in response to at least an event; and

a means for presenting the content through the GUI of the mobile host device.

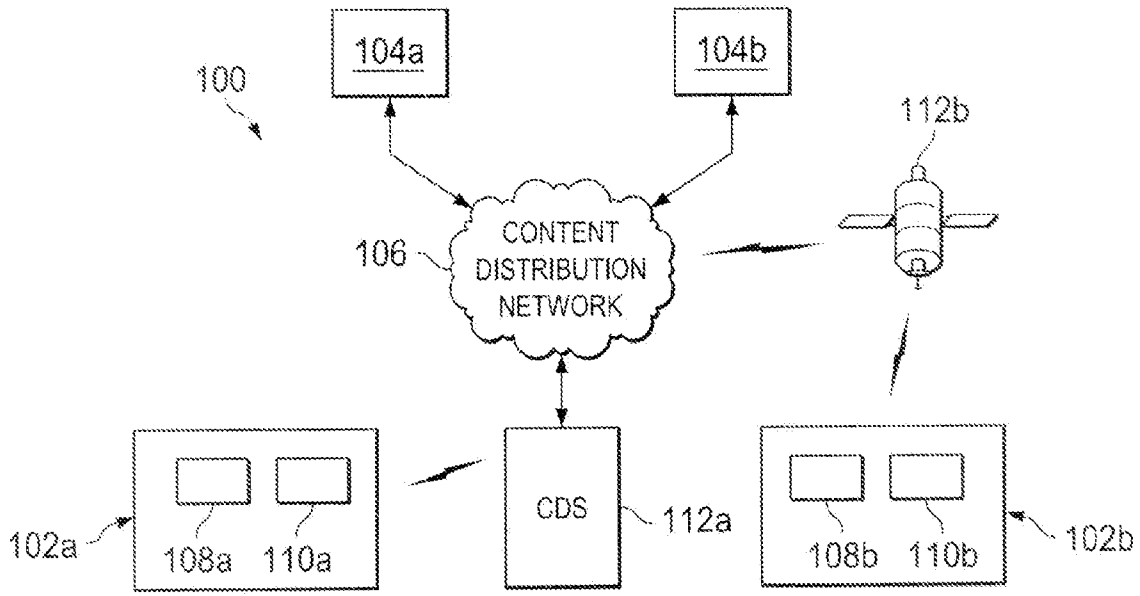

100
104a
104b
112b
106
CONTENT DISTRIBUTION NETWORK
CDS
112a
102a
108a
110a
108b
110b
102b

