



(51) International Patent Classification:

H04W 12/06 (2009.01) H04W 4/06 (2009.01)  
H04W 12/08 (2009.01) H04W 4/12 (2009.01)

(21) International Application Number:

PCT/US2014/049650

(22) International Filing Date:

4 August 2014 (04.08.2014)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

61/861,678 2 August 2013 (02.08.2013) US  
61/947,955 4 March 2014 (04.03.2014) US

(71) Applicant: SIRIUS XM RADIO INC. [US/US]; 1221 Avenue of The Americas, New York, NY 10020 (US).

(72) Inventors: MICHALSKI, Richard, Andrew; 5171 Chardonway Drive, Coral Springs, FL 33067 (US). RINDSBERG, Mark; 22232 Alyssum Way, Boca Raton, FL 33433 (US). VADEKAR, Ashok; 250 Harris Street, Rockwood, Ontario N0B 2K0 (CA). MARKO, Paul; 6320 Sw 6 Street, Pembroke Pines, FL 33023 (US). WADIN, Craig; 11015 Nw 27th Street, Sunrise, FL 33322 (US).

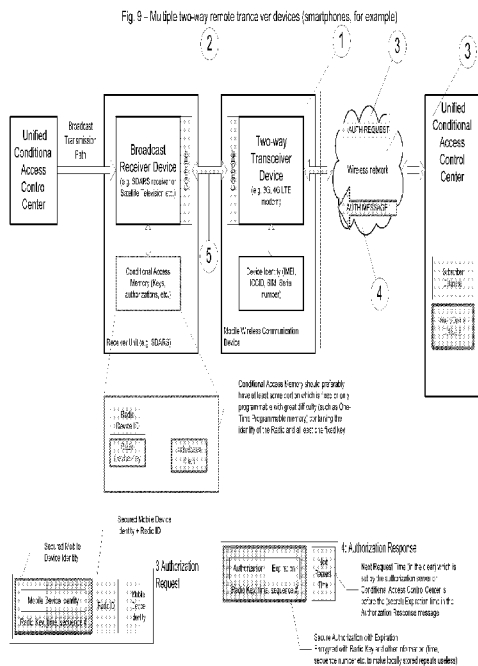
(74) Agents: HALEVA, Aaron et al.; Kramer Levin Naftalis & Frankel LLP, 1177 Avenue of The Americas, New York, NY 10036 (US).

(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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

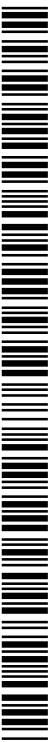
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE,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

[Continued on next page]

(54) Title: SYSTEMS AND METHODS FOR TRANSMITTING CONDITIONAL ACCESS INFORMATION



(57) Abstract: Various multiple methods of data transport, and combinations thereof, may be used to initialize or update conditional access information on various devices. In an integrated device having both a broadcast receiver, such as an SDARS receiver, and a two-way communications transceiver, such as an LTE, 3G or 4G modem, conditional access information for the broadcast receiver may be sent to the transceiver, and then passed to the broadcast receiver, or vice versa. Additionally, for example, the broadcast receiver may be sent, over the broadcast communications channel, a "wake-up" message for the two-way transceiver, which may then be passed to the two-way transceiver, so as to make it ready to receive conditional access information over the two-way communications channel, or vice versa. Moreover, because of the presence of a two-way communications path, various acknowledgements of conditional access status updates received and processed by the broadcast receiver may be sent - thus realizing a significant improvement over the current practice of sending multiple periodic messages over the broadcast channel, to insure (but never have a confirmed) receipt.



**Published:**

— *with international search report (Art. 21(3))*

**PCT PATENT APPLICATION UNDER THE PATENT CO-OPERATION  
TREATY**

**SYSTEMS AND METHODS FOR TRANSMITTING CONDITIONAL  
ACCESS INFORMATION**

**CROSS-REFERENCE TO RELATED APPLICATIONS**

The present application claims priority to United States Provisional Patent Applications No. 61/861,678, filed on August 2, 2013, entitled "HYBRID TRANSPORT CONDITIONAL ACCESS METHODS AND SYSTEMS", and 61/947,955, entitled "SATELLITE PROVISIONING OF CELL SERVICE", filed on March 4, 2014, the entire disclosure of each of which is hereby incorporated herein by this reference.

**TECHNICAL FIELD**

The present invention is generally directed to subscriber based broadcast and communication systems, and in particular to various systems and methods for transmitting conditional access information to various subscribers or authorized users, and their various devices or combinations of devices.

**BACKGROUND OF THE INVENTION**

Conventionally, there are a few methods of effecting Conditional Access for a system with devices to be activated and/or authorized in the field. Broadcast systems (e.g., SDARS) transmit Conditional Access information in a 1-way manner and use multiple repeat methodologies to ensure receipt of such information by the devices. Point-to-point systems (e.g., Telematics) transmit Conditional Access information in a 2-way manner and use acknowledgement methodologies to ensure receipt of such information by the devices.

## **SUMMARY OF THE INVENTION**

Various multiple methods of data transport, and combinations thereof, may be used to initialize or update conditional access information on various devices. In an integrated device having both a broadcast receiver, such as an SDARS receiver, and a two-way communications transceiver, such as an LTE, 3G or 4G modem, conditional access information for the broadcast receiver may be sent to the transceiver, and then passed to the broadcast receiver, or vice versa. Additionally, for example, the broadcast receiver may be sent, over the broadcast communications channel, a “wake-up” message for the two-way transceiver, which may then be passed to the two-way transceiver, so as to make it ready to receive conditional access information over the two-way communications channel, or vice versa. Moreover, because of the presence of a two-way communications path, various acknowledgements of conditional access status updates received and processed by the broadcast receiver may be sent – thus realizing a significant improvement over the current practice of sending multiple periodic messages over the broadcast channel, to insure (but never have a confirmed) receipt.

## **BRIEF DESCRIPTION OF THE DRAWINGS**

The invention will be more readily understood with reference to various exemplary embodiments thereof, as shown in the drawing figures, in which:

Fig. 1 illustrates updating 2-way Conditional Access information using a broadcast 1-way path with an acknowledgement sent using the transmit path of the 2-way portion of the device according to an exemplary embodiment of the present invention;

Fig. 2 illustrates updating 1-way Conditional Access information using a broadcast 1-way path an acknowledgement sent using the transmit path of the 2-way portion of the device according to an exemplary embodiment of the

present invention;

Fig. 3 illustrates updating 1-way Conditional Access information using a 2-way path with an acknowledgement sent using the transmit path of the 2-way portion of the device according to an exemplary embodiment of the present invention;

Fig. 4 illustrates updating 2-way Conditional Access information using a broadcast 1-way path to wake up a 2-way portion of the device to prepare to receive the Conditional Access information using the 2-way path with an acknowledgement sent using the transmit path of the 2-way portion of the device according to an exemplary embodiment of the present invention;

Fig. 5 illustrates updating 1-way Conditional Access information using a 2-way path to wake up a 1-way portion of the device to prepare to receive the Conditional Access information using the 1-way path with an acknowledgement sent using the transmit path of the 2-way portion of the device according to an exemplary embodiment of the present invention;

Fig. 6 illustrates updating 2-way Conditional Access information using a 2-way path to wake up a 1-way portion of the device to prepare to receive the Conditional Access information using the 1-way path with an acknowledgement sent using the transmit path of the 2-way portion of the device according to an exemplary embodiment of the present invention;

Fig. 7 illustrates updating 1-way Conditional Access information using a 2-way path of a tethered or integrated 2-way transceiver device according to an exemplary embodiment of the present invention;

Fig. 8 depicts further details of the various processes depicted in Fig. 7; and

Fig. 9 illustrates multiple two-way remote transceiver devices temporarily connected to a broadcast receiver device and accessing programming that it

receives according to an exemplary embodiment of the present invention.

## **DETAILED DESCRIPTION OF THE INVENTION**

Conditional Access information is needed to access protected communications channels, such as, for example, subscription service satellite radio or television, or, for example, cellular phone and data access via a wireless communications network or the like. In general, a user device needs to receive conditional access information in order to receive and decode the subscribed to service, or to access the communications network. In one approach, this information can be sent initially, and then the device has and retains access until a follow-up message removing the access is sent.

Previous systems and methods for transmitting conditional access information to satellite broadcast services generally relied solely on a broadcast transmission path to send the conditional access information. They tended to rely on a “controller” to make a determination as to whether or not it was connected to the subscription receiver, and then also relied on the same controller to request a deactivation to remove service from the subscription receiver.

In contrast, in exemplary embodiments of the present invention, a subscription receiver may, for example, require a periodic or quasi-periodic sequence of conditional access updates at a substantially fixed, or some configurable, frequency in order to maintain its activation state. This is an inherently more secure method of ensuring that, for example, a radio authorized using this method will only remain authorized for an extremely limited time. In one implementation, using a tethered smart phone to a satellite radio receiver (shown in Fig. 7) a “next request time” may be explicitly sent at the time the authorization is provided, along with an expiration time of the initial authorization. In a scheme such as this, the expiration time could be a short period such as, for example, 10 to 15 minutes and the next request time could be something somewhat less than the expiration time such as, for example, 5

minutes. Thus, the initial authorization would last only for that short period, unless a series of subsequent authorization requests were sent and granted. For example, an initial authorization can be for 15 minutes. Moreover, a request for authorization can be sent every 5 minutes and each granted request for authorization can, for example, push the expiration time 15 minutes past the last granting time. In this way network delays or brief outages will not terminate the broadcast authorization, but once the devices are no longer paired, the broadcast subscription will quickly time out. The time-limited limited authorization eliminates the need for a two-way transceiver device to send a deactivation request. In general, the expiration time maybe a number of minutes  $N$ , and authorization requests can be sent every  $M$  minutes, where  $M < N$ .  $M$  may be, in various implementations,  $N/4$ ,  $N/3$ ,  $N/2$ ,  $2N/3$ , or any other, as desired, length of time less than  $N$ .

In what follows, the term "1-way" refers to a communications channel, where communications are sent from a source to one or more receivers, but the receivers cannot communicate back to the source, such as in a radio service broadcasting to various receivers. Similarly, "2-way" refers to a communications channel, such as a point to point system, where a first point can transmit to a second, and in turn the second point can transmit back to the first point, such as, for example, in cellular communications, satellite telephones, wired and wireless communications networks, etc..

Various methods exist for effecting Conditional Access for a system with devices to be activated and/or authorized in the field. For example, broadcast systems, such as, for example, satellite radio services, transmit Conditional Access information in a 1-way manner and use multiple repeat methodologies to ensure receipt of such information by the devices. Point-to-point systems, such as, for example, Telematics, transmit Conditional Access information in a 2-way manner and use acknowledgement methodologies to ensure receipt of such information by the devices. Combining these modalities in a single device or in a pair of linked or tethered devices, provides enhanced functionality.

