QUALCOMM
ENGINEERING
SERVICES
GROUP

Security Provisions in CDMA2000 Networks

White Paper

November 2011

80-W3633-1 Rev A

Notice

Each User acknowledges that CDG does not review the disclosures or contributions of any CDG member nor does CDG verify the status of the ownership of any of the intellectual property rights associated with any such disclosures or contributions. Accordingly, each User should consider all disclosures and contributions as being made solely on an as-is basis. If any User makes any use of any disclosure or contribution, then such use is at such User's sole risk. Each User agrees that CDG shall not be liable to any person or entity (including any User) arising out of any use of any disclosure or contribution, including any liability arising out of infringement of intellectual property rights.

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, CA 92121-1714
U.S.A.

Security Provisions in CDMA2000 Networks

White Paper

80-W3633-1 Rev A

December 7, 2011

Author: Naidu Mullaguru (mnaidu@qualcomm.com)

Contents

1 Introduction **4**

2 Security Provisions in CDMA2000 1X Networks **5**

2.1 Authentication procedures in CDMA2000 1X 5
2.1.1 CAVE based Authentication procedures 5
2.1.2 AKA based Authentication procedures 13
2.2 Encryption procedures in CDMA2000 1X 17
2.2.1 CAVE based Encryption procedures 17
2.2.2 AKA based Encryption procedures 19
2.3 Security measures in 1X Packet data networks 20

3 Security Provisions in 1xEV-DO Networks **22**

3.1 Session Key exchange through DH Protocol 23
3.2 Authentication procedures in 1xEV-DO 24
3.2.1 RAN Access Authentication procedures 25
3.2.2 IS 856 Air Interface Authentication procedures 27
3.2.3 Service/Subscription Authentication procedures 27
3.3 Encryption procedures in 1xEV-DO Systems 28

4 Developments in C2K Security provisions **30**

4.1 Femto cell network Security measures 30
4.1.1 FAP Authentication and Authorization 31
4.2 Security developments for M2M Communications 32
4.2.1 M2M Device Security measures 33

5 Conclusions & Recommendations **34**

5.1 Authentication recommendations for 1X 34
5.2 Authentication recommendations for 1xEV-DO 35
5.3 Conclusions 35

1 Introduction

Since the birth of the cellular industry, security has been a major concern for both service providers and subscribers. Service providers are primarily concerned with security to prevent fraudulent operations such as cloning or subscription fraud, while subscribers are mainly concerned with privacy issues. The security levels in today's wireless networks approach those on the wired side, but the security protocols continue to be challenged. With the advent of digital technology platform, operators with mobile wireless technologies such as UMTS and CDMA2000 were able to enhance their network security by using improved authentication and encryption algorithms. New security enhancements for CDMA2000 networks (Release C onwards), in the form of new algorithms such as a). Authentication and Key Agreement (AKA) for authentication b). Secure Hashing Algorithm-1 (SHA-1) for hashing and integrity and c). Advanced Encryption Standard (AES) algorithm for message encryption, are being introduced.

CDMA2000 technology is inherently more secure compared to other digital air interface technologies, provided appropriate security measures are implemented by the operators. For example if authentication (a procedure to confirm the identity of the mobile to the network and vice versa) is not implemented properly it is possible to clone a CDMA2000 device. Although CDMA standards were designed with authentication procedures, some operators are not activating full security features because of provisioning procedures required for A-key for authentication and the additional A-key management is not in place. In some cases the infrastructure or the handset vendors have not implemented them. While an authentication procedure is a strong deterrent to cloning fraud, additional security procedures such as SSD updates are also required to be implemented and that can lead to additional signaling load on the network.

This white paper specifically focuses on the security aspects for both CDMA2000 1X and CDMA2000 1xEV-DO (HRPD) systems. Basically the major security aspects that are being discussed in the document are mainly related to authentication and encryption procedures. By the way, the authorization of the device/subscription is not part of this document. In addition to the basic security procedures discussion, also provided information on the special security measures taken in the CDMA2000 systems with respect to the Femto networks as well as CDMA2000 based machine-to-machine communications. The information presented herein should be useful for any operator/service provider interested in implementing or updating the security provisions in their CDMA2000 network.

2 Security Provisions in CDMA2000 1X Networks

Authentication and privacy concerns are the two drivers of wireless network security. Subscribers are more concerned with the privacy issues, while the service providers, because of the huge loss potential, are much more concerned with the authentication security. Authentication is the process by which information is exchanged between the device and the base station to validate that the identity used for communication is legitimate and is generally based on a challenge response mechanism.

2.1 Authentication procedures in CDMA2000 1X

According to standards, in CDMA2000 1X networks, the authentication can be performed at times when the device does registration (when the device does an autonomous registration), call origination, call termination, sending an SMS data burst message, carrying out an SSD update (upon network's request) etc. There are two types of authentication procedures in 1X networks and they are:

1. Cellular Authentication and Voice Encryption (CAVE) algorithm based authentication used by legacy CDMA2000 1X networks.
2. Authentication and Key Agreement (AKA) algorithm based authentication used by both CDMA2000 1X and 1xEV-DO networks.

2.1.1 CAVE based Authentication procedures

In the context of CAVE, the term authentication refers to the mechanism for network validation of device authenticity and clone detection. In the context of AKA, the authentication mechanism is bilateral and supports both network validation of device authenticity and device validation of the network authenticity. From the standards side, TIA-945 (X.S0006-0) specifies MAP support of AKA alternative to CAVE-based authentication. The CAVE-based authentication continues to be deployed and will likely continue to be the most prevalent form of authentication for few more years while the industry migrates to AKA. During this migration, interoperability will necessitate that AKA deployment be done in conjunction with support for CAVE rather than as a complete replacement.

The process of CAVE based authentication involves providing specific inputs into an algorithm to calculate an authentication result. By comparing the result calculated by the handset with the

result calculated by a network entity, such as the Authentication Center (AC), it is possible to immediately detect the presence of a "clone" with no noticeable impact to legitimate subscribers. The essential input for these authentication operations is the A-Key, which is known only to the Authentication Center and the handset. The A-Key is the most protected element of the system and is never broadcast or displayed. The A-Key, the ESN/Pseudo-ESN (in case of the device being identified by MEID), and a random number are used as inputs to the CAVE algorithm that produces a result called Shared Secret Data (SSD). A successful identity of the device is established only if device and network authentication processes yield identical sets of SSD.

2.1.1.1 A-Key

The A-Key is a secret, 64-bit pattern stored only in the device and the AC's database. This secret A-Key may be programmed into the handset when it is manufactured or generated by the AC and then programmed into the handset through "A-Key updating procedure" automatically, without any manual intervention and over the air. The A-Key is the most protected or secure element in the authentication system and is never transmitted over the air interface or in the TCAP messages (signaling network). The AC application includes a subsystem called AC Security that has been designed to provide optimum security of the A-Key and other sensitive data. Once the A-Key is generated, it is used along with ESN/pESN and a random number (RANDSSD) as input to the CAVE algorithm. The result of this execution of CAVE is called Shared Secret Data (SSD). A part of the SSD is then used as a CAVE input to perform subsequent authentication attempts, adding an additional layer of key separation to the authentication process.

There are three different ways to get the A-key into the device. The most common method of programming A-keys into devices is for the A-key value to be generated by the manufacturer and pre-programmed into the device at the factory. When this method is used, the manufacturer must also provide the ESN (or pESN derived from the MEID) and the corresponding A-key information to the service provider for storage in the A-Key Management System (AKMS). Before activating a pre-programmed device, the AKMS must provision the ESN/pESN and A-key associated with the device into the AC.

To ensure the secure transport of ESN/A-key data between manufacturer and service provider, two approaches are commonly used. The first, and most robust, approach involves the use of an Electronic Data Interchange (EDI) between the manufacturer's database subsystem and the service provider's AKMS. This approach allows the AKMS to directly retrieve A-key information from a manufacturer's database subsystem with no risk of exposing the information to anyone within the service provider organization. However, while this solution works very well, smaller service providers often do not have access to an EDI infrastructure.

The second, and more widely used, approach involves the manufacturer providing the service provider with an encrypted file containing the list of ESN/A-key pairs. The service provider then typically uses a script to automatically decrypt and upload this information into the AKMS. This method is somewhat less secure than the EDI infrastructure approach since a person with access to the script could potentially decrypt and access the contents of the file. However, many service providers find this approach to be an equitable tradeoff between security and cost-effectiveness.

The third method used for provisioning A-key into the device is the Over The Air Service Provisioning (OTASP) protocol. This type of provisioning happens only after the sale. This method is also quite secure and supports the ability to provision the A-key after the handset has been sold to the end-user. This is especially useful to support consumer devices (e.g., Tablets, Laptops etc) or machine to machine (M2M) devices embedded with cdma2000 communication modules. The legacy A-key provisioning via keyboard entry of the A-key at the time of sales/provisioning is not secure and must not be used anymore.

Practices such as using all zero default A-key values must not be used by the operators since they are easily detected and essentially nullifies the benefits of authentication. Whether provisioned by the manufacturer or AKMS, A-keys should always be securely and randomly generated and protected from being viewed to the greatest extent practicable. In some emerging markets, some operators also use a smartcard (such as Removable User Identity Module or R-UIM) to store the A-key and other subscription data. The security provisions described in this document also apply to the smartcard case.

2.1.1.2 Shared Secret Data (SSD)

The SSD is a quantity used as the basis for authentication as well as other encryption features. SSD is composed of 8 octets known as SSD-A, and (another) additional 8 octets known as SSD-B. SSD-A is primarily used for general authentication, including global challenge and unique challenge operations. SSD-B is used to generate encryption masks (or keys) to support other features, including Voice Privacy and Signaling Message Encryption.

The A-Key is used along with the device's Equipment Serial Number (ESN) or Pseudo-ESN (generated from device's MEID) and a random number (RANDSSD) as input to the CAVE algorithm. The result of this execution of CAVE is called Shared Secret Data (SSD). The A-Key is only used to produce an SSD value. A part of that SSD (SSD_A) is then used as a CAVE input to perform subsequent authentication attempts, adding an additional layer of key separation to the authentication process. Only the AC and the handset are able to generate the SSD because only they have access to the A-Key unique for 'that' subscription.

The SSD update process (as shown in Figure 2.1 below) allows new SSD information to be generated by both the AC and device. Since this process relies on a device having a legitimate A-key value provisioned, use of the SSD update process is an easy way to turn off service to a cloned device that is using an illegally obtained SSD value. The SSD update process also allows roaming service providers that share SSD with their roaming partners to reduce security concerns by periodically changing SSD information.