FIG. 1

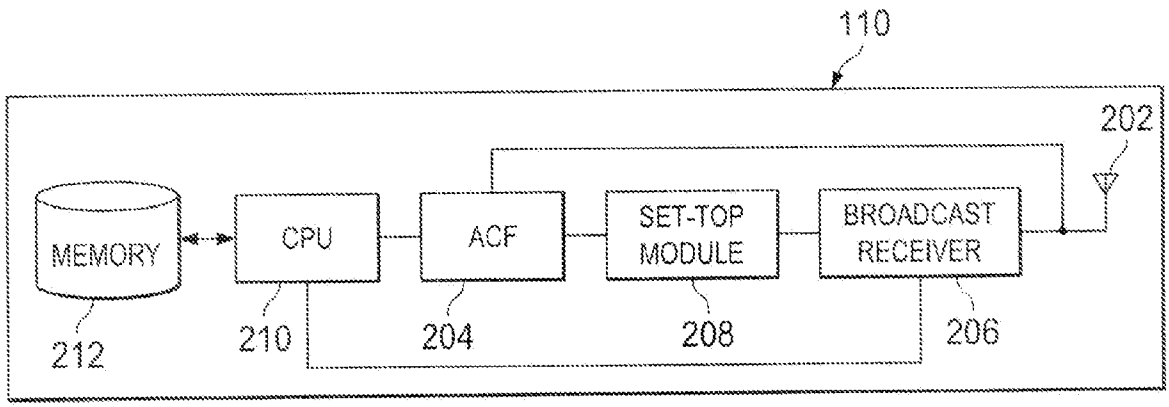

110
202
MEMORY
CPU
ACF
SET-TOP MODULE
BROADCAST RECEIVER
212
210
204
208
206

FIG. 2

FIG. 3

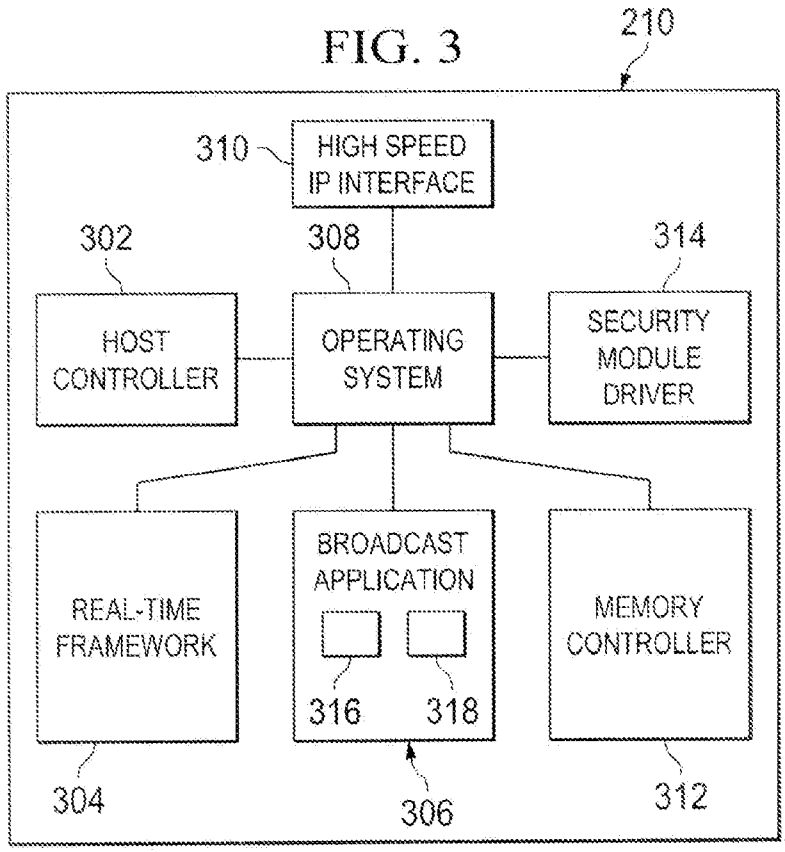

210
310
HIGH SPEED IP INTERFACE
302
308
314
HOST CONTROLLER
OPERATING SYSTEM
SECURITY MODULE DRIVER
REAL-TIME FRAMEWORK
BROADCAST APPLICATION
316
318
MEMORY CONTROLLER
304
306
312

FIG. 4

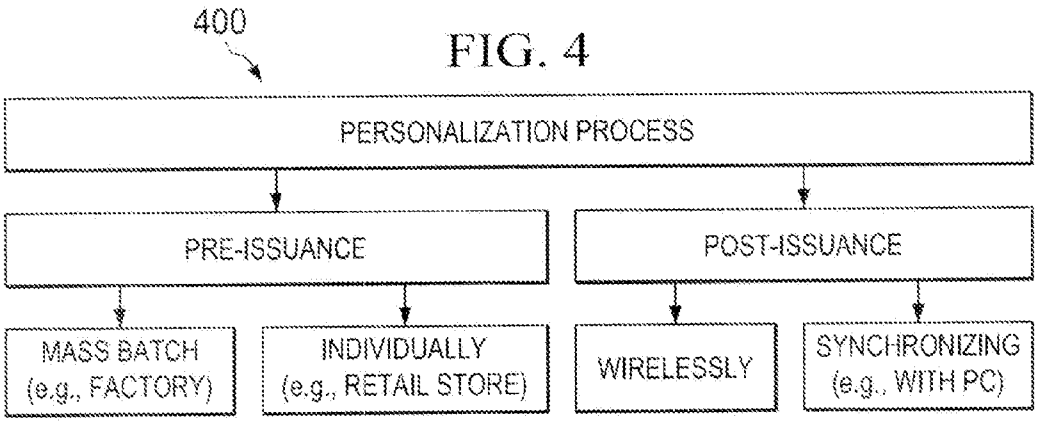

400
PERSONALIZATION PROCESS
PRE-ISSUANCE
POST-ISSUANCE
MASS BATCH (e.g., FACTORY)
INDIVIDUALLY (e.g., RETAIL STORE)
WIRELESSLY
SYNCHRONIZING (e.g., WITH PC)