In what follows, various exemplary implementations to send and acknowledge Conditional Access messages are described, for both a “single device” scenario as well as a “dual device” scenario. In particular, Figs. 1-6 illustrate examples for a single integrated device, such as may be used in an integrated telematics and SDARS unit (sometimes known as a Connected Services Unit, or “CSU”) containing both a 1-way receive path, and at least one 2-way transmit/receive path. Similarly, Figs. 7-8 illustrate an example for two devices that are temporarily tethered or connected, such as may be used in a smartphone tethered to a head unit containing an SDARS receiver, for example.

### **Single Device Concept**

In exemplary embodiments of the present invention, a single device system can, for example, include at least one 1-way receive path, and at least one 2-way transmit/receive path, a controller connected to all receive-only paths and all transmit/receive paths, and a non-volatile memory to store received Conditional Access information. In addition, such a system can interact with a Conditional Access control center that transmits using one or more transmit paths, and receives using one or more receive paths, the relevant Conditional Access information to a plurality of devices in the field. In various exemplary embodiments of the present invention, Conditional Access information can be transmitted using one or more paths, and one or more acknowledgements, if any, can be received using one or more paths. Various permutations of such a process are possible, and thus Figs. 1-6, next described, illustrate six exemplary scenarios for updating Conditional Access information.

As noted, a single device system as shown in Figs. 1-6 can be a “Combined Services Unit” or “CSU”, for use in vehicles. The CSU can integrate SDARS receiver functionality with an LTE, 3G, 4G or even 5G modem, and thereby implement telematics type functionality.

In all of these single device scenarios, as well as any dual device scenario described below, the initial request from a potential subscriber for radio

authorization (what may be termed “Step 0”) is not shown. It is noted that such a request to the Conditional Access control center may be accomplished via a phone call to a listener care center (where the order could be processed by an automated voice response system, or, for example, by a human listener care agent), by accessing a web portal using any device capable of accessing the Internet, or by some user interface connected directly to the single combined device itself.

Fig. 1 illustrates updating 2-way Conditional Access information using a broadcast 1-way path with an acknowledgement (either completion or partial) that is sent using the transmit path of the 2-way portion of the device. With reference thereto, at (index number) 1, the Unified Conditional Access Control Center sends conditional access information to the broadcast receiver device, as shown. At 2, the broadcast receiver device sends the conditional access information to the two-way transceiver device. The two-way transceiver device uses the conditional access information received from the broadcast receiver device to interact with its conditional access memory and update its conditional access information. The interaction with the conditional access memory is shown at 3 in the figure. Next, the two-way device sends an acknowledgement message, over a wireless or a wired network, for example, back to the Unified Conditional Access Control Center over the two-way communications path. As noted, the acknowledgement can be a simple acknowledgement of the conditional access state change, or optionally, can include a hash of the conditional access state, including other useful information. For example, the acknowledgement may contain a hash or permutation of the final conditional access state of the device, the hash including a cumulative result of all messages received along with at least one other event. Or, for example, the acknowledgement may include a hash or permutation of the final conditional access state of the device, the hash including a cumulative result of all messages received along with at least one of listening time and user actions. It is noted that by using a hash of the conditional access state change, or a hash of the complete conditional access state of the device, it is possible to confirm

that (i) not only were the conditional access messages received by the device, but that (ii) they were also processed and acted upon to effect a desired change in conditional access state, and thus that (iii) the device is now in the desired end-state, able to decrypt content in accordance with its account status. Thus, no additional messages would then be required to be sent to the device.

A similar communications process can be used to update the conditional access information for the one-way, or broadcast receiver, device as shown in Fig. 2. Fig. 2 illustrates updating 1-way Conditional Access information using a broadcast 1-way path an acknowledgement (either completion or partial) sent using the transmit path of the 2-way portion of the device. With reference to Fig. 2, the Unified Conditional Access Control Center sends conditional access information at (index number) 1 to the broadcast receiver device. The broadcast receiver device uses the conditional access information to interact with its conditional access memory, as shown at 2, and then, when the information is updated or processed, the broadcast receiver device communicates an acknowledgement at 3 through the controller to the two-way transceiver device. The two-way transceiver device then sends this acknowledgement, at 4, over the wireless or wired network back to the Unified Conditional Access Control Center. Thus, in this scenario the broadcast device is authorized over the broadcast transmission path and an acknowledgement is sent over the two-way path.

Fig. 3 illustrates updating 1-way Conditional Access information using a 2-way path with an acknowledgement (either completion or partial) sent using the transmit path of the 2-way portion of the device. Here the Unified Conditional Access Control Center first sends conditional access information over the wireless or wired network at the right side of Fig. 3, at (index number) 1, to the two-way transceiver device. The two-way transceiver device, at 2, communicates the conditional access information to the one-way device, namely, the broadcast receiver device. In similar fashion to that described above in connection with Fig. 2, the broadcast receiver device at 3 then

accesses the conditional access memory to update its conditional access information. It then sends an acknowledgement at 4 across the controller to the two-way transceiver device which then at five returns the acknowledgement information through the wireless or wired network to the Unified Conditional Access Control Center.

Figs. 4-6 add a bit of complexity, namely, where on device is used to wake up another to then receive conditional access information. These scenarios are next described.

Fig. 4 illustrates updating 2-way Conditional Access information (on the two-way portion of the device) using a broadcast 1-way path to *wake up* a 2-way portion of the device to request the Conditional Access information using the 2-way path with an acknowledgement (either completion or partial) to be sent using the transmit path of the 2-way portion of the device. With reference thereto, at 1, the Uniform Conditional Access Control Center sends a “wake-up” message over the broadcast channel, or the one-way path, to the broadcast receiver device. The broadcast receiver device passes along, at 2, the wake-up message to the two-way transceiver device. The two-way transceiver device, then, having received the wake-up message, at 3, sends a request to the Unified Conditional Access Control Center over the wireless or wired network for the conditional access information. The Unified Conditional Access Control Center sends the conditional access information, at 4, over the same, or over another, wireless or wired network, to the two-way transceiver device which then accesses the two-way transceiver device’s conditional access memory at 5 thereby updating its conditional access information. When the conditional access information has been updated, an acknowledgement message is sent at 6 from the two-way transceiver device over the wireless or wired network to the Unified Conditional Access Control Center.

It is noted that the scenario of Fig. 4 is useful when the broadcast receiver device is continually on -- but for reasons of savings energy or saving power, or

the two-way transceiver device imbedded in an exemplary Combined Services Unit (CSU), as shown in Fig. 4, is not always on and is often in a sleep state. In such a sleep state, therefore, it cannot receive its own conditional access update information unless it is first woken up; that is the function of sending the wake-up message, at 1, to the broadcast receiver device, which then passes the wake-up message, at 2, to the two-way transceiver device. Once the two-way transceiver device has been awakened, it can proceed to request the conditional access update, at 3, as described above.

Fig. 5, in similar fashion to Fig. 4, illustrates updating 1-way Conditional Access information using a 2-way path to wake up a 1-way portion of the device to prepare to receive the Conditional Access information using the 1-way path with an acknowledgement (either completion or partial) sent using the transmit path of the 2-way portion of the device. This is essentially the inverse of the situation illustrated in Fig. 4. With reference to Fig. 5, the Unified Conditional Access Control Center, shown at the right side of the figure, sends a wake-up message at one over the wireless or wired network to the two-way transceiver device embedded in the CSU. (It is noted that the Unified Conditional Access Control Center is simply shown on both the far right and the far left sides of the figure for convenience, and that it can be, and often is, the same Unified Conditional Access Control Center). The two-way transceiver device passes this wake-up message at 2, through the controller, to the broadcast receiver device. The broadcast receiver device, then, now having been awakened, can receive the conditional access information from the Unified Conditional Access Control Center, at 3. It is noted that, unlike the situation of the two-way transceiver device of Fig. 4, the broadcast receiver device in Fig. 5, once awakened, cannot request its conditional access update from the Unified Conditional Access Control Center. Rather, once the wake up is sent, a defined time period can be waited, and following the lapse of such a time period, where it can be safely assumed that the broadcast receiver device has now been awakened, the Unified Conditional Access Control Center can begin

sending conditional access updates, or information messages, over the broadcast channel, at 3. Having received the conditional access information at 3, the broadcast receiver device can now interact with the conditional access memory, at 4, to update its conditional access state. Having completed the update, it can pass an acknowledgement message, at 5, through the controller to the two-way transceiver device embedded in the CSU. Upon receipt of the passed acknowledgement, the two-way transceiver device, at 6, can send the acknowledgement over the wireless or wired network back to the Unified Conditional Access Control Center which can then verify that the broadcast receiver device has received the broadcast conditional access information which was sent at 3.

Finally, Fig. 6 illustrates updating the two-way transceiver's conditional access information using (i) the two-way path to (ii) wake up the one-way portion of the CSU to prepare to receive conditional access information using the one-way path, with an acknowledgement (either completion of update or partial) being sent using the transmit path of the two-way portion of the device. This is essentially the same process as shown in Fig. 5, except that the conditional access information sent to the broadcast receiver device is not used by it itself, but rather is simply passed by the broadcast receiver device, through the controller, to the two-way transceiver device. The reason why one would do this is if, for example, the conditional access information update is large and it would cost some not insignificant amount to send it over the wireless or wired network -- where data is charged for by usage -- and therefore it being cheaper or more economical to send it over the broadcast channel which is, essentially, once in place, free.

Continuing with reference to Fig. 6, the Unified Conditional Access Control Center initiates sending a wake-up message 1 over the wireless or wired network to the two-way transceiver device. Upon receipt of this message, at 2, the two-way transceiver device passes the wake-up message to the broadcast receiver device. The broadcast receiver device, after an appropriate time, can

be assumed to now be awake and able to receive conditional access information. This information is then sent at 3 from the Unified Conditional Access Control Center. Upon receipt of the conditional access information, the broadcast receiver device, at 4, passes that conditional access information to the two-way transceiver device which, at 5, interacts with its conditional access memory to update its conditional access state. Upon completion of the update, or, for example, not an update at all, but rather an initial provisioning or granting of conditional access to the two-way transceiver device, the two-way transceiver device sends an acknowledgement, at 6, over the wireless or wired network back to the unified conditional access control center.

It is noted that the situation of Fig. 6 also assumes that the broadcast receiver device is not always on, but may be in a sleep mode and require waking up through the message 1, which is passed to it at 2, in order to receive the content of the conditional access information which is sent as a message at 3, in order that the broadcast receiver device, once having received it, can pass it to the two-way transceiver device. Thus, the scenario of Fig. 6 assumes that it is (i) cost effective to send the conditional access information over the broadcast channel, namely the one-way channel, and (ii) only to send wake-up messages and acknowledgements over the wireless or wired network, and that (iii) the broadcast receiver device is not always on, whereas the two-way transceiver device *is* always on. In general, when using one device to wake up the other in, for example, an integrated combined services unit, or, for example, in a temporarily connected context (e.g., a tethered smartphone to an SDARS head unit in a vehicle) such as is described below in connection with Figs. 7-9, the device which is assumed to be always on is the one to which the wake-up message is initially sent (because it is unreliable to send a "wake-up" message to a sleeping device which may never get there) and that "always on" device passes the wake-up message to the other device --- which is not always on. Then, once the latter device is awakened, it can receive the actual content of the lengthy conditional access message for either itself, or for the two-way transceiver device, which are the cases shown respectively in Figs. 5 and 6.

