APPARATUS AND METHOD FOR A SECURE BROADCAST SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present Application for Patent claims priority to Provisional Application No. 60/485,791 entitled "Apparatus and Method for a Secure Broadcast System" filed July 8, 2003, and assigned to the assignee hereof and hereby expressly incorporated by reference herein.

BACKGROUND

I. Field of Invention

[0002] The invention generally relates to secure communication systems and more particularly, to access key management for multimedia broadcasting service in a mobile environment.

II. Description of the Related Art

[0003] Wireless communication systems are widely deployed to provide various types of communication such as voice, data, and so on. These systems may be based on code division multiple access (CDMA), time division multiple access (TDMA), or other modulation techniques.

[0004] A system may be designed to support one or more standards such as the "TIA/EIA-95-B Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System" (the IS-95 standard); the "Global System for Mobile" (GSM) communication standard based on TDMA; the "Universal Mobile Telecommunications Service" (UMTS) standard which is a third generation wireless service based on GSM communication standard; the General Packet Radio System (GPRS) communication standard which is an evolutionary step from GSM toward UMTS; the standard offered by a consortium named "3rd Generation Partnership Project" (3GPP) which is embodied in a set of documents including Document Nos. 3G TS 25.211, 3G TS 25.212, 3G TS 25.213, and 3G TS 25.214, 3G TS 25.302 (the W-CDMA standard); the standard offered by a consortium named "3rd Generation Partnership Project 2" (3GPP2) which is embodied in "TR-45.5 Physical Layer Standard for cdma2000 Spread Spectrum Systems" (the IS-2000 standard). Each standard defines

the processing of data for wireless communication between an infrastructure element, such as a base station, and a user end device, such as a mobile device.

[0005] Increasing demand for wireless data transmission and the expansion of services available via wireless communication technology have led to the development of specific data services. In one embodiment, a system may be configured to support multimedia broadcasting services (hereinafter "broadcast service"). Similar to television and/or radio broadcasting, broadcast service may be used for wireless transmission of multimedia content stream from a content provider to user end devices. Here, a content stream can be considered as equivalent to a television channel or radio station. Examples of multimedia content streams include audio and/or video data such as movies, sports events, news and various other programs and/or files. Typically, a service provider indicates the availability of such broadcast service to users. Users desiring broadcast service may receive broadcast service related parameters in overhead messages transmitted by infrastructure elements. When a user desires to receive certain content stream, the user end device reads the overhead messages and learns the appropriate configurations. The user end device then tunes to the channel or frequency containing the content stream, and receives broadcast service.

[0006] There are several possible subscription/revenue models for broadcast service, including free access, controlled access, and partially controlled access. For free access, no subscription is needed by the users to receive the service. Content is broadcasted without encryption such that user end devices of interested users can receive and view the content. The revenue for the service provider can be generated through advertisements that may also be transmitted in the broadcast channel. For example, upcoming movie-clips can be transmitted for which the studios will pay the service provider.

[0007] In controlled access, users are required to subscribe and become authorized to receive the broadcast service by paying a fee. This controlled access can be achieved by encrypting the broadcast service transmission or content with cryptographic access keys such that only subscribed users can decrypt and view the content. Here, the encryption of the broadcast content may be based on symmetric or asymmetric cryptosystems. In symmetric cryptosystems, the same keys are used for encryption/decryption and in asymmetric cryptosystems, different keys are used for encryption/decryption.

[0008] Cryptography is well known to those skilled in art and will not be further described in detail. A hybrid access scheme or partial controlled access provides broadcast service as a subscription-based service that is encrypted with intermittent unencrypted advertisement transmissions. These advertisements may be intended to encourage subscriptions to the encrypted broadcast service.

[0009] For controlled or partially controlled broadcast service, a problem exists in the secure provision of the access key from a content provider to one or more recipients. Therefore, there is a need for a secure way to provision an access key to end user devices. More particularly, the provisioning of the access key needs to conform with existing standards and corresponding infrastructures as well as evolving standards and corresponding infrastructures.