FIG. 5A

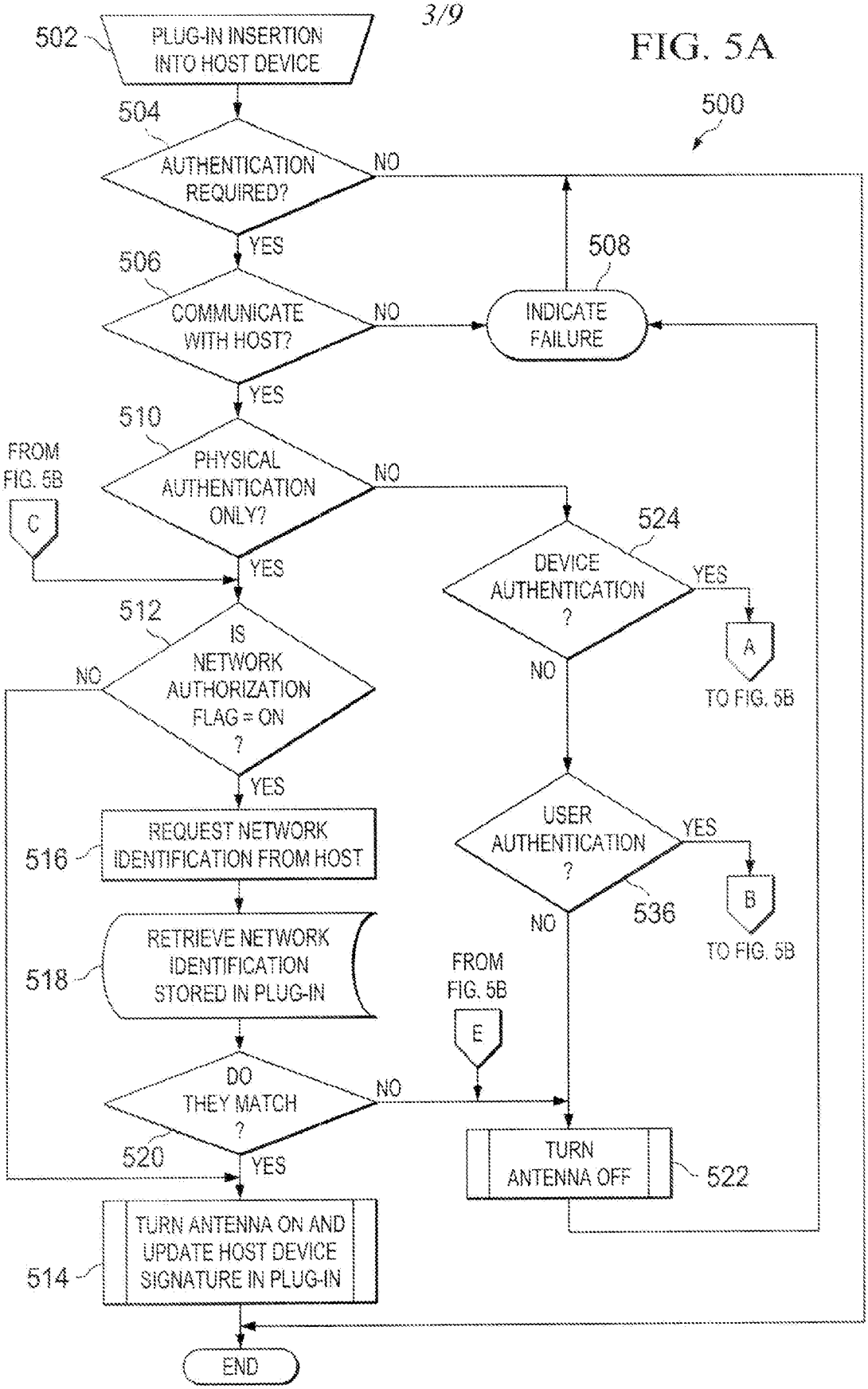
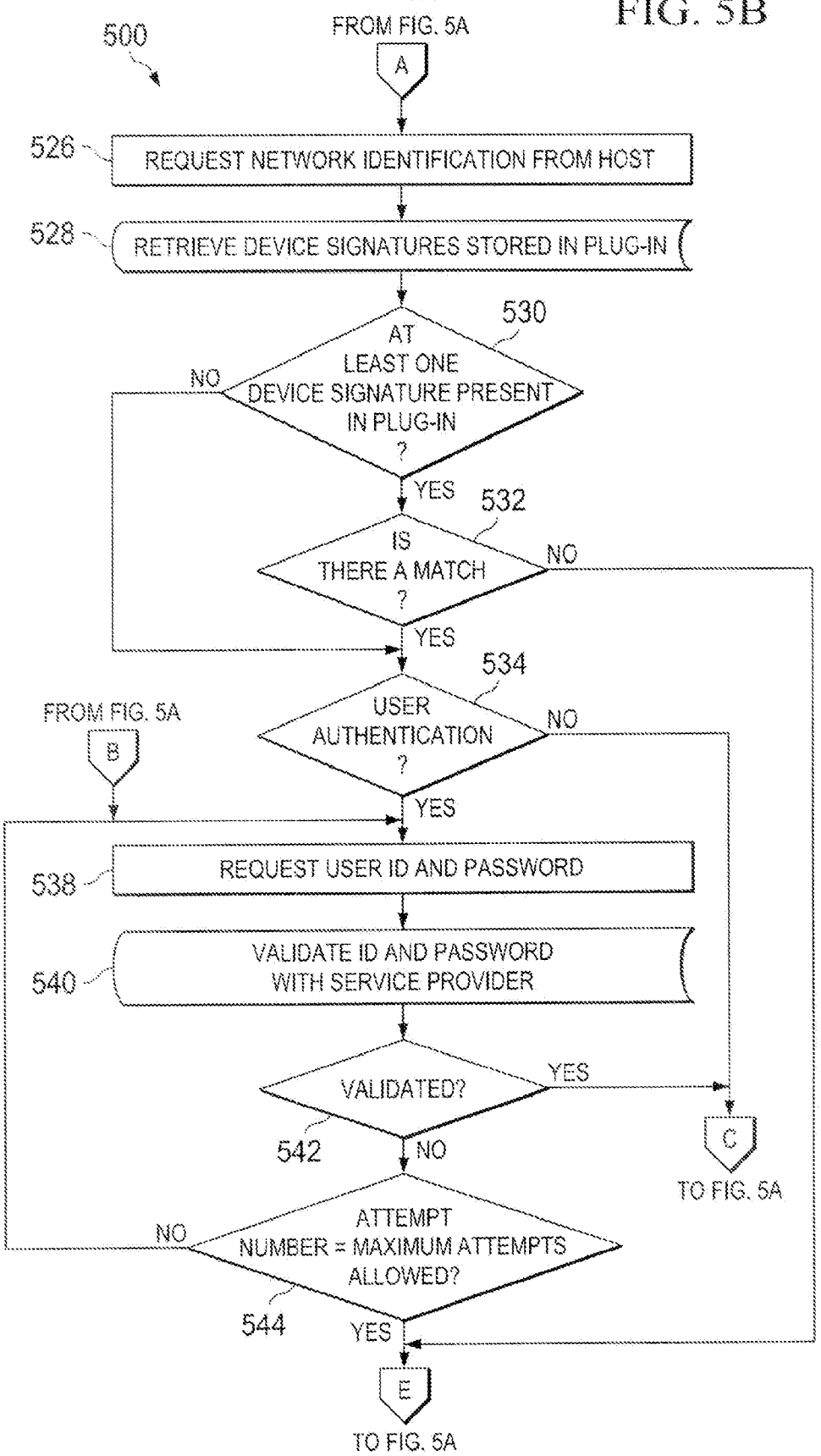