It is here noted that in the context of a future wake-up event, an exemplary device may send an acknowledgement of the fact that a future wake-up message was received, processed and stored so that the Central Conditional Access Center may have some reasonable degree of confidence that (i) it could begin transmitting the conditional access information at that future time, and that (ii) the intended target or targets for the messages would be awake to receive the messages. Clearly, the acknowledgement can only be sent during a period of time when the one-way device itself is awake prior to the scheduled wake-up time of the one-way device to receive the conditional access information. For example, a message could be sent over the two-way path on a Monday morning indicating that a given broadcast receiver device (that is not always on) should wake up on the following Wednesday at 2 AM to receive an update. On Tuesday the broadcast receiver device wakes up as part of normal operation, receives the future wakeup message from the two-way device and acknowledges receipt to the two-way device. Then the two-way device may, for example, send that acknowledgement to the Conditional Access center, and the 2AM transmission from the Conditional Access Center to the one-way broadcast receiver device can take place as scheduled. If the one-way broadcast receiver device is never powered up, and/or never acknowledges receipt of the message, then the 2AM broadcast is delayed, or, for example, in the case that the broadcast is targeted at multiple one-way devices, some of which may have acknowledged receipt while others have not, an alternate path can be used to update those specific one-way devices, such as, for example, using a two-way path of a device connected to them, such as the two-way device in Figs. 5 and 6.

### **Additional Acknowledgements**

It is further noted that in exemplary embodiments of the present invention, various other acknowledgements may be sent, as may be useful, in any of the single unit (e.g., CSU) or double unit (e.g., tethered smartphone to broadcast receiver device in vehicle head unit) scenarios described herein. The

illustrative acknowledgements shown in Figs. 1-8 are thus purely exemplary in nature, and not intended as exclusive or comprehensive.

Other examples of acknowledgements which may be useful, specifically in the case of very lengthy messages or conditional access code updates, which may be sent in pieces or as a plurality of individually identifiable messages or packets, can include, for example:

(1) acknowledgements that include a sequence number or index (or list of sequence numbers or indices), or other similar means of indicating which specific message(s) or packet(s) out of the plurality of required packets have been received by the device, so that the transmission of those specific packets or messages can be stopped; and

(2) acknowledgements that include a sum or total number of received packets or messages so that the effectiveness of the transmission can be evaluated. For example, if only 50% of the required messages have been received via the broadcast path, the transmission of those messages may need to be continued for a longer time, or alternatively, the remaining messages may need to be transmitted via the two-way transmission path.

### **Dual Device Concept/Scenarios**

In addition to the single-device scenarios of Figs. 1-6, there also exist scenarios for hybrid conditional access in which a stand-alone broadcast receiver device (e.g. a satellite radio) is temporarily docked or tethered to one or more devices, such as, for example, a smart phone, smart pad, laptop, etc, that provides access to a two-way wireless or wired communications network. In this “temporarily connected” scenario (which is similar to the scenario of Fig. 3 for the single integrated device) the authorization for the broadcast receiver is valid only for the duration (or substantially only for the duration) that the two devices are tethered or docked. This feature is most useful, as it allows a “portable”

broadcast subscription to be moved around, from device to device, by a subscriber, freeing he or she from a single vehicle, radio, or other dedicated device.

As noted above, Figs. 7 and 8 illustrate exemplary methods for updating conditional access information in a dual device scenario. As noted, such a scenario can include, for example, a pair of devices, where at least one device includes a 1-way receive path for an encrypted broadcast communication and the other device includes at least one 2-way transceiver that enables communication with for example a wide area network, and both devices are temporarily linked or tethered together such that they can exchange information with each other, send requests for authorization to the conditional access control center, and transfer any temporary authorization from the Conditional Access Control Center enabling the broadcast receiver to receive encrypted communications over the broadcast path while the two devices are linked or tethered.

#### **Dual Device Concept:**

In exemplary embodiments of the present invention, a dual device system may include: (1) A Satellite Radio Module or Receiver Unit that includes (1a) at least one method of linking or tethering to (2) a Mobile Wireless Communication Device with the ability to transfer data, at least a (1b) unique Radio Device ID and at least (1c) one secret key or other method for signing or encrypting information, and (1d) the ability to encrypt or otherwise authenticate (using a MAC, for example) a (2a) unique ID associated with (2) a Mobile Wireless Communication Device having (2a) a unique device identity comprising IMEI, CCID, Serial number, or some combination of these factors, and the ability to send (2b) an Authorization Request to (3) A Unified Conditional Access Control Center with at least (3a) a server, and at least (3b) a Subscriber Database and (3c) a Radio Device Database, such that the server (3a) can look up an subscription account in the Subscriber Database based on a unique Mobile

Wireless Communication Device identity, look up (1b) the Radio Device ID in the Radio Device Database to find the appropriate key and/or algorithm to decrypt or validate an authorization request, generate (4) an Authentication Message containing at least (4a) an authorization code or key and (4b) an expiration date and time (4a and 4b are not shown in Fig. 7 explicitly, but are understood to be subsumed under “Authorization Message” 4).

In a preferred exemplary implementation, the Mobile Device, or more correctly, an application running on the Mobile Device, can, for example, send the Mobile Device Identity (2a) to (1) the Receiver Unit (or Radio Module), which in turn can secure the unique ID by encryption or appending a message authentication code. The Mobile Device can then send an (2b) Authorization Request – an example of which is shown at the bottom left of Fig. 7, containing a Secured Mobile Device Identity (with Radio Key, time and sequence number) and a Radio ID, thus identifying each of the two devices shown as tethered in Fig. 7 -- to (3) the authentication server (UCACC), which (i) first determines if an active “portable satellite radio subscription” is associated with that Mobile Device ID (2a), and then (ii) looks up the Radio Device ID of the Receiver Unit (1) so that it can decrypt or authenticate the message and know that the Mobile Device is communicating with the Radio Module (Receiver Unit) in real time. As described above, the authentication server can then generate Authorization Messages (4) in response to each valid authenticated Authorization Request (2b). An example format of the Authorization Response (4) is shown at the bottom right of Fig. 7. It contains a Secure Authorization With Expiration, and may be encrypted with Radio Key and other information, such as, for example, time and sequence number so as to make locally stored repeats useless. It can also, as shown, contain a Next Request Time (in the clear), which can be set by the authorization server or the Unified Conditional Access Control Center to be prior to the (secret) Expiration Time in the Authorization Response. Thus, in a preferred implementation, the expiration date and time in the Authorization Message (4), can be adjusted to be longer than the scheduled frequency of Authorization Requests (2b), so as to allow for lower wireless charges and the

possibility of Internet delays or packet loss. For example, such expiration times can be 1 minute in the future, and the Authorization Request could be sent every 20 or 30 seconds. Various similar combinations of these values can be implemented, as described above.

In an alternate exemplary implementation, the next request time could be hard coded to a specific fixed offset from the expiration time, so that the next request is always sent, for example, N seconds before the authorization expires. Still alternatively, the expiration time could be a fixed offset M from the time that the authorization message was received by the device, such that each authorization message received would grant service for some fixed amount of time, such as, for example, 10 minutes, 15 minutes, 20 minutes, etc.. In the above example, N could be, for example, 60, 90 or 120 seconds, or any other convenient increment.

Fig. 8 provides additional details of the process shown in Fig. 7 and described above. As shown in Fig. 8, Steps 1 and 2 of Fig. 7 happen during the tethering process (or immediately after tethering is complete), and then happen again periodically for the satellite radio device to remain authorized, as noted.

Moreover, Mobile Device ID may be a serial number, MEID or IMEI, ICCID, phone number or CDN or some combination of all, or a defined subset of, these numbers. Finally, Radio Device Key is a secret Key available to the Radio Device (and also, of course, known to the Conditional Access Control Center).

Fig. 8 also shows exemplary fields in each of the Subscriber Database, and Radio Device Database.

Thus, as shown in Fig. 8, at 1 the Wireless Mobile Device sends the Mobile Device ID (2a) to the Radio Device. The Radio Device then sends the (Mobile Device ID) + Radio ID at 2 back to the Wireless Mobile Device, which then sends an Authorization Request at 3, to the Unified Conditional Access Control Center. Upon receiving the Authorization Request, as noted the UCACC first determines if an active "portable satellite radio subscription" is associated with

that Mobile Device ID, and then (ii) looks up the Radio Device ID of the Radio Device so that it can decrypt or authenticate the message and know that the Mobile Device is communicating with the Radio Device in real time. Once verifying this information, the Unified Conditional Access Control Center generates and sends an Authorization Response, at 4, to the Wireless Mobile Device, which then sends an Authorization Credit at 5 to the Radio Device.

### **Multiple Two-way Devices Connected**

Fig. 9 illustrates connecting multiple two-way remote transceiver devices to a broadcast receiver device according to an exemplary embodiment of the present invention. Such a scenario may be very useful in a vehicle equipped with a broadcast receiver, such as, for example, an SDARS receiver, where the broadcast receiver device can actually decode multiple channels simultaneously, even though a user, such as the driver, may choose to only listen to one, or none, or may not even be authorized to play any. In exemplary embodiments of the present invention, other users can each access a different channel of their choice from channels in the broadcast multiplex, and can each play that channel through their two-way transceiver device, such as a smartphone, using ear buds or headphones.

With reference to Fig. 9, the following exemplary process may be implemented. At 1 a Two-way Transceiver Device, say a Smartphone, requests access (e.g. "tune channel 7") from the Broadcast Receiver Device. At 2 the Broadcast Receiver Device requests authorization to serve the smartphone. In response, at 3 the Smartphone requests an authorization code from the Unified Conditional Access Control Center, and at 4, the Unified Conditional Access Control Center sends an authorization code to the Smartphone. Once received, at 5, the Smartphone sends the authorization code to the Broadcast Receiver Device, and now duly authorized, the Broadcast Receiver Device provides

access (e.g., tunes to channel 7 and transmits, for example, the signal over Wi-Fi) to the Smartphone.

In this way, the Broadcast Receiver Device can support multiple smartphones. Moreover, even if the Broadcast Receiver Device is not an authorized SDARS receiver on its own, such as, for example, the owner of the vehicle has not yet subscribed to the SDARS service that the Broadcast Receiver Device receives, the authorization code received from the Smartphone will enable it to be authorized for the specified period of time AND only authorized for the specific two way transceiver device (smartphone) that requested such access. In other words, if the SDARS device is not authorized, it can, for example, provide channel 7 over Wi-Fi to the smartphone, but it will NOT play any channels on its own (in the vehicle). Alternatively, even if not authorized, if an authorized Smartphone is tethered to it, while the two are tethered, the Broadcast Receiver Device can also play any channels on its own, under a “derivative” authorized subscription. Various contractual combinations and permutations are possible in various exemplary embodiments.