SUMMARY

[0010] Embodiments disclosed herein address the above stated needs by enabling a secure provision of access key to end user devices.

[0011] In one embodiment, a method for secure processing in a device that securely stores a secret key comprises receiving a plurality of challenges from a network; generate a plurality of ciphering keys based on the secret key and the plurality of challenges; and generating an access key based on the plurality of ciphering keys. The method may further comprise using the plurality of challenges and the secret key to generate a plurality of authentication responses; and sending at least one authentication response to the network. Generation of the access key may comprise generating a broadcast access key; and wherein the method further comprises: receiving encrypted broadcast content; and decrypting the broadcast content based on the broadcast access key. Decryption of the content may comprises: generating a temporary decryption key based on each challenge and the broadcast access key; and decrypting the broadcast content using the temporary decryption key.

[0012] In another embodiment, apparatus for secure processing in a device having means for securely storing a secret key comprises means for generating a plurality of ciphering keys based on a plurality of challenges received from a network and the secret key; and means for generating an access key based on the plurality of ciphering keys.

[0013] In still another embodiment, a machine readable medium for use in a device that securely stores a secret key and receives a plurality of challenges from a network is

disclosed. The machine readable medium comprises codes for generating a plurality of ciphering keys based on the plurality of challenges and the secret key; and codes for generating an access key based on the plurality of ciphering keys.

[0014] In the above embodiments, a 128 bit subscriber authentication key may be stored as the secret key in a subscriber identity module of a mobile phone using Global System for Mobile communication standard. A 128 bit subscriber authentication key may also be stored as the secret key in a universal subscriber identity module of a mobile phone using Universal Mobile Telecommunications System standard. Moreover, 64 bit ciphering keys may be generated and a 128 bit broadcast access key may be generated using two ciphering keys.

[0015] In a further embodiment, an apparatus for use in a mobile phone comprising: an integrated circuit card (ICC) configured to securely store a secret key and to generate a plurality of ciphering key based on the secret key and a plurality of challenges received from a network; and a processor coupled to the ICC and configured to generate an access key based on the plurality of ciphering keys. The ICC may be a subscriber identity module (SIM) of a mobile phone using Global System for Mobile communication standard. SIM may store a 128 bit subscriber authentication key as the secret key and generate 64-bit ciphering keys. The ICC may also be a universal subscriber identity module (USIM) of a mobile phone using Universal Mobile Telecommunications System standard. USIM may store a 128 bit subscriber authentication key as the secret key and generate 64-bit ciphering keys in a mode that is backward compatible with the SIM. The processor may generate a 128 bit broadcast access key using two ciphering keys.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016] Various embodiments will be described in detail with reference to the following drawings in which like reference numerals refer to like elements, wherein:

[0017] Figure 1 is an example wireless communication capable of supporting broadcast service;

[0018] Figure 2 shows a simplified network for implementing MBMS;

[0019] Figure 3 shows a terminal capable of subscribing to MBMS to receive multimedia content;

[0020] Figure 4 a simplified example of a GSM system;

[0021] Figure 5 is an example system with a network that performs authentication and a terminal for broadcast service; and

[0022] Figure 6 shows a method for secure processing in a device that securely stores a secret key.

DETAILED DESCRIPTION

[0023] In the following description, specific details are given to provide a thorough understanding of the embodiments. However, it will be understood by one of ordinary skill in the art that the embodiments may be practiced without these specific detail. For example, circuits may be shown in block diagrams in order not to obscure the embodiments in unnecessary detail. In other instances, well-known circuits, structures and techniques may be shown in detail in order not to obscure the embodiments.