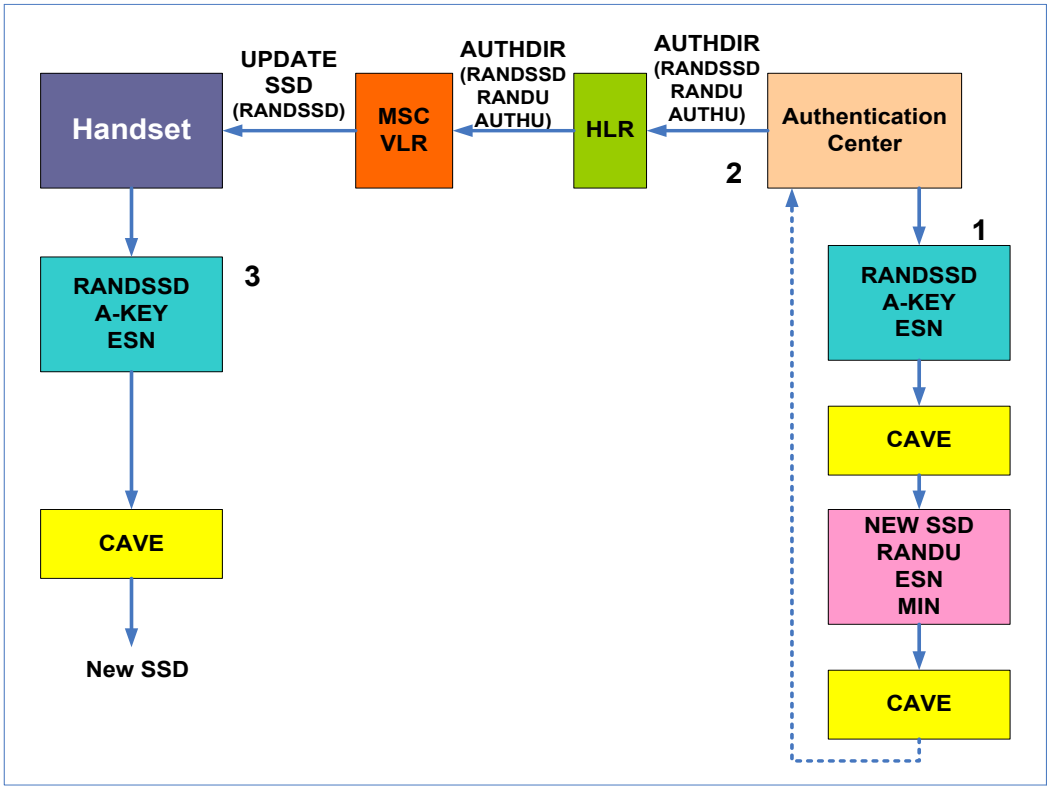

Figure 2.1: SSD Update process in CDMA2000 1X networks

Depending upon manufacturer, an AC may provide multiple mechanisms for initiating SSD updates. These methods include automatic triggering based on a service provider defined algorithm, periodic triggering based on a service provider defined interval, and manual triggering as needed.

The SSD update process involves two authentication challenges. The first is a base station challenge from the device when the request to update SSD is received. The purpose of this challenge is to allow the device to verify that the SSD update request is being initiated from a legitimate source. The second is a unique challenge (as explained in section 3.1.1.4) after the device has updated its SSD. The purpose of this challenge is to validate that the new SSD value generated by the device is legitimate. Once both challenges are complete, the home system receives a status message indicating whether the process was successful. The figure 2.2 shown

below provides details on how the device authenticates the network before it replaces its old SSD with the new SSD.

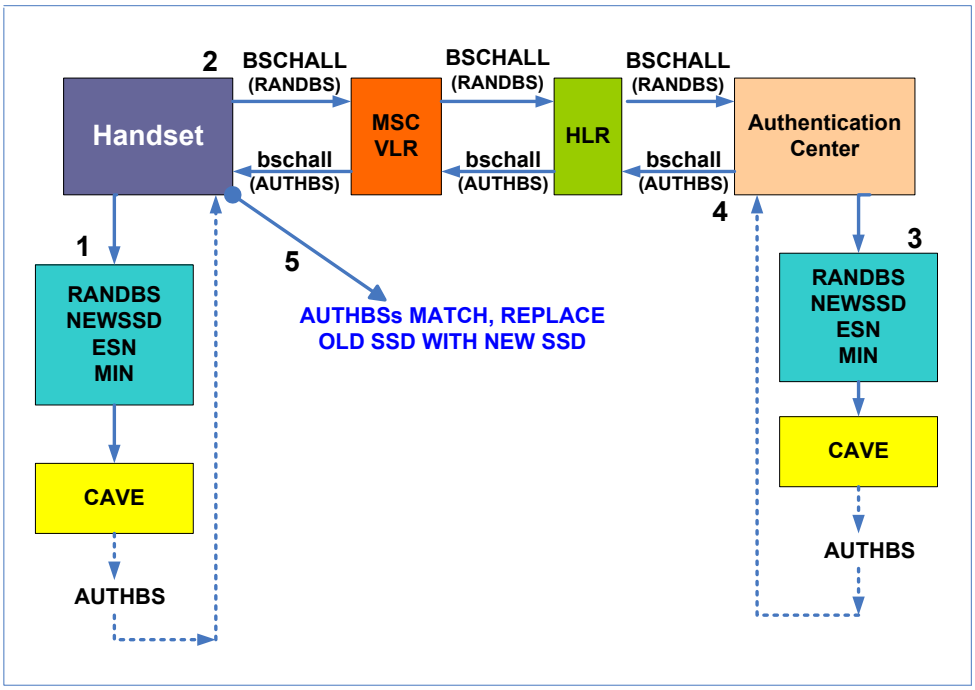

Figure 2.2: Base Station Challenge procedure in SSD update Process

In shared SSD scenario, the new SSD value generated by the AC is provided to MSC/VLR along with the RANDSSD to initiate the update to the device. The MSC/VLR uses this new SSD value to process both base station challenge and unique challenge during the SSD update process. Once these challenges are complete, the network sends an ASREPORT message containing SSD update and unique challenge report to the AC to indicate the outcome of the SSD update process.

In the authentication procedure, the network entity that participates in the challenge may be either the AC or the MSC/VLR (Visitor Location Register) depending on whether SSD is “shared” or not. Maintaining authentication at the AC isn’t necessarily the most efficient or economical process of authentication since it could result in a high volume of traffic on the network. Most viable implementation, therefore would be to “distribute” SSD by shifting the authentication process to the MSC/VLR.

Since the VLR does not have a copy of the A-Key, it cannot generate the SSD value itself, so the AC “shares” (not the ‘A’ key) the SSD value with the VLR. SSD is stored and maintained in the VLR database where it is used to execute the CAVE algorithm. The result of CAVE may be

sent to the MSC associated with the VLR for purposes of comparing authentication results, but SSD (itself) is never shared with the MSC.

The VLR retains the SSD until an event, external or internal to the AC, causes the AC to order the VLR to “drop” the SSD. To maintain security, the AC, if configured, informs the VLR to flush the SSD periodically and whenever fraud is suspected. While there are definite advantages to sharing SSD at the VLR level, sharing of the SSD is optional. The decision to share SSD is based on several factors including the service provider’s desire to share SSD and its ability to support SSD in a secured environment. If SSD is not shared with the VLR, then the AC will continue to perform authentication as necessary. In either case, it is recommended that the operators configure the AC to initiate the SSD update procedures periodically. Furthermore, if the SSD is shared with VLR, the operator may want to initiate SSD update based on certain pre-determined triggers (e.g., whenever the handset roams from one network to another network).

2.1.1.3 Authentication through Global Challenge

Global challenge is used by the 1X network to ensure that all devices attempting to access the system are authenticated. The device is required to perform global challenge in a network that indicates this request by setting the authentication bit (i.e. AUTH=1) in the overhead message. The overhead message would also include the global random challenge value (RAND) to be used in generating the authentication result (AUTHR).

In response to the global challenge indicated by AUTH=1, authentication-capable device will include a set of authentication parameters in system access messages to allow themselves to be authenticated by the network and they are;

- AUTHR: 18 bit Authentication signature value calculated by the device
- RANDC: Most significant 8 bits of the 32 bit RAND used to calculate the AUTHR
- COUNT: Current call history count stored in the MS (6-bit value)

The RANDC consists of the 8 most significant bits of the RAND and is used by the base station to pre-validate the system access message sent by the device. The base station compares the RANDC received from the device to the 8 most significant bits of the active RAND being broadcast on the overhead messages. While a system may discard a system access message if a mismatch is detected, the mismatch does not necessarily indicate that the device attempting to access the system is fraudulent, only that a cloned device scenario may exist. However, frequent mismatches or large differences between RANDC and RAND generally indicate fraud and warrant corrective action.

The basis for authentication is the ability for both the device and the authentication controller (i.e. VLR if SSD is shared or AC if not) to generate authentication signatures that may be

compared. In the case of a global challenge, the authentication signature is referred to as the authentication result (AUTHR) and is calculated using the Cellular Authentication and Voice Encryption (CAVE) algorithm with inputs illustrated in Figure 2.3 below.

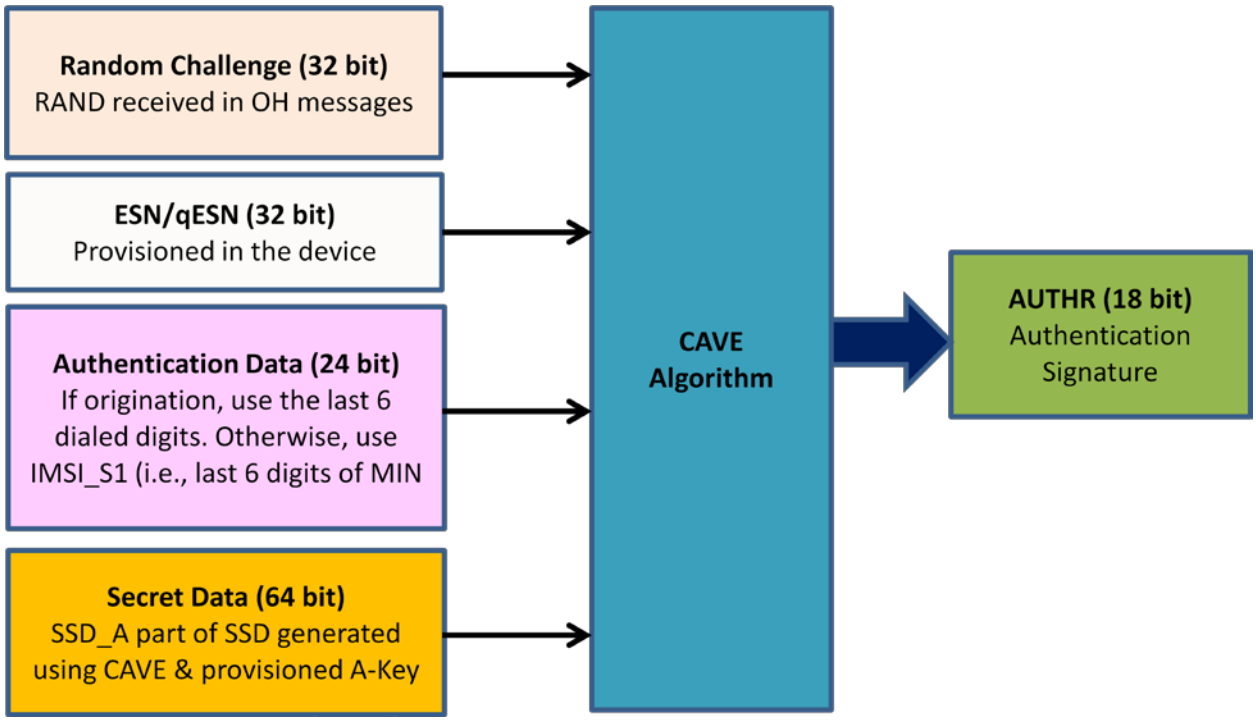

Figure 2.3: Generation of AUTHR for global challenge

Call History Count (COUNT) is a counter value maintained by the device and AC. Used during the global authentication process, this counter provides a mechanism for detecting cloned devices, especially when SSD and/or A-key values have been compromised. When a system access message is received by the network, the COUNT value provided by the device is compared with the one maintained by the authentication controller to determine whether they are consistent. A mismatch suggests that a clone may exist but is not necessarily a conclusive indication of cloning since RF transmission issues may result in occasional minor mismatches. However, there should not be a large delta between these values.