It is noted that one smartphone may request access on behalf of a number of additional smartphone listeners, or for an unauthorized broadcast receiver itself, as long as its account with the SDARS broadcasting service allows such multiple device access. If multiple smartphones request and gain access independently, they may each be independently served by the broadcast receiver device, and then if one leaves, this has no effect on the others' ability to listen. As can well be appreciated, many variations are possible, all dependent upon the level of access granted by the SDARS service to each smartphone owner; all such possibilities being within the scope of the present invention.

### **Sending Decryption Keys Over A Broadcast Receiver**

In exemplary embodiments of the present invention, a large number of encrypted, device specific authentication certificates, for various types of

devices needing conditional access may be stored in a broadcast communication receiver device associated with one or more such devices, and using a decryption key, then be transmitted over a broadcast communication path on a periodic basis (e.g. weekly, monthly or quarterly) to enable the broadcast receiver to unlock one or more certificates or bundles of certificates for use in various types of in-vehicle as well as general two-way network communications. It is noted that the decryption key referred to above is a relatively small amount of data, and it is this decryption key entity that is transmitted over the broadcast path. Once received, the key can then be used to decrypt the (relatively large) certificate that is already stored in a given device.

For example, a given device that regularly updates its access to a network, such as, for example, a V2V device, in-vehicle communications device, or more generally, any other “guest” or temporary user of a large number of users network, may, for example, have three years of certificates stored in it at the time of “personalization” before being deployed to the field. These certificates may be used at some finite rate, say, for example, a rate of 20 per week and then expire over time. In order to be renewed, such a device must communicate with “infrastructure” to request additional certificates. However, at least some vehicles may operate in remote areas where the ability communicate with such infrastructure devices is rare or non-existent. Increasing the number of pre-stored certificates increases the potential number of certificates that must be revoked if one of the in-vehicle or other devices is “rogue” (e.g., transmitting false and/or misleading information with the intent of disrupting traffic) so that other vehicles, or other participants in the multi-user network, will no longer trust the device and all of its certificates. A better solution is to store additional certificates in a way that they can be efficiently released over time with messages broadcast over a satellite path.

Thus, for example, a satellite receiver may have ten years' worth of certificates (such as, for example, 20 certificates per week, for 52 weeks per year, for 10 years, or 10,400 total certificates). Each bundle of 20 certificates can, for example, have a validity period of one week, and each week the satellite transmission system could send messages to radios (or groups of radios) containing the key necessary to decrypt that week's worth of certificates for use, in the event that they were unable to replenish their certificates through the normal network infrastructure. Alternative implementations can, for example, bundle the certificates in groups with longer validity periods, such as, for example, 20 certificates with a one month validity period, and/or in various different size groups. In a further refinement of this approach, the key used to decrypt the certificates can be designed such that each decryption key could be used to decrypt the certificates in one group as well as evolving the decryption keys required for all previous certificate groups. In this way, transmitting a single decryption key to a single device could unlock a variable number of certificates for future use. Thus, for example, transmitting the "July 2020 group key" would unlock certificates for July 2020, June 2020, May 2020, and so forth, back to the current month.

The above-presented description and figures are intended by way of example only and are not intended to limit the present invention in any way except as set forth in the following claims. It is particularly noted that the persons skilled in the art can readily combine the various technical aspects of the various elements of the various exemplary embodiments that have been described above in numerous other ways, all of which are considered to be within the scope of the invention.

**WHAT IS CLAIMED:**

1. A method for authorizing a two-way device for operation on a wireless network, comprising:  
using a broadcast receiver to receive an encrypted broadcast transmission containing conditional access information;  
passing the conditional access information to the two-way device; and  
processing the conditional access information on the two-way device.
2. The method of claim 1, wherein the conditional access information includes a configuration file enabling a cellular device to migrate from one wireless network provider to another wireless network provider without the cooperation of the first network provider.
3. The method of claim 1, wherein at least one of:
  - (i) the broadcast receiver first processes the conditional access information before passing it; and
  - (ii) the conditional access information triggers a switch in a wireless device from one stored profile to another profile; and
4. The method of claim 1 wherein the two-way device and the broadcast receiver are integrated in a single device further including a controller that can coordinate and mediate their communications and route data between them.
5. The method of claim 1 in which the broadcast receiver is a satellite radio receiver.
6. The method of claim 1 wherein the two-way device is one of:  
a cellular phone that is tethered or docked to the broadcast receiver device; and  
an embedded modem in a vehicle.

7. A method, comprising:  
receiving one or more conditional access messages over a broadcast communications path;  
sending an acknowledgement of said receipt or acting upon said received message using a two-way communications path,  
wherein said two-way communications path includes at least one of a wired or a wireless network.
8. The method of claim 7, wherein the acknowledgement identifies the messages that were received using an index or reference.
9. The method of claim 7, wherein the acknowledgement is encrypted or signed by the receiver in a way that authenticates that the messages were received by the targeted device.
10. The method of claim 7, wherein the acknowledgement includes a hash or permutation of the final conditional access state of the device.
11. The method of claim 10, wherein said hash includes a cumulative result of all messages received along with other events such as listening time and user actions.
12. The method of claim 7, wherein receipt of the acknowledgement operates as a trigger to stop the repetition of conditional access messages addressed to the receiver.
13. The method of claim 7, wherein the conditional access messages enable the broadcast receiver to receive encrypted communications over a broadcast signal path.

14. The method of claim 7, wherein the conditional access messages remove authorization to receive encrypted communications over a broadcast path, causing the receiver to at least one of: be unable to decrypt those encrypted transmissions, and be unable to extract the protected transmissions.

15. The method of claim 1 wherein the two-way device and the broadcast receiver are integrated in a single device further including a controller that can coordinate and mediate their communications and route data between them.

16. The method of claim 7, wherein the broadcast receiver is a satellite radio receiver.

17. The method of claim 7, wherein the two-way device is a cellular phone that is tethered or docked to the broadcast receiver.

18. The method of claim 7 wherein the two-way device is one of: a cellular phone that is tethered or docked to the broadcast receiver device; and an embedded modem in a vehicle.

19. A method, comprising:

updating the conditional access state of a broadcast receiver by:

    sending a message over a two-way communications path;

    receiving the message at a two-way transceiver connected to the communications path; and

    passing the message to the broadcast receiver.

wherein said two-way communications path includes at least one of a wired or a wireless network.

20. The method of claim 19, wherein the conditional access messages enable the broadcast receiver to receive encrypted communications over a broadcast signal path.

21. The method of claim 19, wherein the conditional access messages remove authorization to receive encrypted communications over a broadcast path, rendering the receiver unable to decrypt those encrypted transmissions, or otherwise block the extraction of those protected transmissions.
22. The method of claim 19, wherein the two-way device and the broadcast receiver are both located in a single device along with a controller that can coordinate and mediate their communications and route data between them.
23. The method of claim 19 in which the broadcast receiver is a satellite radio receiver.
24. The method of claim 19, wherein the two-way device is a cellular phone that is tethered or docked to the broadcast receiver device
25. The method of claim 19, wherein the two-way device is an embedded modem in a vehicle.
26. The method of claim 19, wherein at least one of:
- (i) the acknowledgement identifies the messages that were received using an index or reference;
  - (ii) the acknowledgement is encrypted or signed by the receiver in a way that authenticates that the messages were received by the targeted device; the acknowledgement includes a hash or permutation of the final conditional access state of the device; and
  - (iii) the acknowledgement includes a hash or permutation of the final conditional access state of the device, and
  - (iv) the acknowledgement includes a hash or permutation of the final conditional access state of the device and said hash includes a cumulative result of all

messages received along with other events such as listening time and user actions.

27. A method, comprising:

sending a message over a broadcast path to a broadcast receiver;  
receiving the message at the broadcast receiver and passing the message to a connected or linked two-way communications device to wake up said two-way communications device so that the communications device can receive a configuration update.

28. The method of claim 27, wherein the two-way device and the broadcast receiver are one of:

(i) both located in a single device along with a controller that can coordinate and mediate their communications and route data between them;

or

(ii) wirelessly tethered or linked together.

29. The method of claim 27, wherein the two-way device and the broadcast receiver are at least one of:

(i) both located in a single device along with a controller that can coordinate and mediate their communications and route data between them;

(ii) wirelessly tethered or linked together;

(iii) linked or tethered through a wired connection;

(iv) linked or tethered through a docking connector or cable running between the two-way device and the one-way device, either directly or through an intermediary processor; or

(v) linked or tethered through a docking connector or cable running between the two-way device and the one-way device, through a vehicle-embedded controller or processor.

30. The method of claim 27, wherein the message sent over the broadcast signal path causes the two-way communication device to initiate communication with a conditional access server.

31. The method of claim 27, wherein one of:

- (i) the acknowledgement sent by the two-way device is sent on the same network as the updated conditional access information; and
- (ii) the acknowledgement sent by the two-way device is sent on a different network from the network over which the conditional access information was sent after applying the configuration file changes.

32. A method, comprising:

using a message transmitted over a two-way path to one of: enable, activate or “wake up” a broadcast receiver device; and  
sending additional messages to update the conditional access state of the broadcast receiver over a broadcast communications path.

33. The method of claim 32, wherein the message sent over the two-way network is one of: an SMS message sent over a wireless communication network, and sent over a wired or wireless internet protocol network .

34. The method of claim 32, wherein all or substantially all of the conditional access messages are sent over the broadcast path

35. The method of claim 32, wherein at least some portion of the conditional access messages are sent over the two-way path, and it is necessary to combine messages from the two-way path and the broadcast path to achieve the desired change in conditional access state.

36. The method of claim 32, wherein transmission of conditional access messages over the broadcast path is delayed until and conditioned on the

conditional access control center receiving a confirmation that the receiver has powered up and is able to receive the messages (i.e. is in good signal coverage).

37. The method of claim 32, wherein transmission of the conditional access messages begins a fixed time after the initial triggering message is sent.

38. The method of claim 32, wherein at least one of:

(i) the acknowledgement identifies the messages that were received using an index or reference;

(ii) the acknowledgement is encrypted or signed by the receiver in a way that authenticates that the messages were received by the targeted device;

(iii) the acknowledgement includes a hash or permutation of the final conditional access state of the device; and

(iv) the acknowledgement includes a hash or permutation of the final conditional access state of the device, and said hash includes a cumulative result of all messages received along with other events such as listening time and user actions.

39. The method of claim 32, further comprising at least one of:

sending an acknowledgement from the broadcast receiver device upon being “woken up”;

the message sent to the broadcast receiver device specifies a future wake up time, or a future wake up period, and the additional messages are sent after such time, or during said future period; and

sending an acknowledgement from the broadcast receiver device that a future wake up message has been received.