[0024] Also, it is noted that the embodiments may be described as a process which is depicted as a flowchart, a flow diagram, a structure diagram, or a block diagram. Although a flowchart may describe the operations as a sequential process, many of the operations can be performed in parallel or concurrently. In addition, the order of the operations may be re-arranged. A process is terminated when its operations are completed. A process may correspond to a method, a function, a procedure, a subroutine, a subprogram, etc. When a process corresponds to a function, its termination corresponds to a return of the function to the calling function or the main function.

[0025] Moreover, as disclosed herein, a storage medium may represent one or more devices for storing data, including read only memory (ROM), random access memory (RAM), magnetic disk storage mediums, optical storage mediums, flash memory

devices and/or other machine readable mediums for storing information. The term "machine readable medium" includes, but is not limited to portable or fixed storage devices, optical storage devices, wireless channels and various other mediums capable of storing, containing or carrying instruction(s) and/or data.

[0026] Figure 1 shows an example of a wireless communications network 100 capable of supporting broadcast service. Network 100 may comprise one or more communication systems supporting different standards. More particularly, network 100 comprises a plurality of service areas 102A - 102G, each of which is serviced by a corresponding infrastructure element 104A - 104G, respectively. Infrastructure elements 104A – 104G communicate with user end devices (hereinafter "terminal") 106A-106J that are within service areas 102A-102G of infrastructure elements 104A-104G, respectively. Depending on the type of communication system, infrastructure elements 104A-104G may include base stations, base transceiver station, gateways or other devices that communicates with terminals106A-106J. Terminals 106A –106J may be, but is not limited to, a mobile (including cellular and personal communications service) phone, wired phone, a wireless handset, a personal data assistant (PDA), various computer devices (including laptop and desktop) or other data transceiver. As shown in Figure 1, terminals 106A – 106J can be hand-held, mobile, portable as in vehicle mounted (including cars, trucks, boats, trains, and planes) or fixed (stationary).

[0027] In one embodiment, network 100 supports a broadcast service referred to as Multimedia Broadcast/Multicast Service (MBMS), or sometimes referred to as Broadcast/Multimedia Service (BCMCS). Generally, MBMS is a packet data service based on the Internet Protocol (IP). A service provider may indicate the availability of such MBMS to users. The users desiring MBMS may receive the service and discover the broadcast service schedule through broadcasts such as advertisements, Short Message System (SMS), and Wireless Application Protocol (WAP). Infrastructure elements transmit MBMS related parameters in overhead messages. When a user desires to receive a broadcast session, a terminal 106 reads the overhead messages and learns the appropriate configurations. Terminal 106 then tunes to the frequency containing the MBMS channel, and receives the broadcast service content.

[0028] Figure 2 shows a simplified network 200 for implementing MBMS. In network 200, video and/or audio information is provided to Packetized Data Service Network (PDSN) 230 by a Content Source (CS) 210. The video and audio information may be

from televised programs or radio transmissions. The information is provided as packetized data, such as in IP packets. PDSN 220 processes the IP packets for distribution within an Access Network (AN). As illustrated, AN is defined as the portions of network 200 including a infrastructure element 240 in communication with a plurality of terminals 250.

[0029] For MBMS, CS 210 provides unencrypted content. Infrastructure element 240 receives the stream of information from PDSN 230 and provides the information on a designated channel to subscriber terminals within network 200. To control access, the content from CS 210 is encrypted by a content encryptor (not shown) using an encryption key before being provided to PDSN 220. While content encryptor may be implemented together or separately from CS 210, content encryptor and CS 210 will hereinafter be referred to as a content provider. The subscribed users are provided with the decryption key so that the IP packets can be decrypted.