The policies of the authentication controller will determine whether to allow access, issue a unique challenge, or deny access based on a COUNT mismatch. However, cases of large discrepancies or repeated mismatches should be treated as indications of cloning fraud.

2.1.1.4 Authentication through Unique Challenge

Unlike global challenges that require all devices to provide authentication parameters before accessing the system, a unique challenge is directed at a specific device. Unique challenges may be used instead of or in addition to global challenges and may be initiated by the network, regardless of whether SSD is shared. Even if the authentication through Global Challenge is performed, it is recommended that operators configure their network to always perform authentication through Unique Challenge procedure during certain events (e.g., registration, call origination). The unique challenge reduces the fraud risk.

As with the global challenge, the basis for authentication is the ability for both the device and the authentication controller (i.e. MSC/VLR or AC) to generate authentication signatures that may be compared. In the case of a unique challenge, the authentication signature is referred to as the Authentication Response Unique Challenge (AUTHU) and is calculated using the CAVE algorithm with inputs illustrated in Figure 2.4 below. Note that the inputs used in generating AUTHU for unique challenge differ from the inputs used in generating AUTHR for global challenge.

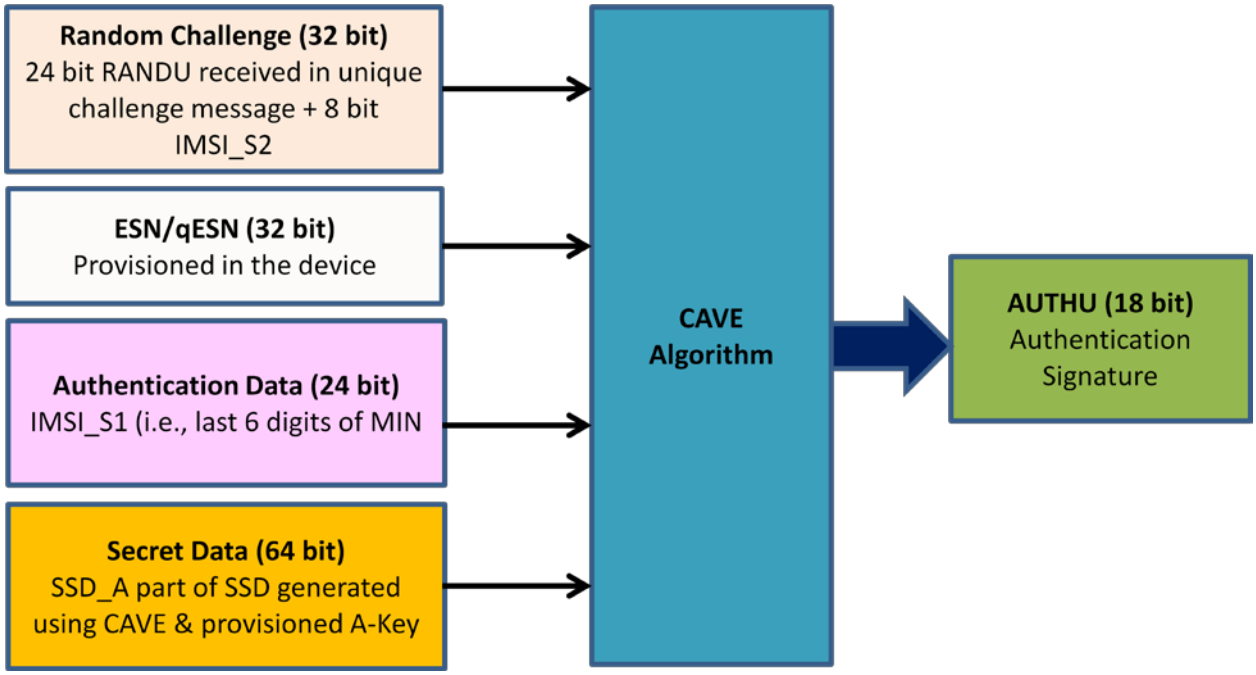

Figure 2.4: Generation of AUTHU for unique challenge

Upon receiving a unique challenge, the MS generates and includes an AUTHU value in a unique challenge response message. The network compares the AUTHU value received from the device with the AUTHU value either generated by the MSC/VLR or received from the AC to determine whether the device is authentic.

2.1.1.5 Protecting A-Key with CAVE based Authentication

A-key management and provisioning systems are additions to the inherent authentication features, but they are also critical to the process of authentication. The A-key is the cornerstone of the authentication process and the need for its security cannot be underestimated as it is generated, stored and programmed into the network and the subscriber's handset. A-key management systems will allow operators to generate random A-keys or provide for the secure transmission of pre-programmed A-keys from the manufacturer using electronic data interchange (EDI). If default A-key (all zeros) is loaded into the device/R-UIM, then it is just similar to having no A-key. Cloners can easily detect that default A-keys are in use and can fully exploit the network.

If operators wish to implement authentication in the future, legacy handsets programmed with default A-keys will inconvenience subscribers as well as operators who will have to have a new A-key loaded. This is especially true when Over The Air Functionality (OTAF) is not available. Random A-keys are important to the authentication process and an A-key management system will facilitate the secure generation and storage of random A-keys.

If an operator's log of A-key and ESN/MEID pair list falls into the wrong hands, the entire process of authentication may also be compromised. This is why A-key storage is critical. A-keys can be stored on the network, but, for heightened security, A-keys should be stored off the network in an A-key management system to limit the number of people who have access to the storage area.

2.1.2 AKA based Authentication procedures

A new form of authentication, based on 3GPP Authentication and Key Agreement (AKA) used in UMTS networks, is being introduced in CDMA2000 systems. It is called Enhanced Subscriber Authentication (ESA) (also referred as 3rd generation (3G) authentication) and is intended to replace CAVE-based authentication currently implemented in the CDMA2000 networks. The support for AKA in CDMA2000 networks is included in all releases following CDMA2000 Rev C. Note, however, that in order to facilitate interoperability and allow for phased introduction of AKA among various CDMA operators, devices and networks that support AKA should also support legacy CAVE-based mechanism.

The major advantages of AKA include robust and mutual authentication support. Robust authentication is provided through the use of larger 128-bit authentication key and a stronger standardized and well-studied authentication algorithm. Mutual authentication is provided via an authentication token passed to the MS during the AKA authentication challenge. The AKA

challenge mechanism is similar to a CAVE-based unique challenge from the perspective of the network authenticating the device. However, the addition of the authentication token provides the device with information that enables it to authenticate the network before completing the challenge. This mutual authentication capability prevents false base station attacks that could disable voice privacy or compromise private identity information.

Similar to A-key in CAVE based security provisions, a master key 'K' is being used in the AKA based security provisions. This 'K' key is stored in the HLR/AC and the R-UIM card (Removable User Identity Module, analogous to SIM card) of the device. Provisioning methods for 'K' key is very much similar to that of the A-key (at the manufacturer facility, manual keying or using OTASP). The HLR/AC generates Authentication Vector (AV) and it consists of RAND, XRES, CK, IK, AUTN and UAK (optional and specific to R-UIM). VLR obtains, stores and distributes AVs as required, there by it need not have constant contact with HLR/AC.

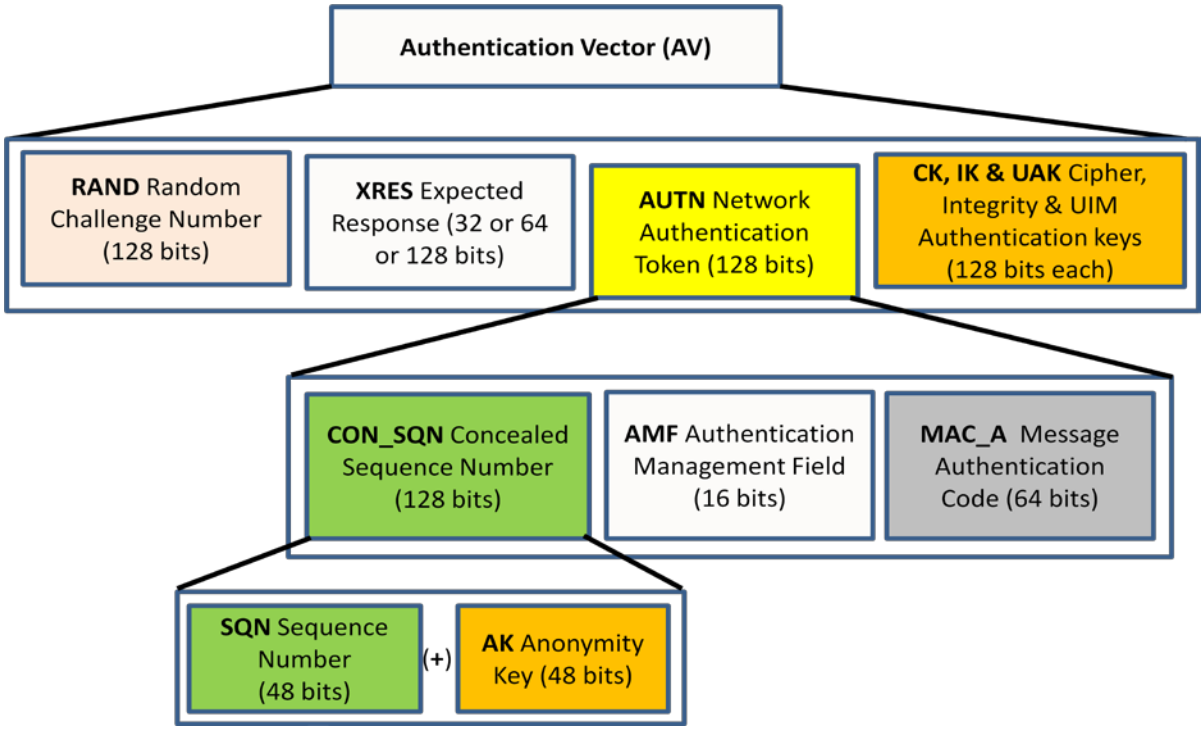

Figure 2.5: Information contained in an Authentication Vector

A fundamental concept in AKA is the authentication vector (AV). An AV is essentially a group of information (RAND, XRES, CK, IK, AUTN) used for one AKA attempt. AVs are generated by the home AC and distributed to the visited network. Each AV contains all information required by the visited network to locally perform AKA with an AKA-enabled device. To thwart replay attempts, each AV can be used only for one AKA attempt (i.e., each AKA attempt uses a different AV. Detailed information contained in an AV is illustrated in Figure 2.5 above.