40. A method, comprising:

using a two-way communications device to send a wake-up message to a broadcast receiver to enable it to receive an update to the two-way device's configuration.

41. The method of claim 40, wherein the message sent over the two-way network is an SMS message sent over a wireless communications network.

42. The method of claim 40, wherein the message sent over the two-way network is sent over a wired or wireless internet protocol network .

43. The method of claim 40, wherein all or substantially all of the conditional access messages are sent over the broadcast path

44. The method of claim 40, wherein at least some portion of the conditional access messages are sent over the two-way path and messages from the two-way path and the broadcast path are combined to achieve the desired change in conditional access state.

45. The method of claim 40, wherein transmission of conditional access messages over the broadcast path is delayed until, and conditioned on, a conditional access control center receiving a confirmation that the receiver has powered up and is able to receive the messages (i.e. is in good signal coverage).

46. The method of claim 40, wherein transmission of the conditional access messages begins a fixed time after the initial wake-up message is sent.

47. The method of claim 40, wherein at least one of:  
the acknowledgement identifies the messages that were received using an index or reference;

the acknowledgement is encrypted or signed by the receiver in a way that authenticates that the messages were received by the targeted device;

the acknowledgement includes a hash or permutation of the final conditional access state of the device;

the acknowledgement includes a hash or permutation of the final conditional access state of the device, said hash including a cumulative result of all messages received;

the acknowledgement includes a hash or permutation of the final conditional access state of the device, said hash including a cumulative result of all messages received along with at least one other event;

the acknowledgement includes a hash or permutation of the final conditional access state of the device, said hash including a cumulative result of all messages received along with at least one of listening time and user actions.

48. A method, comprising:

using a two-way device to:

initiate a connection with a server and request time-limited authorization for a broadcast receiver temporarily connected to the two-way device;

and

periodically repeating the requests for authorization, so that the broadcast receiver remains authorized for as long as it remains connected to the two-way device.

49. The method of claim 48, wherein the two-way device is one of: a cellular phone, other portable wireless communication device, a tablet, and a wearable device.

50. The method of claim 48, wherein the broadcast receiver is a satellite radio receiver embedded in a vehicle.

51. The method of claim 48, wherein the request for authorization is triggered automatically upon linking or tethering the two-way communication device to the broadcast receiver.
52. The method of claim 48, wherein the request for authorization is initially triggered by some user action on the two-way communication device.
53. The method of claim 52, wherein said user action is at least one of: launching an application, turning on the user device, and waking up the user device.
54. The method of claim 48, wherein the authorization contains an explicit expiration and an explicit time to request reauthorization.
55. The method of claim 48, wherein the expiration is implied or derived by adding a defined offset to the time that the authorization is received.
56. The method of claim 48, wherein the time to request additional authorization is implied or derived by applying a defined offset to the authorization expiration.
57. The method of claim 48, wherein the two-way device identifies itself to the authorization server and that identity is linked to an account to determine if it is authorized for a portable broadcast reception subscription.
58. The method of claim 48, wherein an additional authorization is required to confirm that the two-way device is in the possession of an authorized individual.
59. The method of claim 58, wherein said additional authorization is at least one of a password, or a biometric identifier.

60. A method, comprising:

using a two-way device to:

initiate a connection with a server and request time-limited authorization for a broadcast receiver temporarily connected to the two-way device, repeating said request at a defined time period, to maintain the authorization of the broadcast receiver; and  
accessing programming received by the broadcast receiver by the two way device temporarily connected to the broadcast receiver.

61. The method of claim 60, further comprising accessing programming received by the broadcast receiver on at least one additional two way device temporarily connected to the broadcast receiver.

62. The method of claim 61, wherein any of the temporarily connected two-way devices can use the connection to receive programming from the broadcast receiver,  
and wherein each connected device can access different programming or channels received at the broadcast receiver, or can be used solely to maintain the broadcast receiver's authorization.

63. A method, comprising:

storing a large number of encrypted, device specific authentication certificates for one or more types of devices in a broadcast communications receiver device associated with a device; and  
transmitting a decryption key over a broadcast communications path to enable the broadcast receiver to unlock one or more of said certificates, or bundles of certificates, for use in communications.

63. The method of claim 63, wherein the broadcast communications receiver device is an SDARS receiver in a vehicle.

64. The method of claims 63 or 64, wherein said one or more types of devices include inter-automobile communications devices, roadside equipment to automobile communications devices, cell phones, and cellular network modems.

FIG. 1

Updating the 2-way Conditional Access information using the broadcast 1-way path with an acknowledgement (either completion or partial) sent using the transmit path of the 2-way portion of the device.

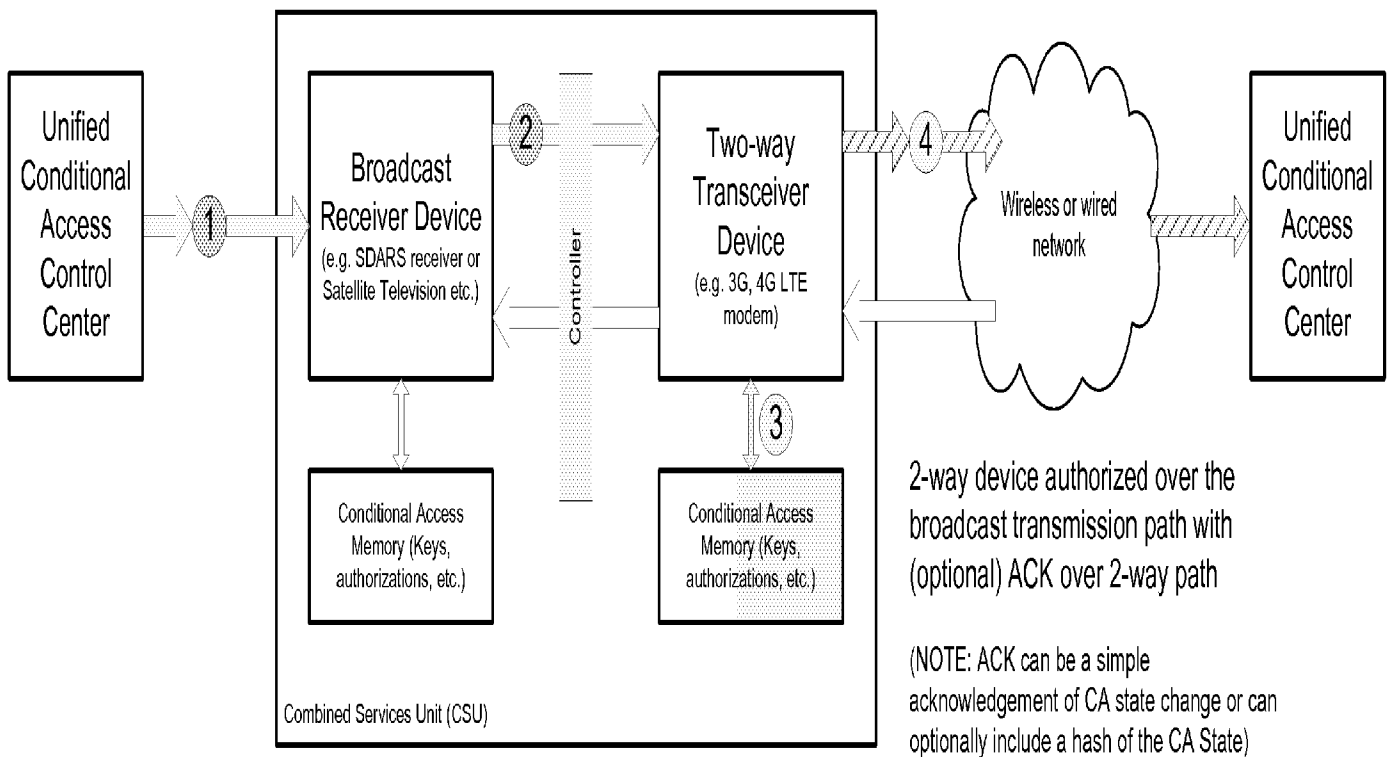


FIG. 2

Updating the 1-way Conditional Access information using the broadcast 1-way path with an acknowledgement (either completion or partial) sent using the transmit path of the 2-way portion of the device.

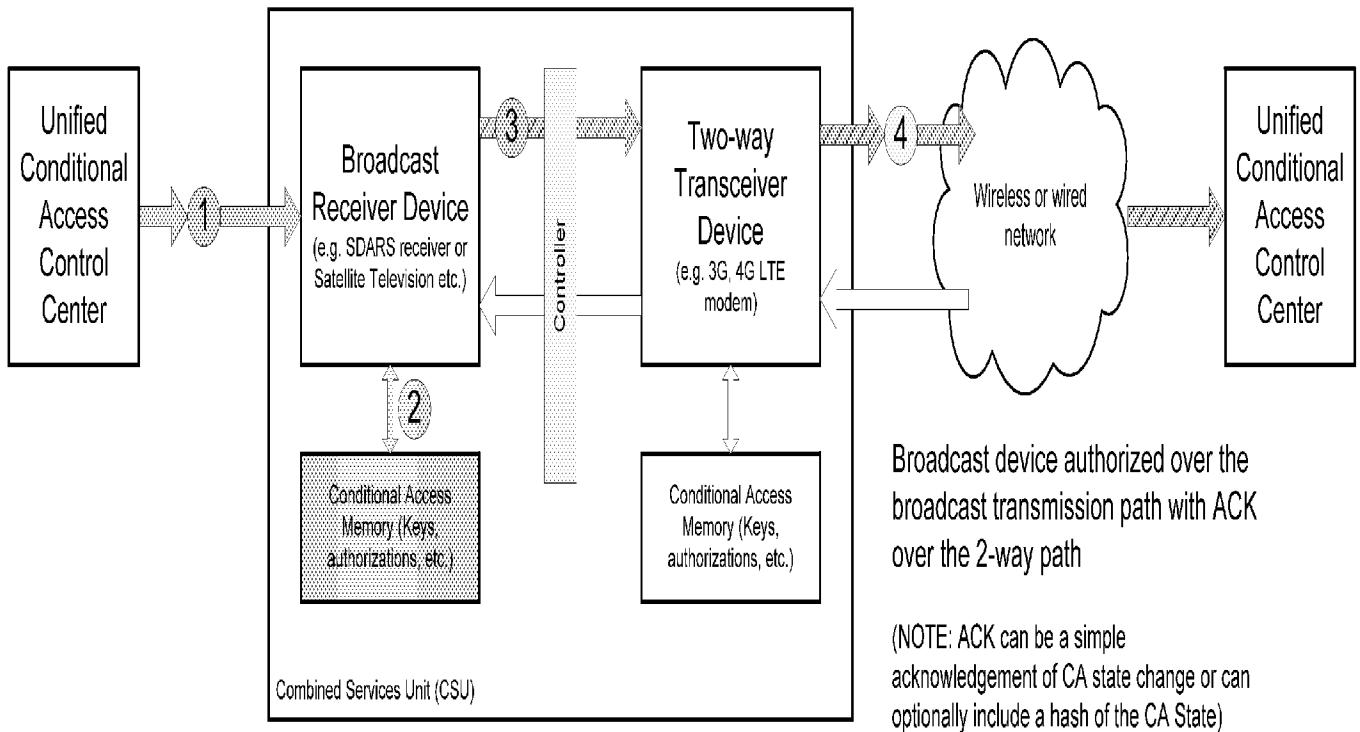


FIG. 3

Updating the 1-way Conditional Access information using the 2-way path with an acknowledgement (either completion or partial) sent using the transmit path of the 2-way portion of the device.