500
502
PLUG-IN INSERTION INTO HOST DEVICE
504
AUTHENTICATION REQUIRED?
NO
YES
506
COMMUNICATE WITH HOST?
NO
YES
508
INDICATE FAILURE
510
PHYSICAL AUTHENTICATION ONLY?
NO
YES
FROM FIG. 5B
C
512
IS NETWORK AUTHORIZATION FLAG = ON ?
NO
YES
516
REQUEST NETWORK IDENTIFICATION FROM HOST
518
RETRIEVE NETWORK IDENTIFICATION STORED IN PLUG-IN
520
DO THEY MATCH ?
NO
YES
514
TURN ANTENNA ON AND UPDATE HOST DEVICE SIGNATURE IN PLUG-IN
END
524
DEVICE AUTHENTICATION ?
YES
NO
A
TO FIG. 5B
USER AUTHENTICATION ?
YES
NO
536
B
TO FIG. 5B
FROM FIG. 5B
E
TURN ANTENNA OFF
522

FIG. 5B


500
FROM FIG. 5A
A
526
REQUEST NETWORK IDENTIFICATION FROM HOST
528
RETRIEVE DEVICE SIGNATURES STORED IN PLUG-IN
530
AT LEAST ONE DEVICE SIGNATURE PRESENT IN PLUG-IN ?
NO
YES
532
IS THERE A MATCH ?
NO
YES
534
USER AUTHENTICATION ?
NO
YES
FROM FIG. 5A
B
538
REQUEST USER ID AND PASSWORD
540
VALIDATE ID AND PASSWORD WITH SERVICE PROVIDER
VALIDATED?
YES
542
NO
C
TO FIG. 5A
ATTEMPT NUMBER = MAXIMUM ATTEMPTS ALLOWED?
NO
544
YES
E
TO FIG. 5A