The AKA authentication process can be explained in three major phases with each phase coming into effect assuming that the previous phase completed successfully. The first phase is

the distribution of AVs and in this phase the AVs are generated by the home AC and provided to the MSC. The Authentication of the network by the device is the second phase and in this phase the message authentication code (MAC_A) received from the network is verified against the expected MAC_A (XMAC_A) generated by the device. Other work performed in this second phase is that the sequence number (SQN) received from the network is verified against the SQN locally maintained by the device. The third phase is about the authentication of the device by the network. In this phase, the authentication response (RES) received from the device is verified against the expected RES (XRES) received from the home system in the network authentication token (AUTN). So, the establishment of security association happens between device and MSC in this third phase.

2.1.2.1 AKA Authentication of the network by the device

Authentication of the network by the device involves an explicit validation that the AC is synchronized with the device and an implicit validation that the AV information being used for this authentication was generated by an AC provisioned with the same master key (K) as the device. To ensure synchronization, a sequence number is provided by the network and compared against the sequence number maintained by the device. To validate the authenticity of the message, a message authentication code (MAC_A) is provided by the network and compared against an expected MAC (XMAC_A) computed by the device.

To maintain the identity and location privacy of the user, the network can optionally conceal the sequence number (SQN) using 48-bit anonymity key (AK). The result is the concealed SQN (CON_MS_SQN) which is provided to the device in the network authentication token (AUTN). Because it is concealed, the SQN must be derived by the device before it can be validated. To derive the SQN from the CON_MS_SQN, device first generates an AK value using f5 algorithm with inputs K and RAND. Since the device and home AC are provisioned with the same master key (K), the AK generated by the device will be the same as the one used by the AC to conceal the SQN. Once this AK has been generated, the device derives the SQN from the CON_MS_SQN and compares this SQN to its own.

If the SQN provided by the network does not match the one maintained by the device, a synchronization problem exists between the network and the device. In such a case, the device will respond to the authentication request with an authentication resynchronize message (AURSYNM). To enable the network to resynchronize with the device, the device includes a concealed version of its own SQN (CON_MS_SQN). In addition to the CON_MS_SQN, the device also includes a message authentication code for resynchronization (MAC_S) to allow the network to validate the authenticity of the resynchronization request and prevent unauthorized devices from initiating resynchronization.

The message authentication code (MAC_A) enables the device to authenticate the network. Using the f1 algorithm with inputs K, RAND, SQN & AMF (part of AUTN received in AV and sent to the device), the device generates an expected MAC_A (XMAC_A) value to compare to the one provided by the network in the AUTN. The XMAC_A generated by the device will only match the MAC_A received from the network if the master key (K) provisioned in the AC is the same as the one provisioned in the device. Therefore, by comparing XMAC_A with MAC_A, the device can ensure that the AV being used for this AKA was generated by its authentic AC. If the MAC_A received from the network in the AUTN does not match the XMAC_A value generated by the device, the device will reject the authentication request. If device decides that the RAND is not fresh, then it can initialize re-synchronization. The re-synchronization request is authenticated by HLR/AC to ensure that only the real UIM can initialize re-synchronization.

2.1.2.2 AKA authentication of the device by the network

Authentication of the device by the network in AKA is similar to a unique challenge without shared SSD in CAVE. In both cases, the network generates both the random challenge value that is sent to the device and the response value that is expected from the device. In AKA these values are the RAND and XRES, respectively. The f2 algorithm with inputs K and RAND is used by the device to generate the response (RES) value and by the AC to generate the XRES value. Figure 2.6 shown below gives a clear picture on the AKA based device authentication process.

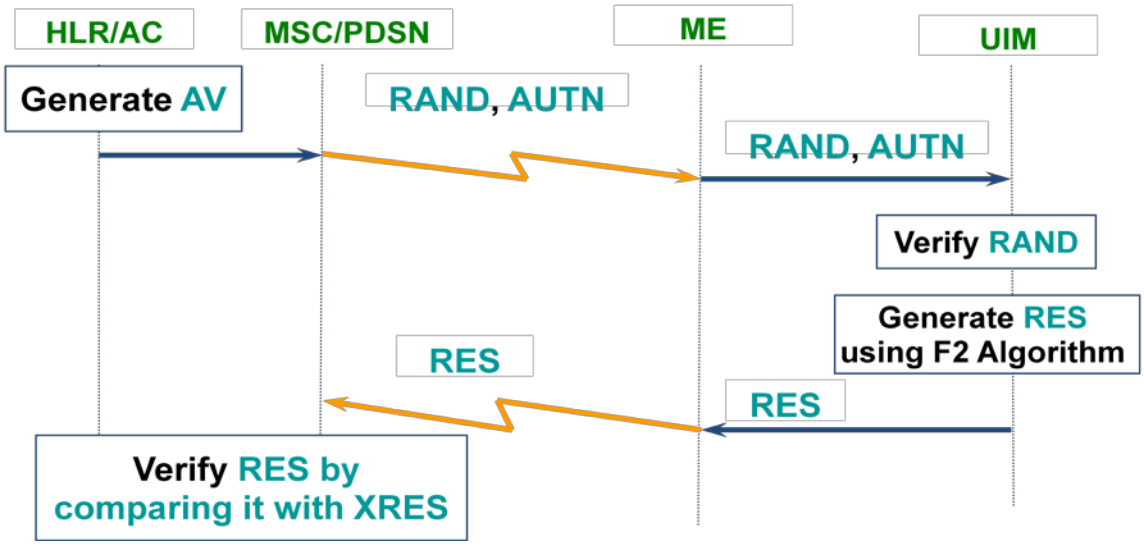

Figure 2.6: AKA based device authentication process

If the RES value returned by the device matches the XRES value contained in the AV being used for the AKA attempt, the network is assured that the master key provisioned in the device matches the one provisioned in its AC. If the RES and XRES values do not match, then the device fails authentication.

2.2 Encryption procedures in CDMA2000 1X

One of the main goals of security is to keep the privacy of the user communication and it can be achieved through radio channel encryption. Through session encryption and integrity protection, the operators can protect the communication session of the users from security vulnerabilities such as tampering, eavesdropping and session hijacking. While Authentication takes care of masquerading (pretending to be a legitimate user) and the unauthorized use of resources, the encryption addresses various forms of the threats such as the interception by hostile agencies; eavesdropping by hackers, criminals, terrorists; getting intelligence from traffic analysis (i.e., observation of user behavior, address & location). The latest developments in the security aspects in CDMA2000 networks also cover the integrity protection. Mainly the integrity protection addresses the threats such as manipulation of information, creation or deletion of messages and recording messages & replaying them later. In addition to addressing the above said threats, the CDMA2000 systems, due to their spread spectrum characteristics, inherently take care of security threats such as denial of service by attempting to use up capacity and jamming base stations by using high RF energy.

2.2.1 CAVE based Encryption procedures

In CAVE based security measures, a special Cellular Message Encryption Algorithm (CMEA) for signaling message encryption and a special ORYX algorithm for data encryption are being used on the CDMA channel. Also a Private Long Code Mask (PLCM) is used for Voice Encryption.

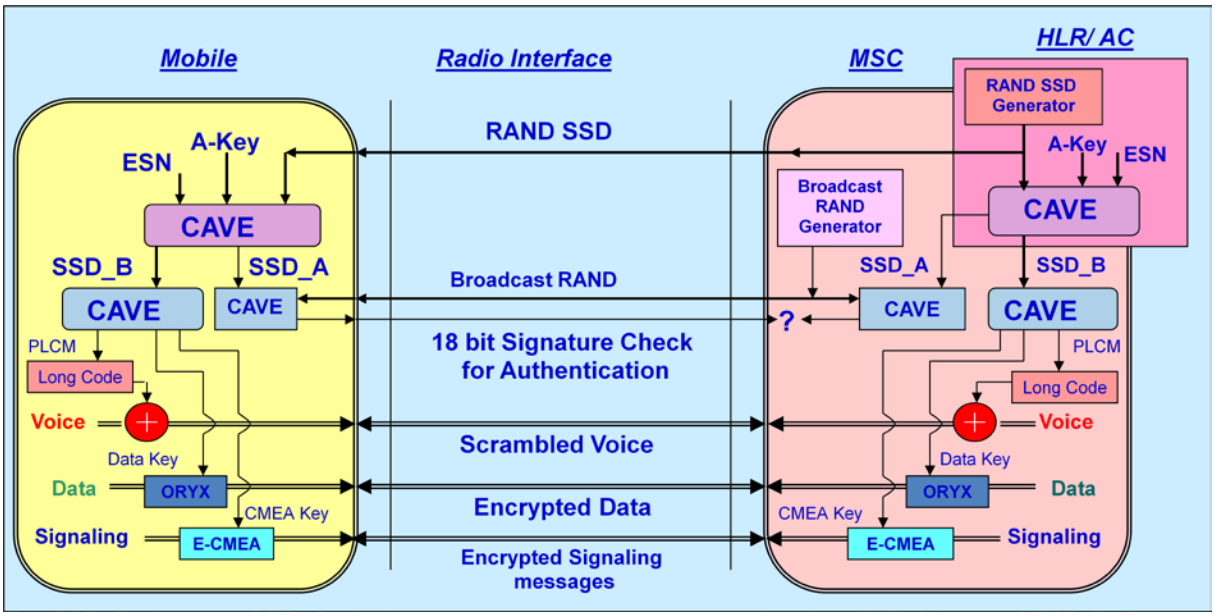

Figure 2.7: CAVE based Authentication and Encryption Procedures

In CDMA 2000 1x Rev 0, an enhanced CMEA or E-CMEA key is used which is again a 64 bit key to encrypt signaling messages. As shown in Figure 2.7 above both the 64 bit CMEA key and the 32 bit ORYX data key are derived using CAVE algorithm. While many of the vendors have implemented signaling message encryption, the data encryption's use for the radio channel in commercial CDMA2000 1X networks is not that popular, since in many cases, the data traffic is often protected at the application layer.

The encryption capability is supported by the device software in origination message for MO call and in page response for MT call. The ENCRYPTION_SUPPORTED field in these messages is an indication for the base station to send the Channel Assignment Message (CAM) with the ENCRYPT_MODE "on" condition. The ENCRYPT_MODE field in this message tells the mode of encryption to be used on the traffic channel. If the field value is '0', it indicates no encryption. It is kept as '1' for CMEA and '2' for E-CMEA. Encryption can be turned ON or OFF after this message on traffic channel. Sending General Handoff Direction Message (GHDM) or Extended Handoff Direction Message (EHDM) does this by setting the value to 1 or 0.