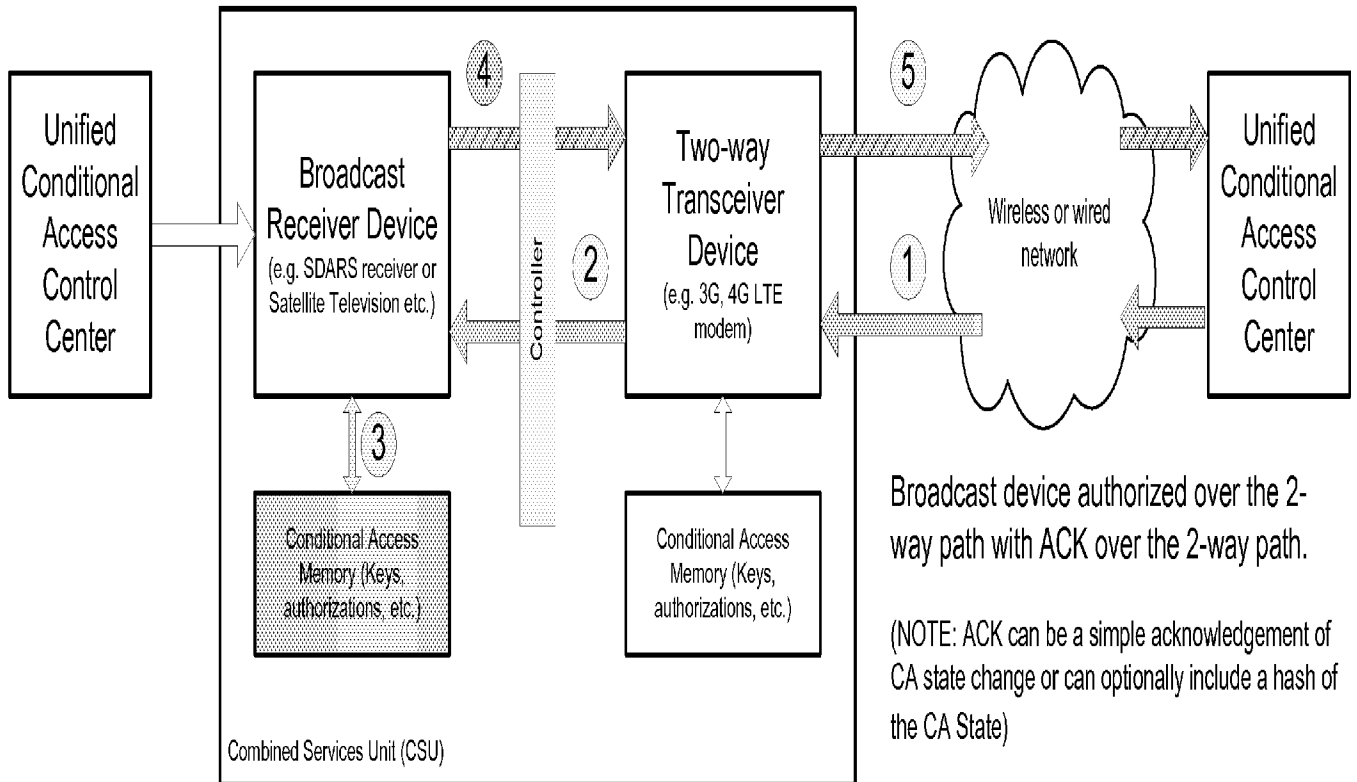
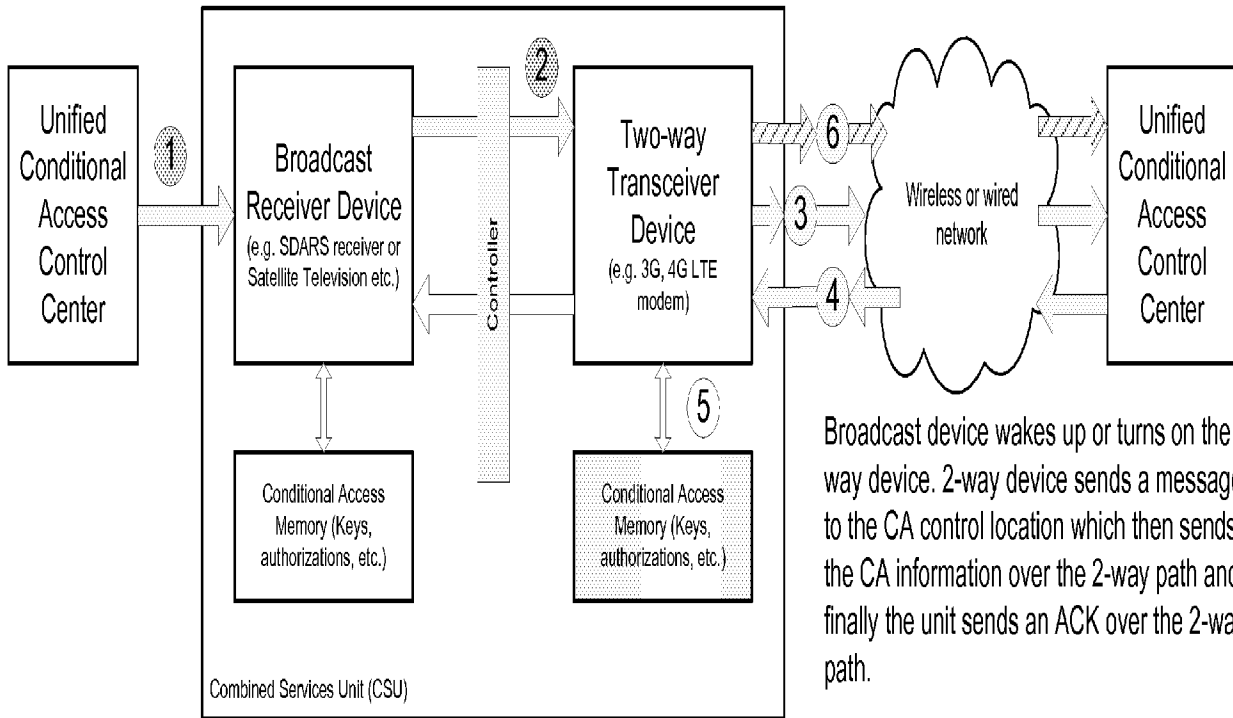


FIG. 4

Updating the 2-way Conditional Access information using the 1-way path to wake up the 2-way portion to prepare to receive Conditional Access information using the 2-way path with an acknowledgement (either completion or partial) sent using the transmit path of the 2-way portion of the device.

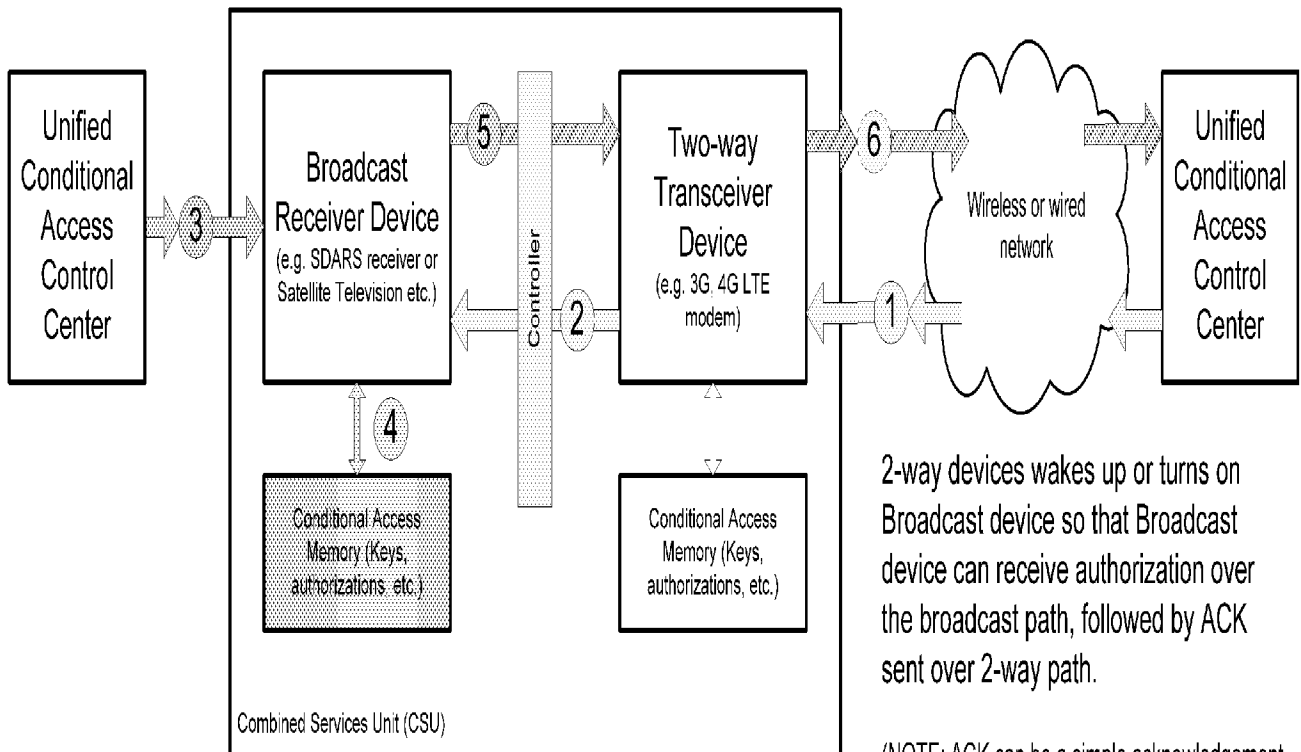


Broadcast device wakes up or turns on the 2-way device. 2-way device sends a message to the CA control location which then sends the CA information over the 2-way path and finally the unit sends an ACK over the 2-way path.

(NOTE: ACK can be a simple acknowledgement of CA state change or can optionally include a hash of the CA State)

FIG. 5

Updating the 1-way Conditional Access information using the 2-way path to wake up the 1-way portion to prepare to receive Conditional Access information using the 1-way path with an acknowledgement (either completion or partial) sent using the transmit path of the 2-way portion of the device.