[0030] More particularly, Figure 3 shows a terminal 300 capable of subscribing to MBMS to receive multimedia content. Terminal 300 comprises an antenna 310 coupled to a receive circuitry 320. Terminal 300 receives transmissions from a content provider (not shown) through an infrastructure element (not shown). Terminal 300 includes a Mobile Equipment 340 and a Universal Integrated Circuit Card (UICC) 330 coupled to receive circuitry 320. It is to be noted that in some terminals, UICC 330 and ME 340 may be implemented together in one secure processing unit. Also, although the embodiment will be described using UICC, other integrated circuits and/r secure processing units, such as User Identification Module (UIM), Subscriber Identity Module (SIM) or universal SIM, may be implemented in a terminal.

[0031] Generally, UICC 330 applies verification procedures for security of the MBMS transmission and provides various keys to ME 340. ME 340 performs substantial processing, including, but not limited to, decryption of MBMS content streams using the keys provided by UICC 330. UICC 330 is trusted to securely store and process secret information (such as encryption keys) that should remain secret for a long time. As UICC 330 is a secure unit, the secrets stored therein do not necessarily require the system to change the secret information often. UICC 330 may include a processing unit referred to as a Secure UICC Processing Unit (SUPU) 332 and a secure memory storage unit referred to as a Secure UICC Memory Unit (SUMU) 334. Within UICC 330, SUMU 334 stores secret information in a way that discourages unauthorized access to

the information. If the secret information is obtained from UICC 330, the access will require significantly large amount of resources. Also within UICC 330, SUPU 332 performs computations on values that may be external to and/or internal to UICC 330. The results of the computation may be stored in SUMU 334 or passed to ME 340.

[0032] In one embodiment, UICC 330 is a stationary unit or integrated within terminal 300. Note that UICC 330 may also include non-secure memory and processing (not shown) for storing information including telephone numbers, e-mail address information, web page or URL address information, and/or scheduling functions, etc. Alternative embodiments may provide a removable and/or reprogrammable UICC. Typically, SUPU 332 does not have significant processing power for functions beyond security and key procedures, such as to allow encryption of the broadcast content of MBMS. However, alternative embodiments may implement a UICC having stronger processing power.

[0033] While UICC 330 is a secure unit, data in ME 340 may be accessed by a non-subscriber and is said to be insecure. Any information passed to ME 340 or processed by the ME 340 remains securely secret for only a short amount of time. It is therefore desired that any secret information, such as key(s), shared with ME 340 be changed often.

[0034] More particularly, MBMS content is encrypted using a unique and frequently changing temporary encryption keys referred to as short-term key (SK). In order to decrypt the broadcast content at a particular time, ME 340 must know the current SK. The SK is used to decrypt the broadcast content for a short-amount of time such that SK can be assumed to have some amount of intrinsic monetary value for a user. For example, this intrinsic monetary value may be a portion of the registration costs. Here, different content types may have different intrinsic monetary value. Assuming that the cost of a non-subscriber obtaining SK from ME 340 of a subscriber exceeds the intrinsic monetary value of SK, the cost of obtaining SK illegitimately exceeds the reward and there is no benefit. Consequently, there is no need to protect SK in ME 340. However, if a broadcast has an intrinsic value greater than the cost of illegitimately obtaining this secret key, there is a benefit to the non-subscriber in obtaining such a key from ME 340. Hence, ME 340 ideally will not store secrets with a lifetime longer than that of an SK.

[0035] In addition, the channels used by a content provider (not shown) for transmission of data are considered insecure. Therefore, SK is not transmitted over the

air. It is derived either by UICC 330 or ME 340 from an access key called a broadcast access key (BAK) and SK information (SKI) broadcasted along with the encrypted content. BAK may be used for a certain amount of time, for example one day, one week or a month, and is updated. Within each period for updating the BAK, a shorter interval is provided during which SK is changed. The content provider may use a cryptographic function to determine two values SK and SKI such that SK can be determined from BAK and SKI. In one embodiment, SKI may contain SK that is encrypted using BAK as the key. Alternatively, SK may be a result of applying a cryptographic hash function to the concatenation of SKI and BAK. Here, SKI may be some random value.