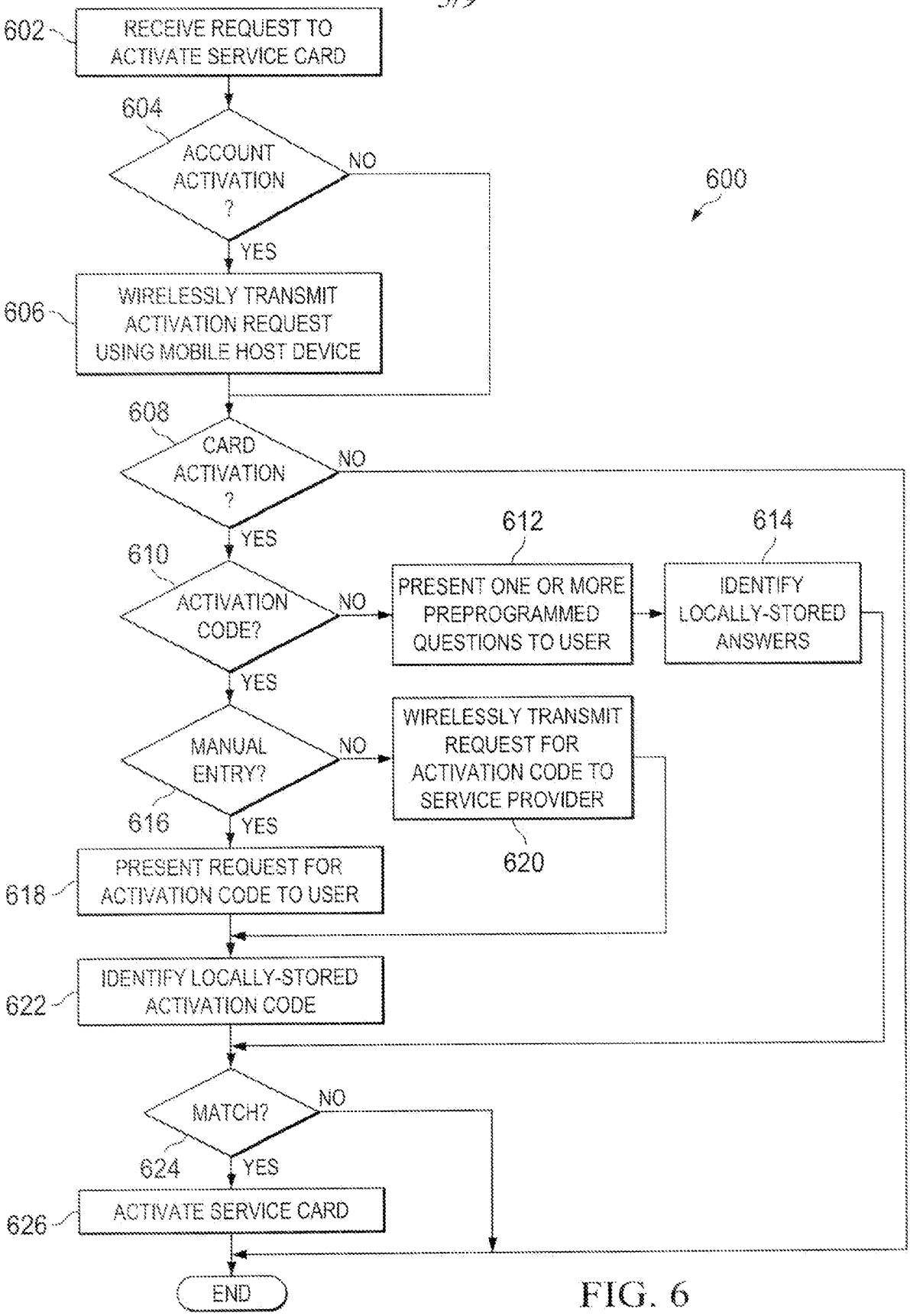

602
RECEIVE REQUEST TO ACTIVATE SERVICE CARD
604
ACCOUNT ACTIVATION ?
NO
YES
600
606
WIRELESSLY TRANSMIT ACTIVATION REQUEST USING MOBILE HOST DEVICE
608
CARD ACTIVATION ?
NO
YES
610
ACTIVATION CODE?
NO
612
PRESENT ONE OR MORE PREPROGRAMMED QUESTIONS TO USER
614
IDENTIFY LOCALLY-STORED ANSWERS
YES
MANUAL ENTRY?
NO
WIRELESSLY TRANSMIT REQUEST FOR ACTIVATION CODE TO SERVICE PROVIDER
620
616
YES
618
PRESENT REQUEST FOR ACTIVATION CODE TO USER
622
IDENTIFY LOCALLY-STORED ACTIVATION CODE
MATCH?
NO
624
YES
626
ACTIVATE SERVICE CARD
END