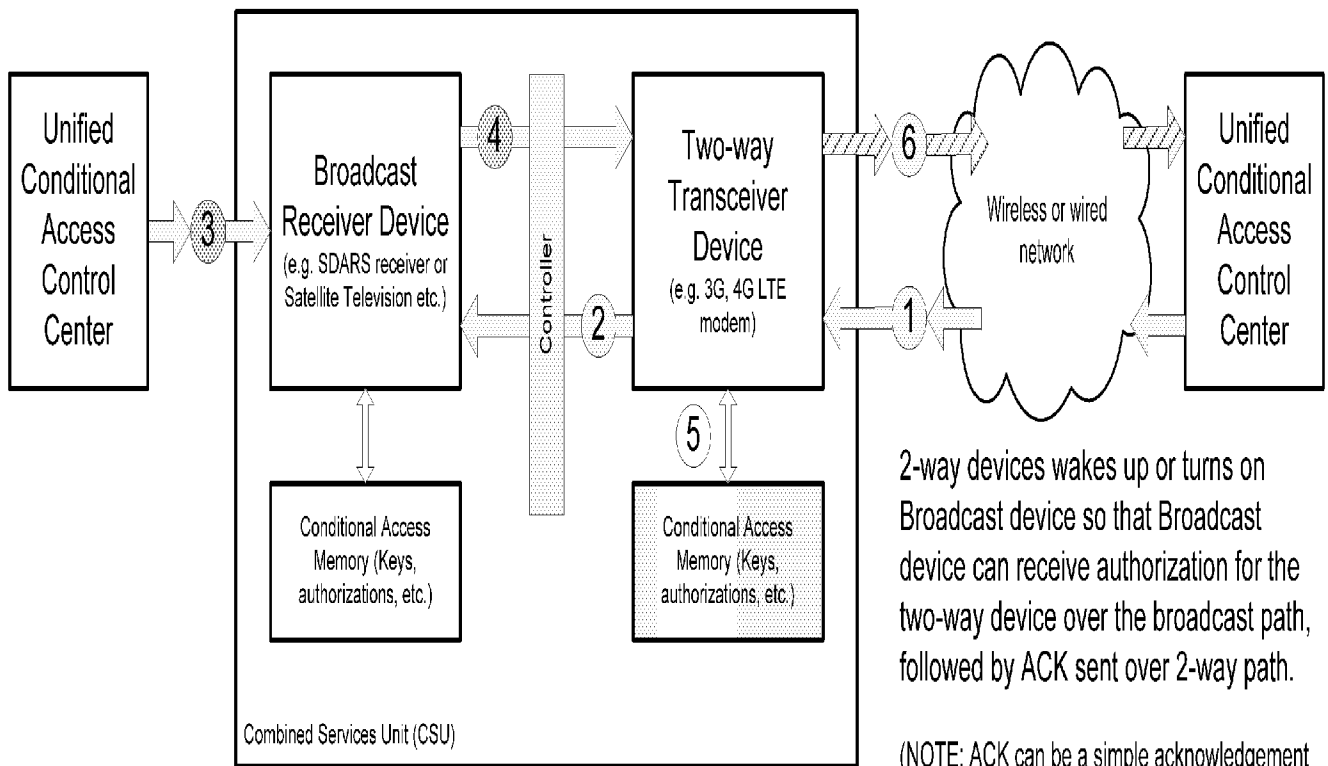


2-way devices wakes up or turns on Broadcast device so that Broadcast device can receive authorization over the broadcast path, followed by ACK sent over 2-way path.

(NOTE: ACK can be a simple acknowledgement of CA state change or can optionally include a hash of the CA State)

FIG. 6

Updating the 2-way Conditional Access information using the 2-way path to wake up the 1-way portion to prepare to receive Conditional Access information using the 1-way path with an acknowledgement (either completion or partial) sent using the transmit path of the 2-way portion of the device.



2-way devices wakes up or turns on Broadcast device so that Broadcast device can receive authorization for the two-way device over the broadcast path, followed by ACK sent over 2-way path.

(NOTE: ACK can be a simple acknowledgement of CA state change or can optionally include a hash of the CA State)