[0036] To obtain access to MBMS, a user registers and subscribes to the service. In one embodiment of the registration process, a content provider and UICC 330 agree on a Registration Key or root key (RK) that serves as a security association between the user and the content provider. The registration may occur when a user subscribes to a broadcast channel offered by the content provider or may occur prior to subscription. A single content provider may offer multiple broadcast channels. The content provider may choose to associate users with the same RK for all channels or require users to register for each channel and associate the same user with different RKs on different channels. Multiple content providers may choose to use the same registration keys or require the user to register and obtain a different RK.

[0037] If possible, RK is then kept as a secret in UICC 330. RK is unique to a given UICC, i.e., each user is assigned a different RK. However, if a user has multiple UICCs, then these UICCs may be configured to share the same RK depending on the policies of the content provider. The content provider may then send UICC 330 further secret information such as BAK encrypted with RK. UICC 330 is able to recover the value of the original BAK from the encrypted BAK using the RK. Since ME 340 is not a secret unit, UICC 330 does not provide BAK to ME 340.

[0038] The content provider also broadcasts SKI that is combined with the BAK in UICC 330 to derive SK. UICC 330 then passes SK to ME 340 and ME 340 uses the SK to decrypt encrypted broadcast transmissions received from a content provider. In this way, the content provider can efficiently distribute new values of SK to subscribed users.

[0039] As described, controlled access may be achieved by provisioning an agreed upon RK in SUMU 334 of UICC 330. However, in the existing infrastructure of some systems, an appropriate value of RK cannot be kept in a secure unit such as UICC 330, because of the cost and/or inconvenience of replacing existing UICCs, SIMs, UIMs or other Integrated Circuit Cards.

[0040] For example, in GSM systems, a Subscriber Identity Module (SIM) is the secure unit and contains subscriber identifying data about a user that can be used to gain access to a network. For purposes of explanation, Figure 4 shows a simplified example of a GSM system 400 for authenticating a subscriber to allow access to a network. System 400 comprises a Home Location Register (HLR) 410, a Visitor Location Register (VLR) 420 and a terminal such as a mobile device 430. Note that system 400 comprise of additional elements, but GSM systems are well known to those skilled in the art and will not be described in detail.

[0041] HLR 410 is a subscriber database for a mobile system. HLR 410 is maintained by a terminal's home carrier and contains important user information for billing and for authentication to a network. VLR 420 is also a database and contains temporary user information, such as the current location of a terminal, to manage requests from subscribers who are out of the area covered by their home system. When a user initiates a call and the terminal of the user is our of the home area, VLR 420 communicates with HLR 410 to obtain information required to process a call, including information required to authenticate the subscriber.

[0042] Terminal 430 comprises a SIM module 432 that securely contains a subscriber authentication key (K) used to authenticate a subscriber. Here, a challenge-handshake authentication protocol known as Authenticated Key Agreement (AKA) is typically used for GSM authentication. In AKA, a network sends a challenge message to a subscriber terminal, which responds with a value obtained using a one-way hash function. Here, the challenge message may be a random value. The network checks the response by comparing it with its own expected hash value. If the values match, the authentication is acknowledged. While generating this response, a key that can be used to secure subsequent communications is also generated.

[0043] More particularly, in GSM system, VLR 420 requests authentication parameters from HLR 410. HLR 410 sends to VLR a 128 bit random number RAND, a signed response (RES) and a ciphering key (Kc). The RES and Kc are both generated from the

subscriber authentication key K and RAND, by using different algorithms. Using this Authentication Triplet (RAND, RES, Kc), a challenge message is issued by sending the random number RAND to Terminal 430. The received RAND is passed to SIM 432 which generates RES and Kc using RAND and K. The generated RES is returned to VLR 420 which checks that the two values of RES match. If they match, the subscriber is authenticated and both terminal and network begin to encrypt/decrypt using Kc.