FIG. 6

FIG. 7A

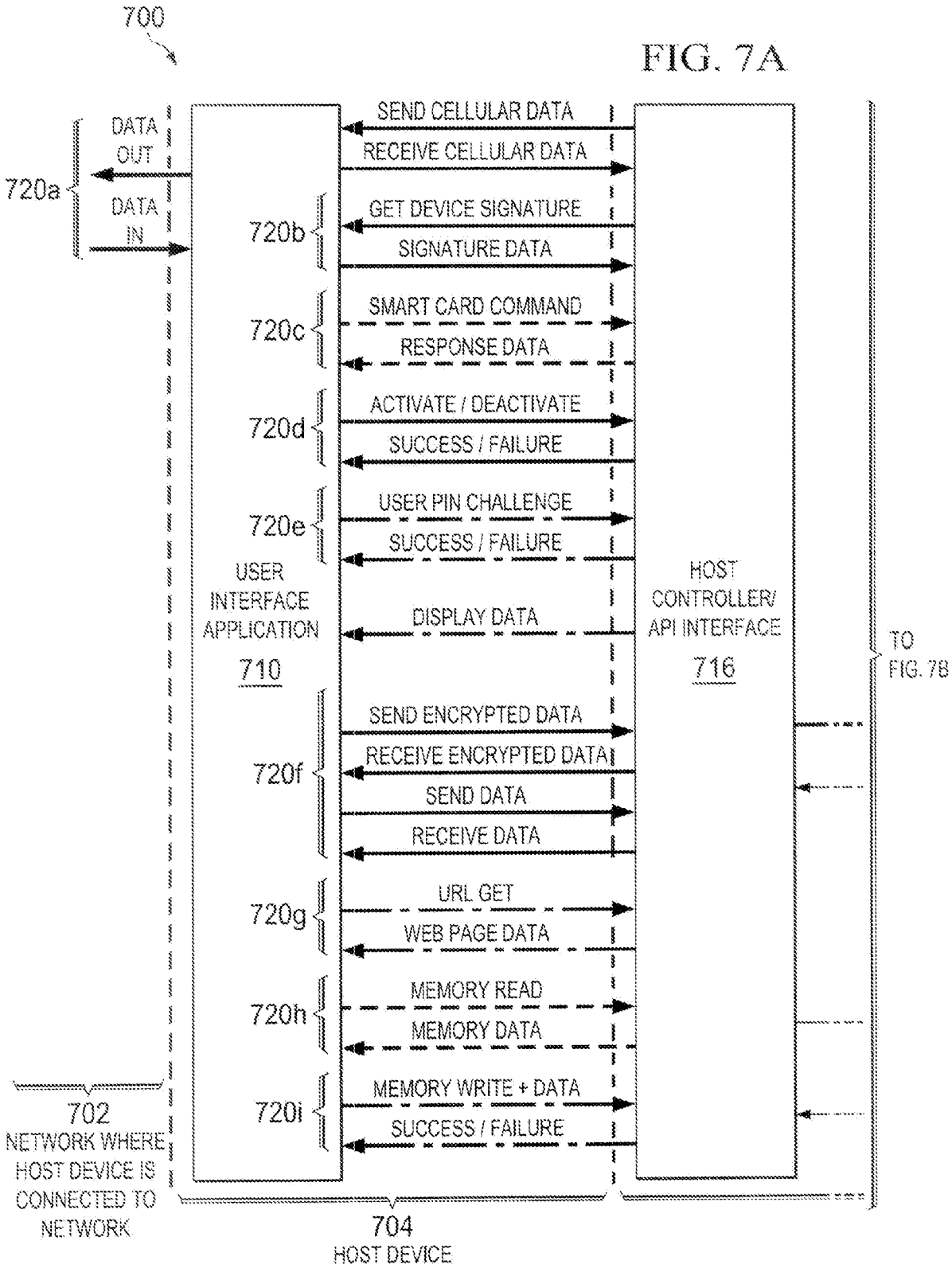

700
DATA OUT
DATA IN
720a
720b
720c
720d
720e
720f
720g
720h
720i
SEND CELLULAR DATA
RECEIVE CELLULAR DATA
GET DEVICE SIGNATURE
SIGNATURE DATA
SMART CARD COMMAND
RESPONSE DATA
ACTIVATE / DEACTIVATE
SUCCESS / FAILURE
USER PIN CHALLENGE
SUCCESS / FAILURE
DISPLAY DATA
SEND ENCRYPTED DATA
RECEIVE ENCRYPTED DATA