2.2.1.1 Signaling and Data Encryption

The security process would get enhanced when sensitive information such as PIN and DTMF tones sent in certain fields of the Traffic Channel Messages is encrypted. These types of specific fields in traffic channel messages are encrypted using the Cellular Mobile Encryption Algorithm (CMEA)/Enhanced-CMEA (E-CMEA). By the way, in CAVE based security mechanism, for encryption to take place, the device should be working in standard authentication mode. Basically, both the device and the network use CMEA key with the Enhanced CMEA (E-CMEA) algorithm to encrypt signaling messages sent over the air and also to decrypt the information received.

A separate data key, and an encryption algorithm called ORYX, is used by the mobile and the network to encrypt and decrypt data traffic on the CDMA channels. Figure 2.7 illustrates both the CDMA2000 1X authentication as well as encryption mechanisms.

2.2.1.2 Voice Privacy

Voice Privacy is provided by means of a Private Long Code Mask (PLCM) used for PN spreading. Transition to PLCM is done only when the device is in the standard authentication mode and also it is in traffic channel state. All calls are originated initially on Public Long Code Mask (42 bit long). To initiate a transition to the private or public code mask, either the device or base station (BS) sends a Long Code Transition Request Order on traffic channel.

The device or the user of the device may request voice privacy during call set up using the Origination Message or Page Response Message and during traffic channel operation using Long Code Transition request Order. The BS or the device responds to this with a Long Code Transition Completion Order. The BS can also cause a transition to private or public long code mask by sending the EHDM or the GHDM with the PRIVATE_LCM bit set appropriately.

To be precise, the Private Long Code Mask is utilized in both the device and the network to change the characteristics of a Long code. This modified Long Code is then used for voice scrambling, which adds an extra level of privacy over the CDMA air interface. The Private Long Code Mask doesn't encrypt information, it simply replaces the well-known value used in the encoding of a CDMA signal with a private value known only to both the device and the network. It is therefore will be harder to eavesdrop on conversations without knowing the Private Long Code Mask.

2.2.2 AKA based Encryption procedures

While CAVE based security procedures takes care of the authentication and encryption related security aspects, the AKA based security procedures would also takes care of other security features such as Confidentiality, Integrity and Anonymity. The confidentiality is achieved through the encryption process of all voice, data & signaling information to/from the device. The integrity is achieved through MAC protection of signaling to/from the device. The anonymity can be achieved through frequently assigning the device with a new temporary identity (TMSI).

The AKA mechanism also allows for the generation of new cipher key (CK) and integrity key (IK). These 128-bit keys enable a security association between the device and the serving MSC for supporting advanced security services such as signaling message data integrity, signaling information element encryption and user data encryption. To protect against a "Rogue Shell Attack", a new procedure is standardized. Conventional AKA does not validate the continued presence of an R-UIM in the terminal, hence a "Rogue Shell" may continue using CK and IK after the R-UIM is removed from the terminal. R-UIM authentication requires a new 128 bit UIM Authentication Key (UAK) computed by the R-UIM and the HLR/AC and shared with the VLR. The device and the AC each generate these keys independently. In the roaming context, the keys generated by the home AC are provided in authentication vectors to the visited network and are never transmitted over the air to or from the device. The Figure 2.8 shown below gives an idea on how various security keys generated within R-UIM of the device.

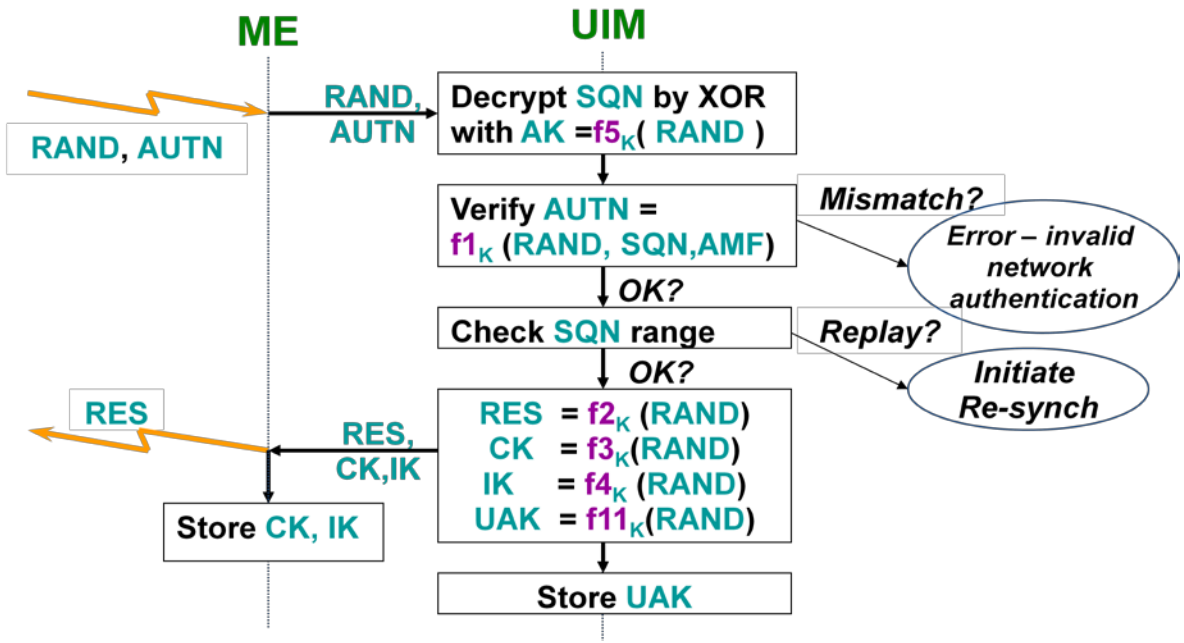

Figure 2.8: Security Keys generation process in the C2K UIM

2.3 Security measures for 1X Packet data service

In CDMA2000 1X networks, additional security measures exist for the packet data services, in form of service/subscription authentication and ORYX/AKA based encryption measures. The 1X packet data service/subscription authentication procedure is similar to the service/subscription authentication procedure used in 1xEV-DO networks. Kindly refer to sub-chapter 3.2.3 in the subsequent chapter for details on service/subscription procedures.

Another new security mechanism that is gaining popularity in 3GPP2 (both 1X and EV-DO) packet data networks is EAP-AKA (Extensible Authentication Protocol- Authentication and Key Agreement). This method for authentication and session key distribution uses AKA mechanism. AKA is based on challenge-response mechanism and symmetric cryptography. AKA typically runs in a CDMA2000 device or Removable User Identity Module (R-UIM). EAP-AKA is a new EAP method that binds the derived keys to the name of the access network. When the network is configured with the Authentication State set to 'ON' condition, the network's authentication server can start an EAP-AKA authentication procedure with the device during the PPP session negotiation (the device acts as an EAP-AKA peer). The network and the device mutually authenticate each-other. Upon successful authentication, the device is authorized to access the network.

With AKA based encryption procedures applied, a CDMA2000 1X packet data call gets Enhanced Subscriber Privacy (ESP) with encryption on all information bearers and also in multiple layers. At the air interface level, a strong encryption algorithm 'AES' with large keys (128-bit) gets applied. Application encryption can also be applied with any standard end-to-end encryption at the application layer level, such as IP security (IPsec) and Pretty Good Privacy (PGP). The Figure 2.9 shown below gives a clear idea on how the user privacy is maintained through multi-layer encryption techniques in CDMA2000 1X packet data networks.

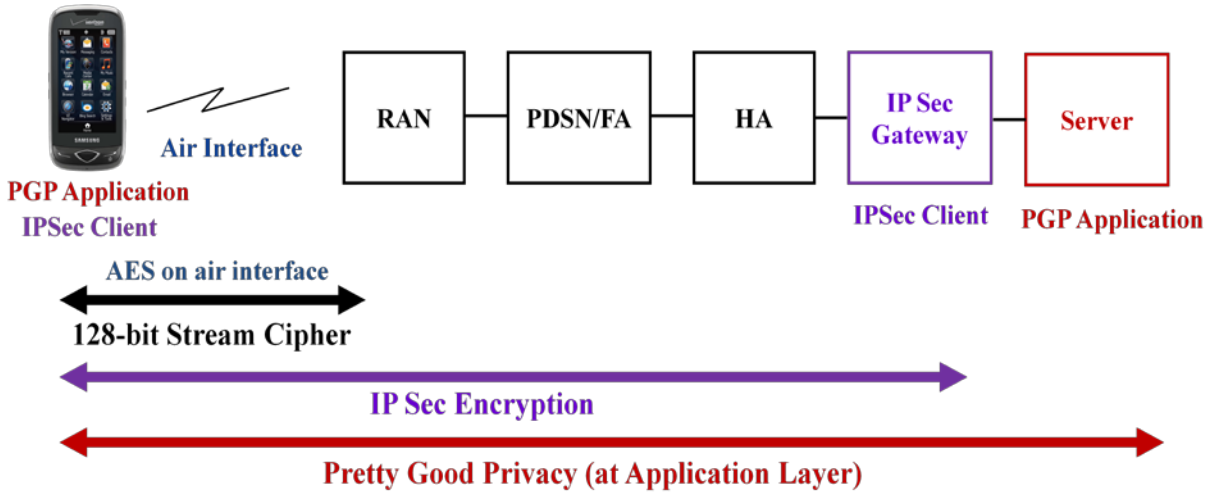

Figure 2.9: Multi-layer Encryption Possibility with C2K 1X Packet data

When it comes to handling packet data in CDMA2000 1X networks, additional security measures are to be considered such as:

- Firewalls: Reliable and secure, hardware and software based firewall solutions are used to enforce security policies in network gateways
- Secure Routing: Done in a secure manner using different routing protocols to access only the required parts of the network
- Proper IP-addressing: By using private IP addresses in the Mobile Wireless network, it is not possible to see the MS from the outside
- Usage of Secure Protocols: Secure protocols such as IPsec, SSL and SSH are used to connect the network
- IPsec, which is invisible to upper layer protocols, has been developed to solve the security weaknesses of IP by protecting both the integrity and confidentiality of the IP packet, without changing the application interface to IP

3 Security Provisions in 1xEV-DO Networks

In CDMA2000 1xEV-DO systems, a separate layer called “security layer” has been defined exclusively to take care of all security related requirements. As shown in Figure 3.1, the security layer sits in between the MAC and Connection layers of the 1xEV-DO layered architecture. The protocols defined within the security layer are as follows:

- Key Exchange protocol: Provides the procedures followed by the access network and by the access terminal to exchange security keys for authentication and encryption
- Authentication protocol: Provides the procedures followed by the access network and the access terminal for authenticating traffic
- Encryption protocol: Provides the procedures followed by the access network and the access terminal for encrypting traffic
- Security Protocol: Provides public variables needed by the authentication & encryption protocols (e.g., cryptosync, time stamp etc.)