[0044] While GSM SIM securely contains a subscriber authentication key (K) used to authenticate a subscriber, it does not allow provisioning of an additional key such as RK. Namely, existing GSM SIMs cannot be changed. Therefore, one way to deliver BAK for broadcast service may be to use Kc rather than RK to encrypt BAK. A content provider would send a message containing RAND and BAK encrypted with Kc. A terminal receives the message and forwards the RAND to the SIM as if it was a normal GSM authentication. Accordingly, RES and Kc is generated by SIM using RAND and K. Here, the RES generated by SIM may be discarded. This protects against an attacker that might send the same RAND and record the returned RES for unauthorized access. The Kc may be used to decrypt the encrypted BAK.

[0045] However, Kc is typically a 64 bit key while some broadcast service such as MBMS is designed to give 128 bit security. Therefore, it is necessary to use a key as longer than 64 bits to encrypt BAK. As a result, a plurality of triplets is used for encryption of BAK.

[0046] Figure 5 shows an example system 500 with a network 510 that performs authentication and terminal 520 for broadcast service. Network 510 comprises one or more content providers and other infrastructure elements necessary for broadcast service. Terminal 520 comprises ICC 522 coupled to a processor 524. In GSM system, network 510 may comprise a VLR and HLR, and ICC 522 would be a SIM module as described in Figure 4. Generally, network 510 sends challenge messages for performing authentication. The challenge messages are used by terminal 520 to generate BAK for controlled access. Namely, ICC 522 of terminal 510 securely stores a secret key used in the generation of BAK. The operation of system 500 will be explained with reference to Figure 6 below.

[0047] Figure 6 shows a method 600 for secure processing in a device such as terminal 620, that securely stores a secret key such as a subscriber authentication key in a secure unit such as ICC 622. In method 600, the device receives a plurality of challenges from

a network (610). The plurality of challenges may be in one message or a plurality of messages. A plurality of ciphering keys are generated based on the secret key and the plurality of challenges (620). The access key is then generated based on the plurality of ciphering keys (630). In system 500, for example, ICC 522 is configured to generate the ciphering keys as the secret key should be kept within ICC 522. Processor 524 is configured to generate the access key based on the ciphering keys.

[0048] The access key is generated using a plurality of ciphering keys because the access key is typically longer than a ciphering key. For example, in GSM for MBMS, the ciphering key is 64 bits while the access key is 128 bits. In such case, the access key can be generated using two ciphering keys. Any known technique may be used to generate an access key from the plurality of ciphering keys. In one embodiment, the access key is generated by concatenating the plurality of ciphering keys. In an alternative embodiment, the access key is generated using a hash function on the plurality of ciphering keys. The hash function may comprise SHA-1 to mix the plurality of ciphering keys.

[0049] For authentication, method 600 may further comprise using the plurality of challenge messages and the secret key to generate a plurality of authentication responses as described with reference to Figure 4. Thereafter, at least one of the authentication response is returned to the network using a transmitter (not shown) implemented in terminal 520 and any authentication responses not sent to the network may be discarded.

[0050] Therefore, after generating the access key, method 600 may further comprise receiving encrypted broadcast content and decrypting the broadcast content based on the access key. For example in MBMS, the access key would be the BAK and SKI would be used to generate SK. In such case, method 600 may further comprise generating a temporary encryption/decryption key such as SK based on each challenge message and current BAK. The current SK can then be used to decrypt and view/process encrypted content.

[0051] Accordingly, embodiments described allow a secure provisioning of an access key for broadcast service. It is to be noted here that although the embodiments have been described with reference to MBMS, the scope of the invention applies to broadcast services other than MBMS and to various systems requiring controlled access. Similarly, the access key may be shorter or longer than 128 bits. Moreover, the embodiments may apply to systems other than GSM system. For example, UMTS

systems have a USIM which is analogous to GSM SIM and has a backward compatibility mode allowing it to act as a GSM SIM.