SEND DATA
RECEIVE DATA
URL GET
WEB PAGE DATA
MEMORY READ
MEMORY DATA
MEMORY WRITE + DATA
SUCCESS / FAILURE
USER INTERFACE APPLICATION
710
HOST CONTROLLER/ API INTERFACE
716
TO FIG. 7B
702
NETWORK WHERE HOST DEVICE IS CONNECTED TO NETWORK
704
HOST DEVICE

FIG. 7B

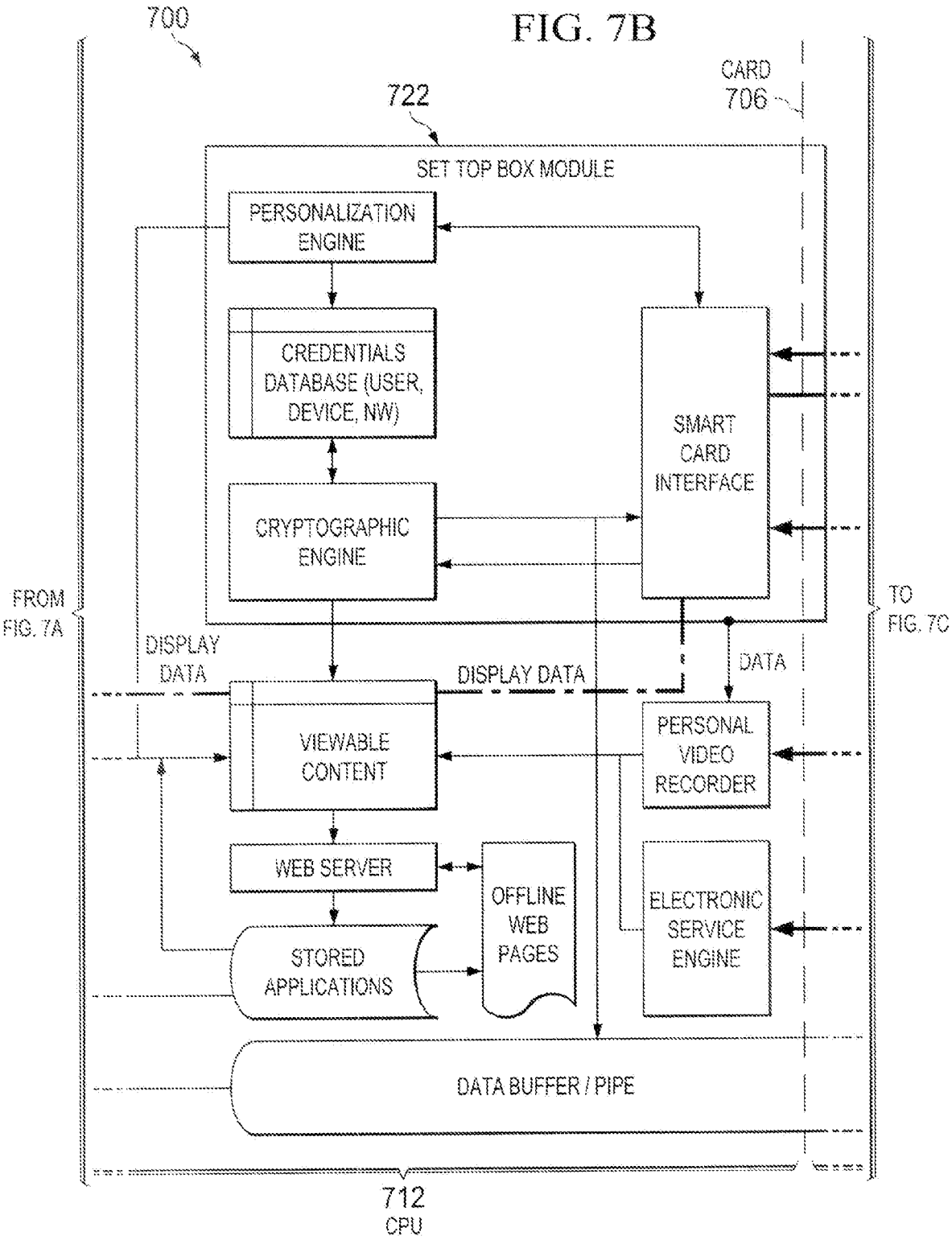
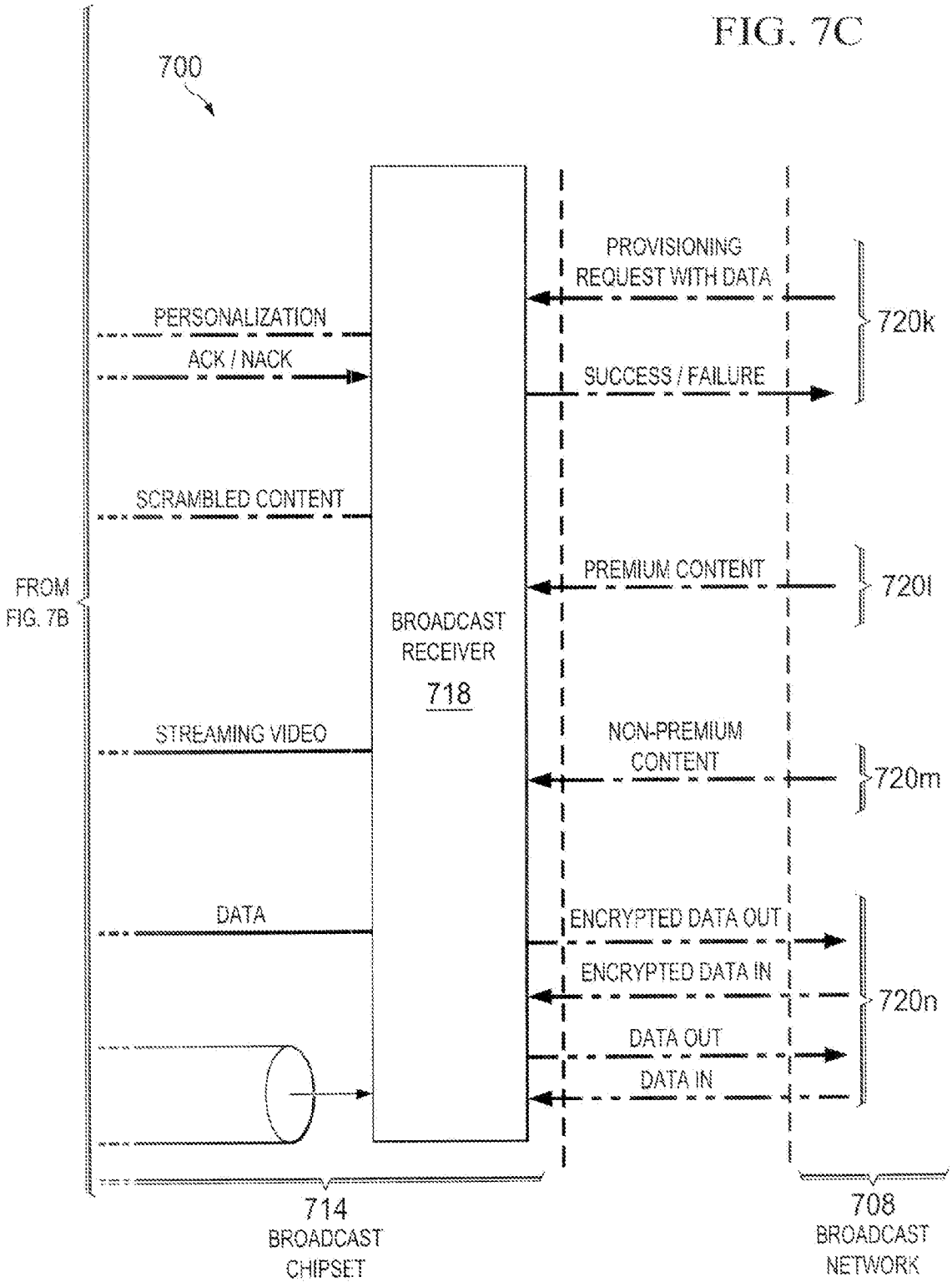