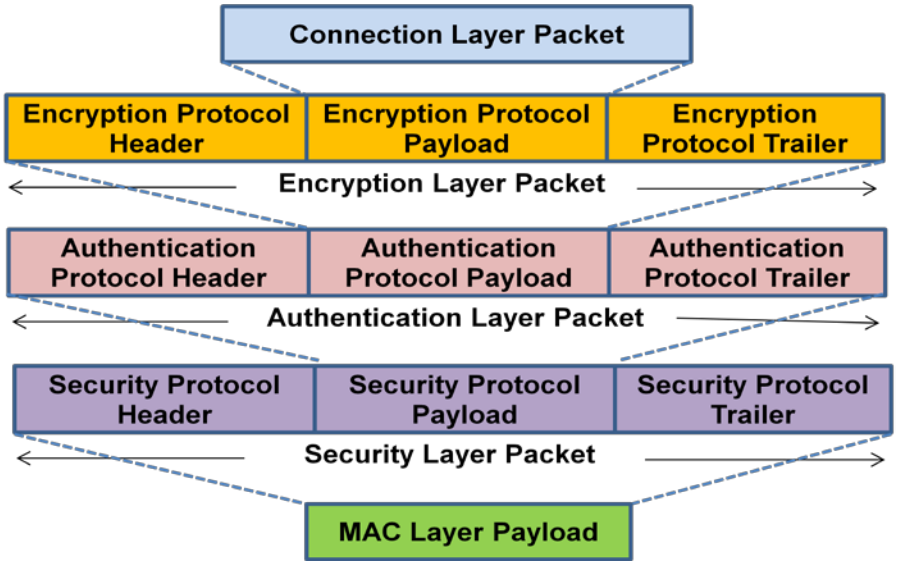

Figure 3.1: Security layer encapsulation procedures

The Figure 3.2 shown below provides a clear picture on the entities as well as the keys involved with all the security features (key exchange, authentication and encryption) in an EV-DO system.

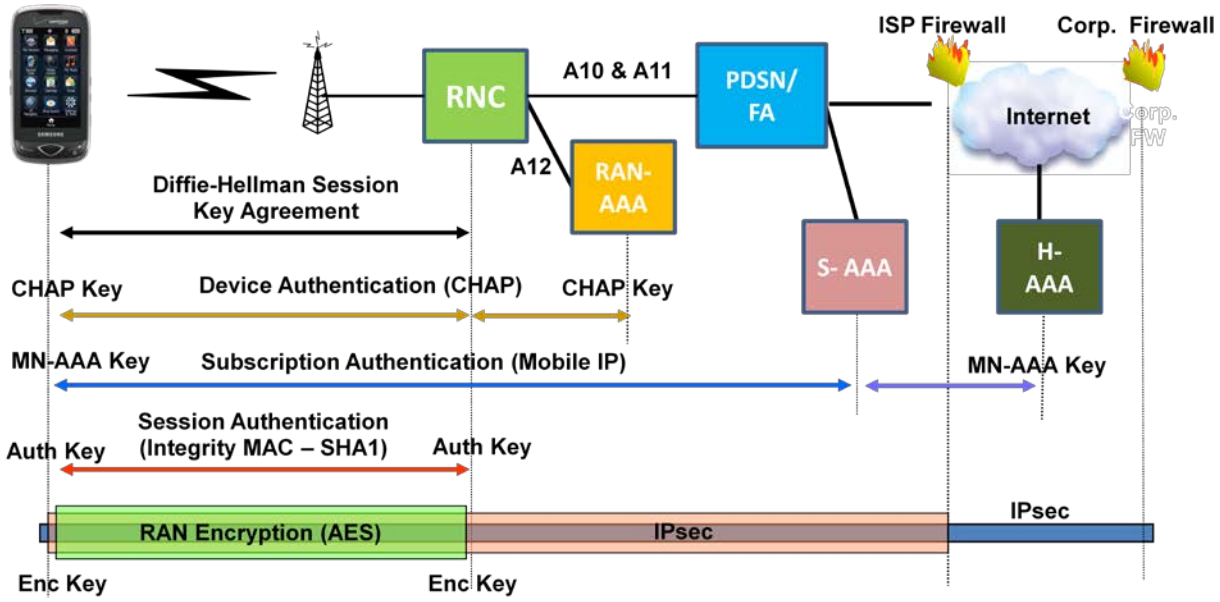

Figure 3.2: Security provisions in CDMA2000 1xEV-DO systems

3.1 Session Key exchange through DH Protocol

The DH Key Exchange Protocol provides a method for session key exchange based on the Diffie-Hellman (DH) key exchange algorithm. This Key Exchange Protocol uses the KeyRequest and KeyResponse messages for exchanging public session keys (SKey), and the ANKeyComplete and ATKeyComplete messages for indicating that the secret session keys have been calculated. The AT and the AN perform key exchange procedure during session configuration. Steps involved in the key exchange procedure from the AT perspective:

- Upon receiving KeyRequest message from AN, the AT shall choose a random number "ATRand" and set the ATPubKey field of the KeyResponse message with "g ATRand mod p" where g and p are KeyLength dependent protocol constants for the DH Key Exchange protocol, and KeyLength is specified during session configuration of the DH Key Exchange Protocol.
- AT sends KeyResponse message and starts a timer (as per AN's in KeyRequest message) and computes the session key (SKey) as per the formula:
  SKey = "ANPubkeyATRand mod p" and a 64 bit TimeStampLong
- AT disables the timer when it receives the ANKeycomplete message with matching Transaction ID (as that in KeyRequest message)
- AT commutes the 160 bit "Message Digest" based on computed SKey, computed TimeStampLong, Transaction ID and Nonce fields of the ANKey complete message
- If the message digest computed in the previous step matches the KeySignature field of ANKeyComplete message, the AT sends an ATKeyComplete message with the result field set to '1'

Steps involved in the key exchange procedure from the AN perspective:

- Before sending the KeyRequest message to AT, the AN shall choose a random number "ANRand" and set the ANPubKey field of the KeyRequest message with "g ANRand mod p" where g, p and KeyLength are specified during session configuration of the DH Key Exchange protocol
- If the AN does not receive a KeyResponse message with a TransactionID field that matches the TransactionID field of the associated KeyRequest message, within stipulated time period (kept at 3.5 seconds), the AN shall declare failure and stop performing the rest of the key exchange procedure.
- After receiving KeyResponse message AN starts a timer and computes the session key (SKey) as per the formula: SKey = "ATPubkeyANRand mod p" and the 64 bit TimeStampLong
- AN commutes the 160 bit "Message Digest" based on computed SKey, computed TimeStampLong, Transaction ID and few padding bits
- The AN sends an ANKeyComplete message with the KeySignature field of the message set to the message digest computed in the previous step and the TimeStampShort field of the message set to the 16 least significant bits of the CDMA System Time used in the previous step. The AN shall then start the AT Signature Computation Timer with a time-out value of TKEPSigCompAN (also kept at 3.5 seconds)
- The AN disables both AT Key Computation Timer and AT Key Signature Computation Timer when it receives an ATKeyComplete message with a TransactionID that matches the TransactionID field of the associated KeyRequest and KeyResponse messages

This secretly shared session key (SKey) is being used to generate the other security keys such as the Encryption Keys (FACEncKey & RACEncKey) and the Authentication Keys (FACAuthKey & RACAuthKey). These security keys are associated with the EV-DO session. If a default Authentication Protocol is chosen then it does not provide any services except for transferring packets between the Encryption Protocol and the Security Protocol, without adding any header or trailer. Other Key Exchange Protocol that can be used to create independent sessions keys for encryption and integrity is Generic Key Exchange (GKE) protocol that uses the Pair-wise Master key (PMK) at the AT and AN.

3.2 Authentication procedures in 1xEV-DO

In CDMA2000 1xEV-DO systems, there are three distinct types of authentication procedures in use and they are:

1. RAN Access authentication.
2. IS-856 Air interface authentication for integrity protection.
3. Service/Subscription authentication with the Operator/ISP
    a. With PDSN/FA for Simple IP
    b. With Home Agent for Mobile IP

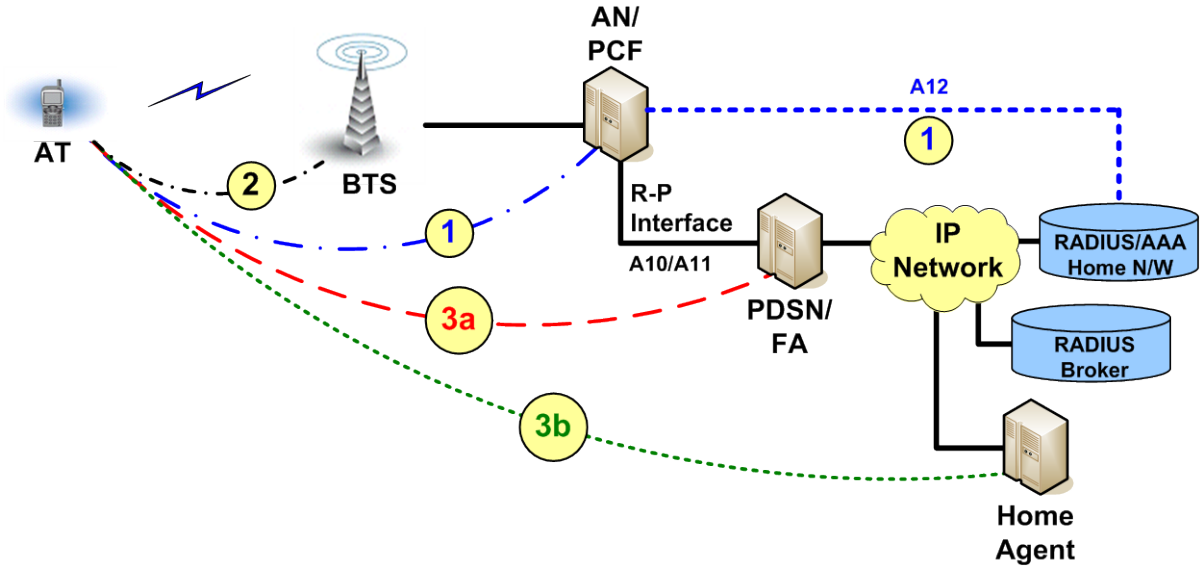

Figure 3.3: Types of authentication procedures in EV-DO systems

The main purpose of Authentication in EV-DO networks is to establish that the AT is the true owner of a). The radio session b). A legitimate subscription record with the operator & c). The R-P pipe (A10/A11) to the PDSN (and hence the PPP session). In a hybrid (1X/1xEV-DO) device, 1X registration and authentication occurs first and hence 1X authentication is already complete when 1xEV-DO authentication begins. The figure 3.3 shown above gives an idea of the entities and interfaces involved in each type of authentication procedure.

3.2.1 RAN Access Authentication procedures

The RAN access authentication (also known as ‘A12’ or RAN authentication by the device) validates the device’s subscription with the wireless operator. It enables the operator to authenticate the device independent of the ISP. The Challenge Handshake Authentication Protocol “CHAP” is used to identify and authenticate the user with an access network AAA (AN-AAA). As shown in ‘procedure 1’ of Figure 3.2 above, EV-DO systems use a special packet data stream for device authentication and the end points for this PPP session are the device and the RNC/PCF and the PCF talks to the AN-AAA over the ‘A12’ interface.