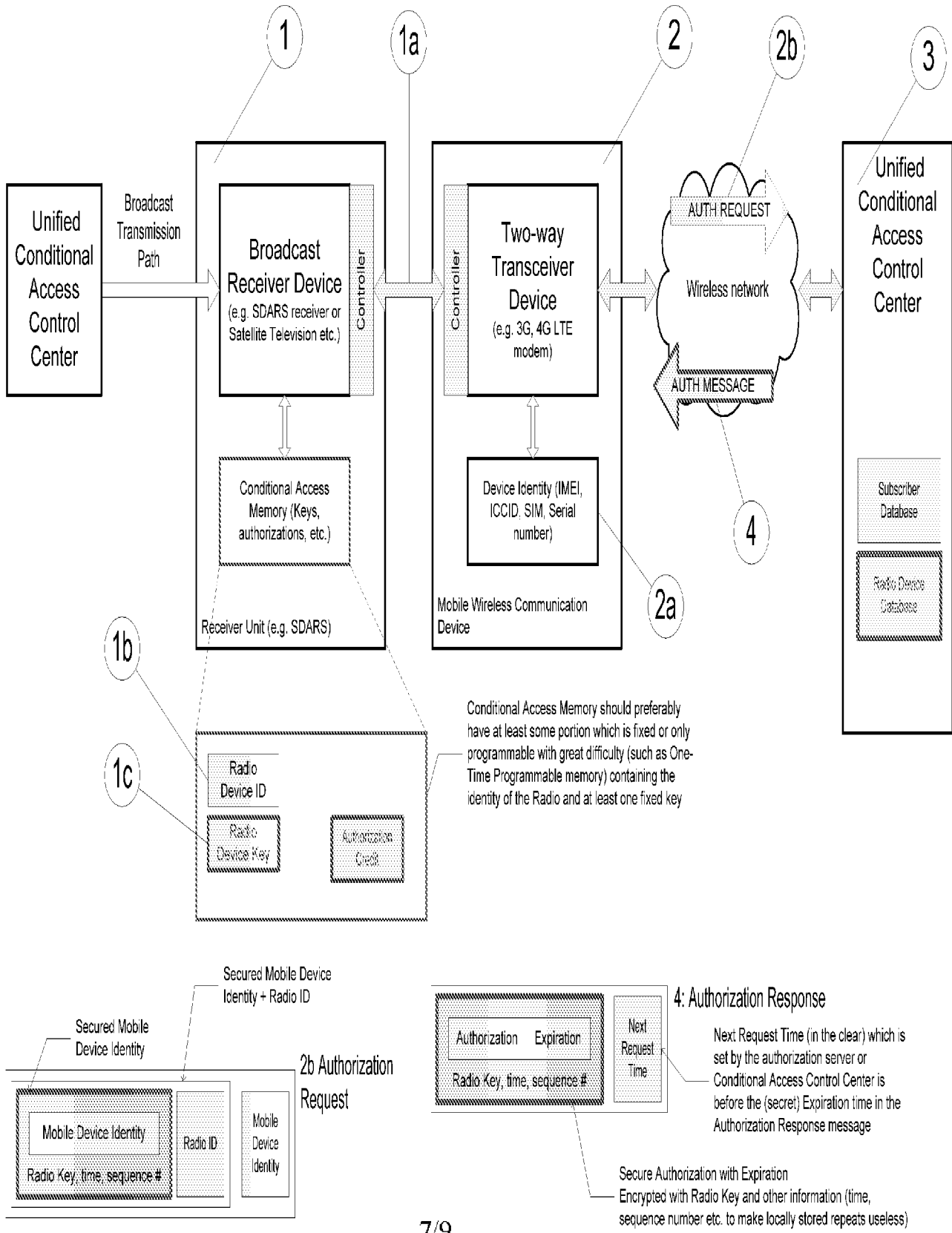


FIG. 8

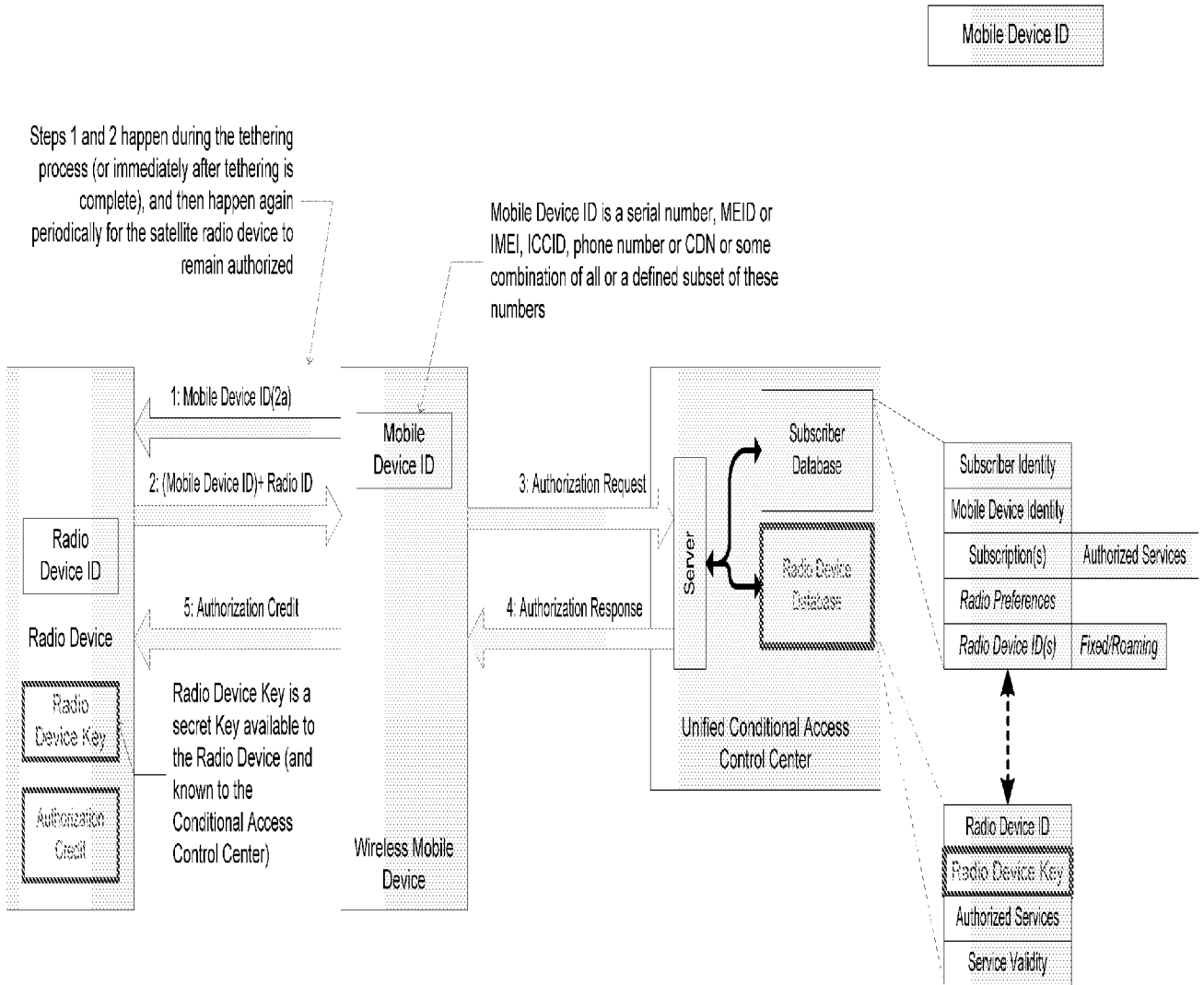
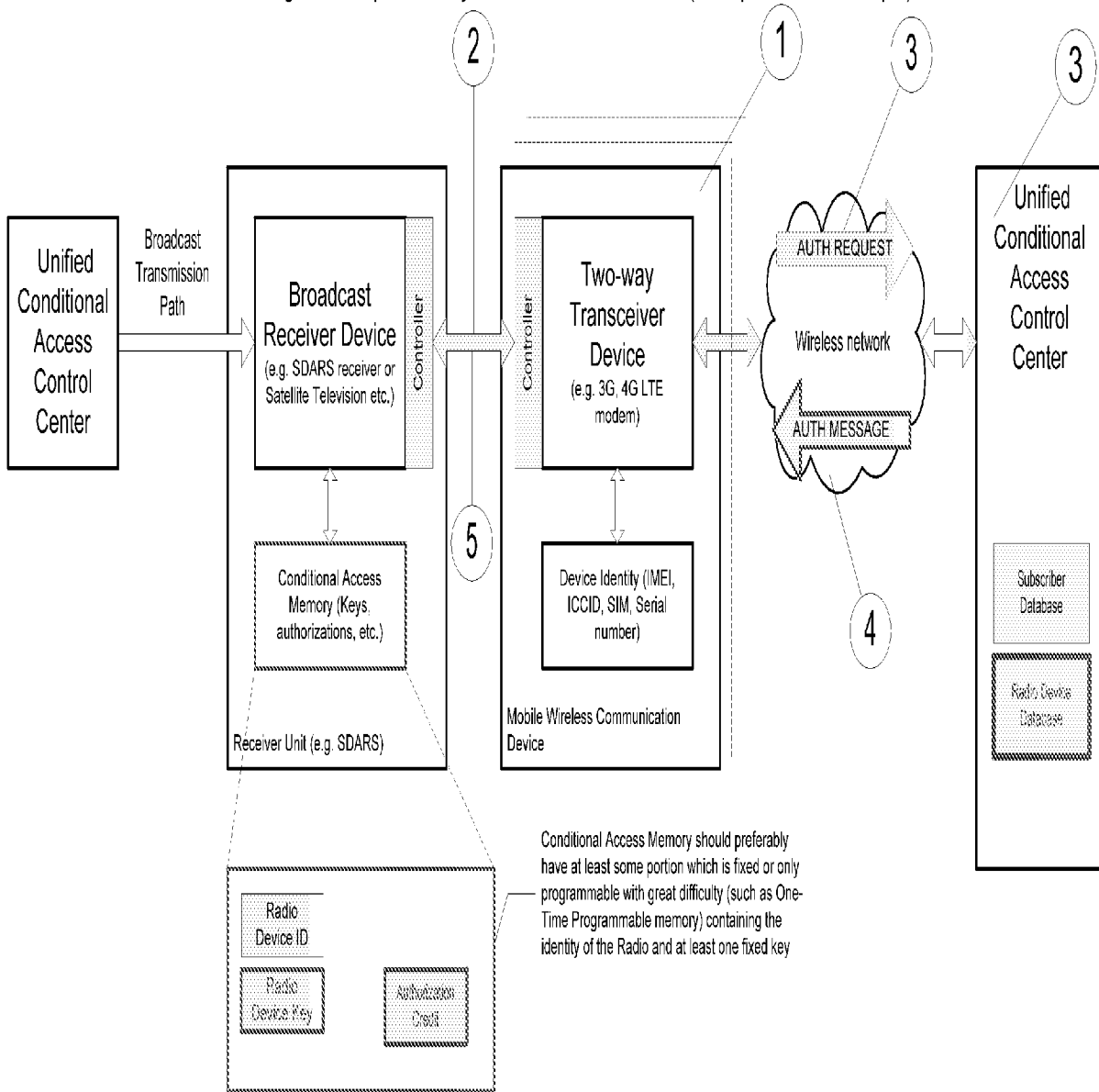
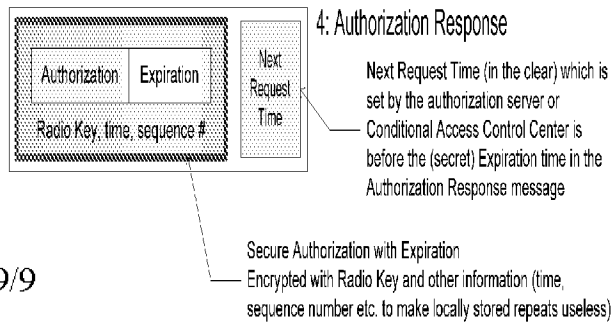
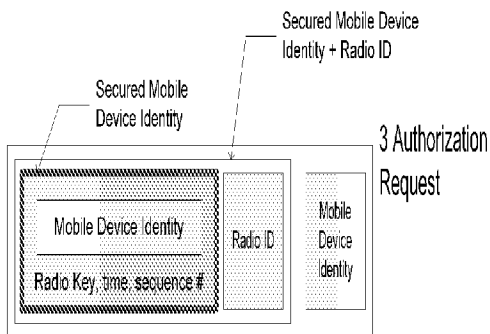


Fig. 9 – Multiple two-way remote transceiver devices (smartphones, for example)



Conditional Access Memory should preferably have at least some portion which is fixed or only programmable with great difficulty (such as One-Time Programmable memory) containing the identity of the Radio and at least one fixed key



**A. CLASSIFICATION OF SUBJECT MATTER****H04W 12/06(2009.01)i, H04W 12/08(2009.01)i, H04W 4/06(2009.01)i, H04W 4/12(2009.01)i**

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

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

H04W 12/06; G06F 15/16; H04N 7/173; H04W 4/02; H04J 3/04; G06F 21/00; H04W 12/08; H04W 4/06; H04W 4/12

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) &amp; Keywords: , ,

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	US 2006-0294250 A1 (CHRISTOPHER J.STONE et al.) 28 December 2006 See abstract, paragraph [0005], figure 2 and claims 1-18.	1,5,7,9,13,16 2-4,6,8,10-12 ,14-15,17-64
A	US 2011-0302624 A1 (XUEMIN CHEN et al.) 08 December 2011 See abstract, figures 3-6 and claims 1-20.	1-64
A	US 2010-0080163 A1 (RAGHURAMAN KRISHNAMOORTHY et al.) 01 April 2010 See abstract, figures 1-57 and claims 1-162.	1-64
A	US 2005-0047448 A1 (KYUNG-EUN LEE et al.) 03 March 2005 See abstract, figure 3 and claims 1-24.	1-64

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

\* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&amp;" document member of the same patent family

Date of the actual completion of the international search

19 November 2014 (19.11.2014)

Date of mailing of the international search report

**20 November 2014 (20.11.2014)**

Name and mailing address of the ISA/KR

International Application Division  
Korean Intellectual Property Office  
189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan City, 302-701,  
Republic of Korea

Facsimile No. +82-42-472-7140

Authorized officer

YOO, Sun Jung

Telephone No. +82-42-481-5775



**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No.

**PCT/US2014/049650**

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006-0294250 A1	28/12/2006	CA 2612024 A1	28/12/2006
		CA 2612024 C	11/09/2012
		US 7987504 B2	26/07/2011
		WO 2006-137976 A2	28/12/2006
		WO 2006-137976 A3	14/05/2009
US 2011-0302624 A1	08/12/2011	US 2011-299410 A1	08/12/2011
		US 2011-299411 A1	08/12/2011
		US 2011-299540 A1	08/12/2011
		US 2011-299541 A1	08/12/2011
		US 2011-299542 A1	08/12/2011
		US 2011-299543 A1	08/12/2011
		US 2011-299544 A1	08/12/2011
		US 2011-299546 A1	08/12/2011
		US 2011-299547 A1	08/12/2011
		US 2011-299548 A1	08/12/2011
		US 2011-299550 A1	08/12/2011
		US 2011-300825 A1	08/12/2011
		US 2011-301963 A1	08/12/2011
		US 2011-302010 A1	08/12/2011
		US 2011-302068 A1	08/12/2011
		US 2011-302077 A1	08/12/2011
		US 2011-302248 A1	08/12/2011
		US 2011-302275 A1	08/12/2011
		US 2011-302276 A1	08/12/2011
		US 2011-302296 A1	08/12/2011
		US 2011-302308 A1	08/12/2011
		US 2011-302313 A1	08/12/2011
		US 2011-302324 A1	08/12/2011
		US 2011-302431 A1	08/12/2011
		US 2011-302442 A1	08/12/2011
		US 2011-302497 A1	08/12/2011
		US 2011-302596 A1	08/12/2011
		US 2011-302610 A1	08/12/2011
		US 2011-302612 A1	08/12/2011
		US 2011-302632 A1	08/12/2011
		US 2011-302634 A1	08/12/2011
		US 2011-302663 A1	08/12/2011
		US 2014-082219 A1	20/03/2014
		US 2014-122211 A1	01/05/2014
		US 2014-219136 A1	07/08/2014
US 8589591 B2	19/11/2013		
US 8638804 B2	28/01/2014		
US 8693484 B2	08/04/2014		
US 8705543 B2	22/04/2014		
US 8707359 B2	22/04/2014		
US 8763141 B2	24/06/2014		
US 8869290 B2	21/10/2014		

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No.

**PCT/US2014/049650**

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010-0080163 A1	01/04/2010	CN 102227923 A	26/10/2011
		CN 103647798 A	19/03/2014
		CN 103647799 A	19/03/2014
		KR 10-1398260 B1	26/05/2014
		KR 10-2011-0086811A	01/08/2011
		KR 10-2012-0112820 A	11/10/2012
		US 2014-223479 A1	07/08/2014
		US 8635645 B2	21/01/2014
		WO 2010-039833 A2	08/04/2010
		WO 2010-039833 A3	01/07/2010
US 2005-0047448 A1	03/03/2005	CN 100563112 C	25/11/2009
		CN 1592126 A	09/03/2005
		CN 1592126 C0	09/03/2005
		EP 1511296 A1	02/03/2005
		JP 03-895741B2	22/03/2007
		JP 2005-073235A	17/03/2005
		KR 10-0547810 B1	31/01/2006
		KR 10-2005-0022936A	09/03/2005