700
722
CARD
706
SET TOP BOX MODULE
PERSONALIZATION ENGINE
CREDENTIALS DATABASE (USER, DEVICE, NW)
CRYPTOGRAPHIC ENGINE
SMART CARD INTERFACE
FROM FIG. 7A
TO FIG. 7C
DISPLAY DATA
DISPLAY DATA
DATA
VIEWABLE CONTENT
PERSONAL VIDEO RECORDER
WEB SERVER
OFFLINE WEB PAGES
ELECTRONIC SERVICE ENGINE
STORED APPLICATIONS
DATA BUFFER / PIPE
712
CPU

FIG. 7C


700
FROM FIG. 7B
PERSONALIZATION
ACK / NACK
SCRAMBLED CONTENT
STREAMING VIDEO
DATA
BROADCAST RECEIVER
718
PROVISIONING REQUEST WITH DATA
SUCCESS / FAILURE
720k
PREMIUM CONTENT
720l
NON-PREMIUM CONTENT
720m
ENCRYPTED DATA OUT
ENCRYPTED DATA IN
DATA OUT
DATA IN
720n
714
BROADCAST CHIPSET
708
BROADCAST NETWORK

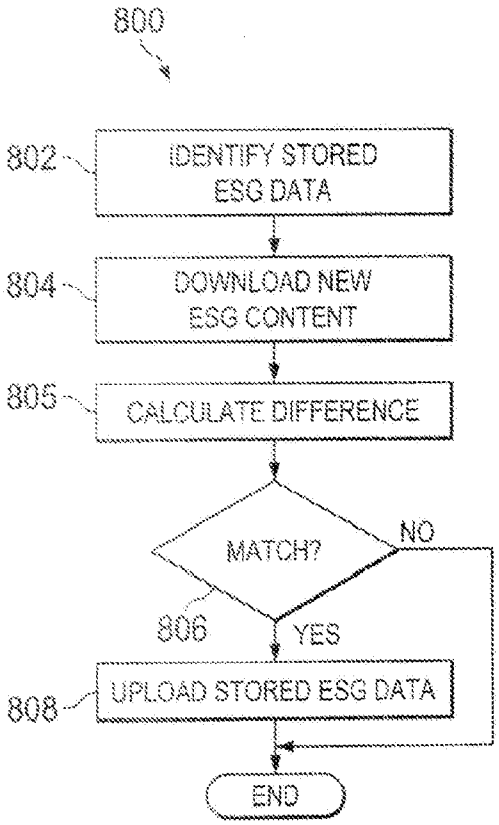

800
802
IDENTIFY STORED ESG DATA
804
DOWNLOAD NEW ESG CONTENT
805
CALCULATE DIFFERENCE
MATCH?
NO
806
YES
808
UPLOAD STORED ESG DATA
END

FIG. 8

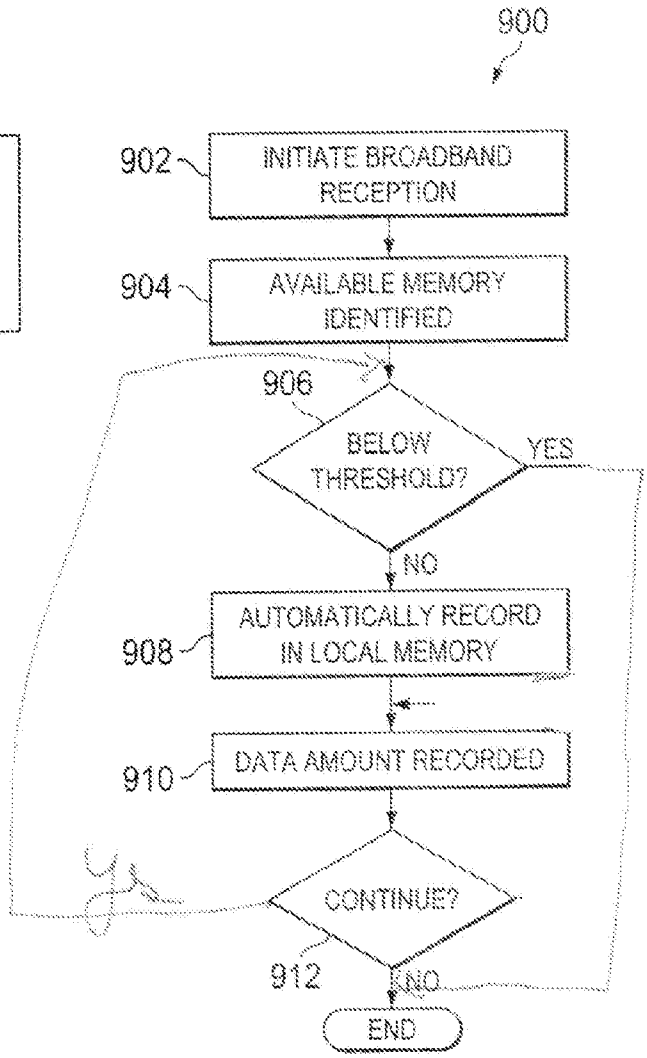

900
902
INITIATE BROADBAND RECEPTION
904
AVAILABLE MEMORY IDENTIFIED
906
BELOW THRESHOLD?
YES
NO
908
AUTOMATICALLY RECORD IN LOCAL MEMORY
910
DATA AMOUNT RECORDED
CONTINUE?
912
NO
END

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2008/076318

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04N7/16 H04N5/00

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04N

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/204845 A1 (SIBLEY ERIN H [US] ET AL) 30 October 2003 (2003-10-30) abstract paragraphs [0016], [0023], [0046], [0058], [0091] - [0097] claim 1	1-31
X	US 2007/113260 A1 (PUA KHEIN-SENG [TW] ET AL) 17 May 2007 (2007-05-17) paragraphs [0006], [0008], [0009], [0020] - [0023], [0035], [0039] - [0042] figures 1,2	1-31
X	DE 20 2006 001690 U1 (TERRATEC ELECTRONIC GMBH [DE]) 27 April 2006 (2006-04-27) abstract paragraphs [0005], [0006], [0010], [0015], [0025], [0026]	1-31

-/--

[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 document but published on or after the international filing date

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 January 2009	02/02/2009

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Naci, Suphi Umut

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2008/076318

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 773 059 A (AXALTO SA [FR]) 11 April 2007 (2007-04-11) paragraphs [0023] - [0025] claims 1-8	1-31
X,P	WO 2007/125223 A (OBERTHUR CARD SYST SA [FR]; BERTIN MARC [FR] OBERTHUR TECHNOLOGIES [FR) 8 November 2007 (2007-11-08) page 1, lines 5-18 page 2, lines 4-12,18-29 page 7, lines 12-20 page 9, lines 2-20 page 10, lines 15-21 figure 2	1-31

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2008/076318

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003204845 A1	30-10-2003	AU 2003225143 A1	17-11-2003
		WO 03094511 A1	13-11-2003
		US 2006048208 A1	02-03-2006
US 2007113260 A1	17-05-2007	NONE	
DE 202006001690 U1	27-04-2006	NONE	
EP 1773059 A	11-04-2007	NONE	
WO 2007125223 A	08-11-2007	FR 2900750 A1	09-11-2007
		US 2008263680 A1	23-10-2008