The EV-DO standards specify the use of CHAP for access authentication. In addition to CHAP, in some networks the AN-AAA server also provides a means for doing hardware ID verification. However, the hardware ID verification mechanism is inherently insecure since the device’s hardware ID is not a secret value and is sent in clear over the air. Besides, it does not add any additional security value beyond what a unique NAI and shared secret already provided. Despite this, a number of operators are relying on the hardware ID for an authentication mechanism. Relying on hardware ID as an authentication must be avoided in order to prevent unauthorized access to IP data services.

The device (or R-UIM in the device) should be provisioned with a unique NAI and unique CHAP shared secret (also referred to as password). These same unique values should also be provisioned in the AN-AAA for the appropriate user's profile. The generation of the NAI and password are the responsibility of the service provider. The NAI and password should be chosen and managed using procedures that minimize the likelihood of compromise, i.e., they should be cryptographically strong and difficult to guess or predict. It is strongly recommended that service providers choose unique shared secret or password for each device with a length of at least 32 hexadecimal digits (i.e., equivalent to 128-bit value).

After the PPP session is established, and CHAP is negotiated between the AT and AN:

- AN sends a CHAP Challenge to the AT
- AT uses the CHAP Challenge and the CHAP shared secret as input to the MD5 algorithm to compute the CHAP response
- AT sends the NAI, CHAP Challenge and CHAP Response back to the AN over the PPP session
- Upon receipt of the CHAP response message containing NAI, CHAP challenge and CHAP response, AN in-turn passes this information to the AN-AAA over the A12 interface using the A12 Access -Request message
- AN-AAA uses the NAI it receives to look up the CHAP shared secret associated with the appropriate subscriber. It then uses the shared secret and CHAP Challenge it received as input to the MD5 algorithm to generate the CHAP Response.
- If the computed CHAP Response matches the received value of CHAP Response, authentication succeeds. If not, authentication fails
- AN-AAA informs the AN of the outcome of authentication over the A12 interface via A12 Access-Accept or (A12 Access-Reject Message in case CHAP responses don't match), which in-turn informs the AT via PPP session

When device access authentication is performed during session establishment, the RAN remembers that the device has a valid subscription with the operator. Subsequent access attempts are validated by associating the key that was exchanged during radio session establishment with the Access authentication. A12 authentication occurs before the packet data authentication. A12 authentication allows the AN to obtain the Mobile Node Identifier (MN ID) which is used by the RAN on the A8/A9 and A10/A11 interfaces to support handoffs of PDSN packet data sessions between ANs and between 1xEV-DO and 1X systems. An AT that has not been provisioned with A12 credentials will not be able to roam into networks with the that require A12 authentication.

To be precise, the SC/MM (Session Control and Mobility management) function in the AN performs the access authentication procedure. This function judges whether an AT should be authenticated when the AT is accessing the EV-DO RAN. The SC/MM performs Point-to-Point Protocol (PPP) procedures for access authentication. The A12 interface carries signaling information related to access authentication between the SC/MM function in the AN and the AN-

AAA (Authentication, Authorization and Accounting) entity. A PPP session between the AT and SC/MM function in the AN is used to authenticate the AT.

3.2.2 IS 856 Air Interface Authentication procedures

If the device access authentication is analogous to establishing a checking account at a bank (you fill out paper work and also provide a legal form of identification), then the IS-856 air interface authentication is analogous to the online banking process that requires you to provide credentials at all times.

In 1xEV-DO systems, the AN verifies that each message received over the access channel is from a known device (AT), and the messages have not been altered or replayed. EV-DO standards support SHA-1 hashing algorithm to authenticate every Access channel message. The SHA-1 Authentication Protocol provides a method for authentication of the Access Channel MAC Layer packets. This is done by applying the SHA-1 hash function to message bits that are composed of the ACAuthKey (derived from the SKey), security layer payload, CDMA System Time (to avoid replay attacks) and the sector ID. Air Interface authentication only verifies that the mobile is the owner of the radio session and hence owns that particular A10/A11 connection. Figure 3.3 provides pictorial description of this air interface authentication procedures.

If a wireless operator owns both the PDSN as well as the AAA server that the PDSN uses to authenticate the user NAI, then the operator does not need two separate AAA servers. Similarly, if an operator controls both the user's Radio Access NAI and the user's Service Access NAI, then the operator can use the same or different NAI for both Radio Access and Service Access procedures, depending on their deployment and roaming needs. The AN-AAA maps the NAI to the IMSI and provides the IMSI to the base station. Upon successful authentication, the base station binds the Air interface session key to the IMSI.

3.2.3 Service/Subscription Authentication procedures

The IP Service requests from the device are authenticated and authorized by an entity in the PDN (e.g., PDSN/FA) or the home agent (HA). Subscription authentication has the following functionalities:

a. Performed when initially establishing a data session
b. Performed between the device and PDSN or HA based on User NAI ("user@H-AAA-realm.com") and Password

In Simple IP networks, the authentication is executed between the PDSN/FA and AAA/RADIUS server. The CHAP is generally used for the authentication. PDSN first challenges the AT and the AT uses MD5 to hash the CHAP ID, shared secret and CHAP Challenge to calculate the challenge response. PDSN forwards the access request to AAA/RADIUS server, which contains Network Access Identifier (NAI), CHAP ID, Challenge and Challenge Response. The AAA/RADIUS server uses the NAI as the index for obtaining the AT's shared secret and uses it to verify the Challenge Response. The CHAP shared secret is pre-provisioned in both the AT and the AAA/RADIUS server.

In Mobile IP networks, two phases of the authentication are executed between the HA and AAA/RADIUS server. In Phase 1, the AT is authenticated by home AAA/RADIUS server. AT receives Agent Advertisement. Advertisement contains FA COA and FA Challenge. AT sends Registration Request which contains NAI, FA Challenge, MN-AAA Authentication Extension (i.e., Challenge Response), and MN-HA Authentication Extensions. FA forms an Access Request which contains NAI, Challenge and Challenge Response; and routes it to the AT's home AAA/RADIUS server based on NAI. Home AAA/RADIUS server verifies the Challenge Response and replies with Access Accept if successful. So, this authentication in Phase 1 is analogous to CHAP for Simple IP.

In Phase 2 the AT is authenticated by the HA. Upon receiving Access Accept, PDSN forwards the Registration Request to HA. HA authenticates the AT, assigns an address (if requested by the AT) and updates the mobility binding. Actually, the HA sends Registration Reply to PDSN, which includes MN-HA Authentication Extension, AT's home address, lifetime etc. The FA adds the AT to the visitor-list and binds the AT's home address as well as the HA address to the AT's A10 connection ID. The FA forwards Registration Reply to AT that authenticates the HA by verifying the MN-HA Authentication Extension.

3.3 Encryption procedures in 1xEV-DO Systems

In EV-DO systems, the traffic channel encryption (or confidentiality protection) is available to provide privacy of user data over the traffic channel as well as to provide prevention against session hijacking. EV-DO systems support AES (Advanced Encryption System) for traffic channel encryption.

The encryption is an essential part of the Packet Data Network (PDN) Security involving entities such as PDSN, HA (if mobile IP is used) and Home AAA in the EV-DO network. The IP termination point for the Simple IP (v4/v6) case is PDSN, where as for the Mobile IP (v4/v6) case it is the HA (Home Agent). The IPsec protocol is supported for securing traffic between the AT and these nodes within the PDN in a hop-by-hop fashion. IPsec provides security services to enable secure communication between peers and replaces the older Point-to-Point Tunneling

Protocol (PPTP). IPsec services include mechanisms for peers to agree upon security protocols and encryption keys and procedures for using these selections to ensure secure data transport. Once two peers have agreed on the encryption mechanism there is said to be a “security association” between them. As shown in Figure 3.2, the AES encryption mechanism at the link layer mainly takes care of the air interface security where as the IPsec based security is extended further to end points in the network.

IPsec encryption mechanism can either be used in transport mode to directly encrypt the traffic between two peers or in tunnel mode to build “virtual tunnels” between two networks. These virtual tunnels are more commonly known as Virtual Private Networks (VPNs).

4 Developments in C2K Security provisions

A Femtocell Access Point (FAP) or in short a Femto Cell is a wireless access point that provides coverage in a small area, usually a private residence or a small office and connects the MS to an operator's network via a broadband connection (e.g., DSL, cable). The FAP can be operating in cdma2000 1x mode, HRPD mode, or both modes. Usage of FAPs in CDMA2000 network is slowly gaining popularity because the operators can offload traffic from their macro network to the femtocells, thereby freeing up the valuable macro network capacity. The use of femtocells also has a potential to expand network coverage considerably, and be an element in assisting operators to provide network coverage in areas where macro coverage is poor or non-existent. Hence, a closer look into the special security needs of femto cell deployment is very much required.

The other area, where the usage of the CDMA2000 networks gaining popularity is the Machine-to-Machine (M2M) communications. Optimizing support for Machine-to-Machine (M2M) communications in 3GPP2 networks will allow operators to penetrate and establish a strong position in this emerging and potentially large market. The credentials of these M2M devices should be managed securely and hence the need for special security measures.

4.1 Femto cell network Security measures

The 3GPP2 specifications provide a complete security architecture that allows CDMA2000 femtocell networks to support large numbers of femtocells via standard commercial IPsec/IKEv2-based security gateways. The 3GPP2 security architecture and protocols (most notably for the security gateway and FAP authentication mechanisms) are compatible with the security architecture for 3GPP radio technology-based femtocell devices. The foundations of that common femtocell security model were pioneered in the Femto Forum. This architecture not only protects system operators' core networks, but also provides for highly secure authentication of FAP devices using certificate-based mechanisms and protocols that are widely deployed and validated for security, robustness, manageability, and scalability.

In Femtocell environment, the device (MS/AT) uses the CDMA2000 air interface to access services through a Femto cell, also known as Femtocell Access Point (FAP). The FAP uses a Security Gateway (SeGW) to securely connect using any IP network (such as the internet) to a CDMA2000 operator's core network. Since the IP network (e.g., broadband connection) between the FAP and the SeGW is assumed to be un-trusted, the FAP needs to be authenticated and authorized by the CDMA2000 network before a FAP is allowed to provide service to the devices. The Femtocell AAA is an optional functional entity in the CDMA2000 network that allows for management of more advanced authorization information and femtocell

based services. It is possible for operators to upgrade their existing AAA infrastructure to support Femtocell AAA functions.

So, basically there is a requirement for two types of authentication, authentication of the FAP with the CDMA2000 core network and the authentication of the MS while it is attached to the FAP. The Security Gateway (SeGW) is a network entity that resides in an operator's network and provides secure access for the Femtocell or more precisely Femtocell Access Point (FAP) to securely connect to the system operator's core network.

The Security Gateway (SeGW) provides security functions for FAP access to the CDMA2000 core network. It supports secure tunnel management procedures between itself and the FAP, including establishment and release of the tunnel; allocation of an IP address to the FAP from the CDMA2000 core network so that the FAP can route the MS traffic to the operators network; and encapsulation and de-capsulation of packets to and from the FAP. Through the interface to the Femtocell AAA, the SeGW supports Femtocell level authorization and transfer of authorization policy information.