[0052] Furthermore, embodiments may be implemented by hardware, software, firmware, middleware, microcode, or any combination thereof. When implemented in software, firmware, middleware or microcode, the program code or code segments to perform the necessary tasks may be stored in a machine readable medium (not shown). A processor may perform the necessary tasks. A code segment may represent a procedure, a function, a subprogram, a program, a routine, a subroutine, a module, a software package, a class, or any combination of instructions, data structures, or program statements. A code segment may be coupled to another code segment or a hardware circuit by passing and/or receiving information, data, arguments, parameters, or memory contents. Information, arguments, parameters, data, etc. may be passed, forwarded, or transmitted via any suitable means including memory sharing, message passing, token passing, network transmission, etc. Also, the machine readable medium may be implemented in an article of manufacture for use in a computer system and may have machine readable code means embodied therein

[0053] Finally, it should be noted that the foregoing embodiments are merely examples and are not to be construed as limiting the invention. The description of the embodiments is intended to be illustrative, and not to limit the scope of the claims. As such, the present teachings can be readily applied to other types of apparatuses and many alternatives, modifications, and variations will be apparent to those skilled in the art.

CLAIMS

What is claimed is:

1. A method for secure processing in a device that securely stores a secret key, the method comprising:

receiving a plurality of challenges from a network;

generating a plurality of ciphering keys based on the secret key and the plurality of challenges; and

generating an access key based on the plurality of ciphering keys.

2. The method of claim 1, further comprising:

using the plurality of challenges and the secret key to generate a plurality of authentication responses; and

sending at least one authentication response to the network.

3. The method of claim 2, further comprising:

discarding any authentication responses not sent to the network.

4. The method as in any one of the preceding claims, wherein receiving a plurality of challenges comprises:

receiving a plurality of random values.

5. The method as in any one of the preceding claims, wherein the access key is longer than a ciphering key.

6. The method of claim 5, wherein generating the access key comprises:

concatenating the plurality of ciphering keys.

7. The method of claim 5, wherein generating the access key comprises:

using a hash function on the plurality of ciphering keys.

8. The method of claim 7, wherein the hash function comprises SHA-1 to mix the plurality of ciphering keys.

9. The method as in any one of the preceding claims, wherein storing the secret key comprises:

storing a 128 bit subscriber authentication key as the secret key in a subscriber identity module of a mobile phone using Global System for Mobile communication standard.

10. The method of claim 9, wherein generating the plurality of ciphering keys comprises generating 64-bit ciphering keys; and

wherein generating the access key comprises generating a 128 bit broadcast access key using two ciphering keys.

11. The method as in claim 1 or any one of claims 2-8 as dependent thereon, wherein storing the secret key comprises:

storing a 128 bit subscriber authentication key as the secret key in a universal subscriber identity module of a mobile phone using Universal Mobile Telecommunications System standard.

12. The method of claim 11, wherein generating the plurality of ciphering keys comprises generating 64-bit ciphering keys; and

wherein generating the access key comprises generating a 128 bit broadcast access key using two ciphering keys.

13. The method as in any one of the preceding claims, wherein generating the access key comprises generating a broadcast access key; and wherein the method further comprises:

receiving encrypted broadcast content; and

decrypting the broadcast content based on the broadcast access key.

14. The method of claim 13, wherein the decrypting the content comprises:

generating a temporary decryption key based on each challenge and the broadcast access key; and

decrypting the broadcast content using the temporary decryption key.

15. Apparatus for use in a mobile phone comprising:

an integrated circuit card (ICC) configured to securely store a secret key and to generate a plurality of ciphering key based on the secret key and a plurality of challenges received from a network; and

a processor coupled to the ICC and configured to generate an access key based on the plurality of ciphering keys.