The Femtocell Management System (FMS) is a management server that is used to configure and monitor the operation of the FAPs using TR-069 protocol. The FMS is typically assumed to be located inside the operator's core network (i.e., reachable by the FAP only through the SeGW).

4.1.1 FAP Authentication and Authorization

The authentication between the FAP and the SeGW (referred to as the FAP authentication) is performed using IKEv2 with X.509 digital certificates. The FAP is authenticated by the SeGW using the FAP's certificate. The FAP's certificate is installed by the FAP vendor during its manufacturing. The FAP certificate is identified using device identifier of the FAP (i.e., FEID) and is compliant to the IEEE Extended Unique Identifier-64 (EUI-64) format containing the IEEE hardware address of the device. The EUI-64 format supports encapsulation of both 48-bit and 64-bit IEEE hardware addresses such as the MAC address. FEID is encoded in FQDN format (e.g., FEID.devicemodel.vendor.com) in the subjectAltName extension of the FAP certificate. The same FEID in FQDN format is also used in the IKEv2 Identification payload (i.e., IDi field) of the IKE_AUTH request from the FAP. The SeGW checks the FAP certificate validity time. The SeGW is authenticated by the FAP using SeGW's certificate.

The SeGW certificate is assigned to the SeGW by the CDMA2000 network operator. In order to support interoperability between the FAP and the SeGW, the SeGW server certificate needs to be compliant to the SeGW certificate profile specified by 3GPP2. The SeGW certificate is

identified by using either the SeGW's FQDN or its IP address in the subjectAltName extension of the SeGW certificate. The SeGW's FQDN (or the IP address) is used in the IKEv2 Identification payload (i.e., IDr field) of the IKE_AUTH response from the SeGW. The FAP checks that the subjectAltName extension in the SeGW certificate matches the value received in the IDr field. The FAP also checks the SeGW certificate validity time. At least one CA certificate in the trust chain of SeGW certificate needs to be pre-provisioned in the FAP for verifying the SeGW certificate. At least one CA certificate in the trust chain of FAP certificate needs to be pre-provisioned in the SeGW for verifying the FAP certificate.

After the FAP is successfully authenticated by the SeGW, based on the network policy, (e.g., FAP authorization is required), the SeGW may contact the Femtocell AAA for authorization using FEID in FQDN format received in the IDi payload as the FAP username in NAI format (i.e., FAP-FQDN@realm) using AAA protocols. The Femtocell AAA checks the FAP authorization policy based on the FEID received in the AAA message. If the FAP authorization check fails, the Femtocell AAA sends a AAA message to the SeGW indicating authorization failure. The Femtocell AAA needs to maintain the FAP authorization policy. The authorization policy may be based on a black list/white list of FEIDs or a profile for each FAP. The FAP authorization policy may be associated with the existing user profile at the AAA.

4.2 Security developments for M2M Communications

Machine-to-Machine (M2M) communication, also referred to as Machine Type Communication (MTC), is a form of data communication that involves one or more entities that do not necessarily require human interaction or intervention in the process of communication. The common characteristics of M2M communication services are:

- Communication scenarios that do not require human control
- Limited human interaction in the communication process
- Anticipation of a potentially huge number of communicating devices
- Lower complexity and less effort compared to human communication
- Mostly uses data communications (both packet/circuit-switched data services)
- Low volumes of traffic per device for a majority of M2M applications

Security and privacy is a major concern for M2M customers. Customers are concerned with fraudulent operations, such as eavesdropping, cloning, message interception and last but not the least, the subscription fraud. Enhancements in CDMA2000 1X (Rel C onwards) as well as in 1xEV-DO systems provide end-to-end security by using improved encryption algorithms and other means such as improved authentication, hashing, data protection through integrity and anonymity features. The enhanced security features (as given below) are well suited for providing a secure M2M communications network using the CDMA2000 systems. The 3G based enhanced security features that would help in creating a secure working atmosphere for M2M communications are:

- Enable authentication
- Ensure end-to-end network security
- Prevent cloning
- Eliminate eavesdropping
- Preclude message interception
- Provide anonymity
- Guarantee message integrity and
- Safeguard privacy

Other important security measures that need special attention with M2M communications are:

1. Secure connection of the M2M devices or applications with a M2M Application Server in the network (e.g., at the M2M customer premises).
2. Ability to perform secure and remote management of the deployed M2M devices, as some of them may not be easily accessible.
3. M2M device initiatilization, and provisioning has to be done in a secure environment.
4. Security of the unattended M2M devices with removable UIM or smartcards as they are more prone to theft and reuse on other devices.
5. If each M2M device needs to be given a unique addresses, such as mobile directory number and IPv4 addresses, there can be an address exhaustion issue soon because of the limited address space with these addresses.
6. Secure provision needed for software and/or security credential upgrades and also for remote device configuration.

4.2.1 M2M Device Security measures

M2M devices might use a smartcards for authenticating to the CDMA2000 network. Since many of M2M terminals might be installed outside and not be monitored in real time, use of a removable smartcard for storing subscription information would create security issues. Therefore, use of smartcards for storing subscription information should be avoided. In cases where the use of smartcards with M2M devices is unavoidable, it might be required to develop a mechanism to prevent theft, tampering with subscription credentials and misuse of subscription information. In order to support such a functionality, an M2M specific smartcard (M2M Form Factor smartcard) was standardized in ETSI Smart Card Platform (SCP) group and can be used with M2M devices for authenticating to the CDMA2000 network.

5 Conclusions & Recommendations

CDMA2000 standards support comprehensive set of security provisions to address modern security threats that arises with wireless communication. However, the implementation of many of the standards based security provisions in CDMA2000 networks is left to service providers' choice. Therefore, operators should carefully consider the security threats in their network and implement the security provisions in their networks. Recommendations are given below to help operators implement some of the available security provisions.

5.1 Authentication recommendations for 1X

Whether authentication must be enforced by the visited network should be agreed upon and specified in the roaming agreement between roaming partners. The following recommendations are offered for authentication:

- Global challenges provide rapid authentication of any roaming device attempting to access the visited network. The network should still be configured to require authentication using unique challenges. Global challenge mechanism is not an alternative to performing unique challenge.
- Validation of COUNT during global challenge authentication provides a mechanism for detecting cloned mobile stations, especially when SSD and/or A-key value compromise is being suspected.
- Local authentication reduces signaling between the home and visited systems and minimizes call setup delay during authentication.
- Perform an SSD update when activating a new device to ensure that any device with a default SSD value of zero is updated with an SSD value based on the ESN/pESN, A-key, and RANDSSD. Home network should also be configured to automatically trigger SSD update periodically.
- While a COUNT mismatch does not definitively indicate that an device is a clone, large discrepancies or repeated mismatches should trigger fraud procedures
- Trigger a unique challenge when a cloned device is suspected as it allows the specific device to be challenged to ensure that it possess correct SSD
- Trigger an SSD update if cloning is still suspected after a unique challenge, because a cloned device is still suspected after a successful unique challenge, the SSD update process should be used to limit the service provider's exposure in case the device is a clone using valid SSD and/or A-key information
- Ensure that roaming partner denies service if authentication fails as many equipment manufacturers provide service providers with a configurable field to either deny or allow service to a user when authentication fails and if authentication fails, service should be denied

Authentication process with SSD update procedures is strongly recommended and Shared SSD should be used in the network to minimize signaling load between MSC / VLR and HLR/AC. Authentication is recommended to be carried out preferably on (i) Registration (ii) Call Origination and (iii) on Flash Requests (assuming 3 in number per subscriber in a busy hour (BH) - using 1 Flash request per subscriber in a BH). Thus a total of maximum of 6 to 7 authentications is a reasonable compromise per subscriber in a BH from an additional load point of view. Cloning Fraud is thus preventable and hence can protect revenue if the security features and procedures are enabled in the network and implemented correctly.

5.2 Authentication recommendations for 1xEV-DO

For new EV-DO networks with no legacy EV-DO subscriptions and also for networks without AT hardware ID verification requirement, it is recommended to use unique NAI and password for new subscriptions. Further, it is recommended that the AN-AAA be configured not to perform the hardware ID verification as an alternative to authentication. The service provider should also review procedures for NAI and shared secret distribution with the handset or smartcard vendor and finalize procedures that minimize the probability of leaked credentials during or after distribution.

With existing networks that rely on hardware ID verification for providing service, the service provider should switch all existing devices in the network to use unique NAI and strong unique passwords and configure their AN and the AN-AAA to require authentication. If the service provider feels disabling the hardware ID check for existing subscriptions is not safe, it is recommended that they disable hardware ID check at least for all new R-UIM subscriptions. All new R-UIM subscriptions should use unique NAI and strong unique passwords. This means the AN-AAA may be required to turn off hardware ID check selectively for different subscriptions based on the user profile of the individual subscriber.

By ensuring that the NAI and CHAP Shared Secret for EV-DO access authentication are unique for each subscription (just as an A-key is unique for each 1X subscription), service providers can prevent any fraud related to data services.

5.3 Conclusions

The Cellular Authentication and Voice Encryption (CAVE) algorithm based authentication and encryption procedures available for early versions of the CDMA2000 1X networks (Rel 0). More sophisticated and more robust security procedures (on par with 3G/4G networks of the 3GPP world) based on Authentication and Key Agreement (AKA) algorithm are also available now in CDMA2000 1X networks (Rel C onwards) for authentication, integrity & anonymity protection, encryption. Larger length security keys (128 bit instead of 64 bit) and mutual authentication

provisions are the new additions in the later releases of CDMA2000 1X systems. Apart from the above security measures, the CDMA2000 systems, due to their spread spectrum characteristics, would inherently offers resistance against Jamming and other denial of service kind of security threats. The operators are required to take special measures to keep the A-key/Device ID pair information very safely and securely.

The CDMA2000 1xEV-DO systems use three types of authentication procedures such as device authentication, subscription authentication and message authentication for integrity protection while transmission in the air interface. 3GPP2 standards mainly talks about the air interface encryption using the session key based encryption keys and the operators have to implement other encryption provisions such as the IPsec & any other tunneling protocols for protecting traffic within the core network side. The operators are required to take special measures to keep the unique NAI and CHAP shared secret information very safely and securely. In EV-DO systems, the session key exchange between the device and the network is performed using the Diffe-Hellman key change algorithm.

The new developments such as CDMA2000 based Femtocell deployment for home/enterprise coverage/capacity solutions as well as usage of CDMA2000 systems for M2M communications etc., need additional security measures. When an operator considers deploying Femtocells in their network, they should first install a security gateway to provide security functionality for the femtocells' access to CDMA2000 core network. New security provisions are to be taken to authenticate the femtocell with the CDMA2000 network as well as passing on the security related information to the CDMA2000 network from the devices that are attached to the femto.

With possible drastic increase in the number of M2M devices in the CDMA2000 network and also due to the basic need for good security and privacy for M2M connections, special security measures are to be taken by the CDMA2000 operators to curb the fraudulent operations, such as eavesdropping, cloning, message interception, subscription fraud etc. Additional security measures such as preventing the use of stolen R-UIM cards of M2M devices, secure remote provisioning of M2M devices etc., are also to be taken.