16. The apparatus of claim 15, further comprising:

a transmitter coupled to the ICC; wherein the ICC uses the plurality of challenges and the secret key to generate a plurality of authentication responses; and wherein the transmitter is configured to send at least one authentication response to the network.

17. The apparatus as in claim 15 or claim 16 as dependent thereon, wherein the challenge comprises a random value.

18. The apparatus as in claim 15 or any one of claims 16-17 as dependent thereon, wherein the ICC is a subscriber identity module (SIM) of a mobile phone using Global System for Mobile communication standard.

19. The apparatus of claim 18, wherein the SIM stores a 128 bit subscriber authentication key as the secret key and generates 64-bit ciphering keys; and wherein the processor generates a 128 bit broadcast access key using two ciphering keys.

20. The apparatus as in claim 15 or any one of claims 16-17 as dependent thereon, wherein the ICC is a universal subscriber identity module (USIM) of a mobile phone using Universal Mobile Telecommunications System standard.

21. The apparatus of claim 20, wherein the USIM stores a 128 bit subscriber authentication key as the secret key and generates 64-bit ciphering keys; and wherein the processor generates a 128 bit broadcast access key using two ciphering keys.

22. The apparatus as in claim 15 or any one of claims 16-21 as dependent thereon, wherein the receiver receives encrypted broadcast content; and wherein the processor generates a broadcast access key to decrypt the broadcast content.

23. Apparatus for secure processing in a device having means for securely storing a secret key, the apparatus comprising:

means for generating a plurality of ciphering keys based on a plurality of challenges received from a network and the secret key; and

means for generating an access key based on the plurality of ciphering keys.

24. The apparatus of claim 23, further comprising:

means for using the plurality of challenges and the secret key to generate a plurality of authentication responses; and

means for sending at least one authentication response to the network.

25. The apparatus of claim 24, further comprising:

means for discarding any authentication responses not sent to the network.

26. The apparatus as in claim 23 or any one of claims 24-25 as dependent thereon, wherein the means for generating the access key comprises:

means for concatenating the plurality of ciphering keys.

27. The apparatus as in claim 23 or any one of claims 24-25 as dependent thereon, wherein the means for generating the access key comprises:

means for using a hash function on the plurality of ciphering keys.

28. The apparatus as in claim 23 or any one of claims 24-27 as dependent thereon, wherein the means for generating the access key generates a broadcast access key; and wherein the apparatus further comprises:

means for receiving encrypted broadcast content; and

means for decrypting the broadcast content based on the broadcast access key.

29. An article of manufacture for use in a computer system embodying a system that securely stores a secret key and receives a plurality of challenges from a network, said article of manufacture comprising a machine readable medium having machine readable code means embodied in said medium comprising:

machine readable code means embodied in said machine readable medium for generating a plurality of ciphering keys based on the plurality of challenges and the secret key; and

machine readable code means embodied in said machine readable medium for generating an access key based on the plurality of ciphering keys.

30. The article of manufacture of claim 29, further comprising:

machine readable code means embodied in said machine readable medium for using the plurality of challenges and the secret key to generate a plurality of authentication responses; and

machine readable code means embodied in said machine readable medium for sending at least one authentication response to the network.

31 . The article of manufacture of claim 30, further comprising:

machine readable code means embodied in said machine readable medium for discarding any authentication responses not sent to the network.

32. The article of manufacture of claim 29, wherein the machine readable code means for generating the access key comprises:

machine readable code means embodied in said machine readable medium for concatenating the plurality of ciphering keys.

33. The article of manufacture of claim 29, wherein the machine readable code means for generating the access key comprises:

machine readable code means embodied in said machine readable medium for using a hash function on the plurality of ciphering keys.

34. The article of manufacture of claim 29, wherein the system receives encrypted broadcast content, wherein the machine readable code means for generating the access

key generates a broadcast access key; and wherein the article of manufacture further comprises:

machine readable code means embodied in said machine readable medium for decrypting the broadcast content based on the broadcast access key.