CDMA NETWORK SECURITY

VERIZON WIRELESS WHITE PAPER

verizonwireless

CONTENTS

1. INTRODUCTION

As wireless data networks become increasingly prevalent, new possibilities and challenges continue to emerge. Security becomes key to delivering solutions that meet today's demand for mobility. Verizon Wireless has been at the forefront of offering secure wireless broadband solutions that minimize the security risk to personal and corporate data. Verizon Wireless implements many aspects of innovative and commercially available methods for securing data.

This document focuses on secure mobile data—the Verizon Wireless mobile data network features that enable mobile users to enjoy secure access to hosted and enterprise-wide applications. Voice services are not covered.

2. SECURITY OVERVIEW

Protecting corporate network assets is an ongoing task for IT professionals. Increased worker mobility and mobile workers' needs for immediate, secure access to critical business information add challenges to maintaining network security. Mobility benefits all, but it can introduce security risks.

Some of today's top security issues and concerns are:

- Unauthorized systems and network access
- Auditability and compliance
- Customer data breaches
- Internal and external sabotage
- Theft of intellectual property and confidential business information
- Cost of mobile device administration

The following diagram illustrates many elements critical to mobile data security.

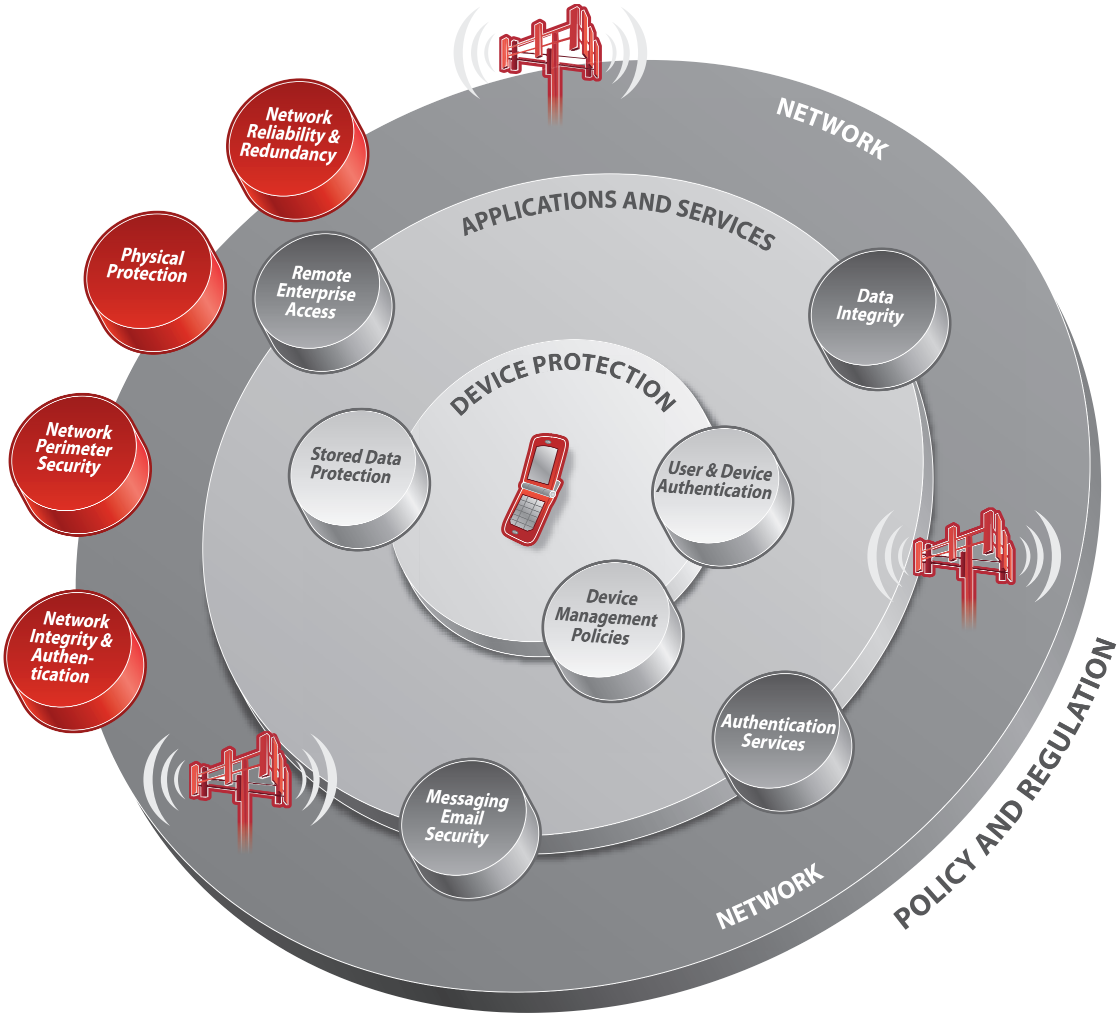

Figure 1: The different layers of mobile data security.

This white paper explains the security features, capabilities, and benefits of the following areas in the Verizon Wireless mobile data network:

- Air interface
- Access network
- Core network
- Transport
- Perimeter
- Endpoint

3. CDMA NETWORK AND TECHNOLOGY OVERVIEW

The core network of the Verizon Wireless mobile data network has many of the same components found in a typical corporate network, and managing these components requires similar techniques and practices that IT professionals commonly use in their own networks. The difference between the Verizon Wireless mobile data network and a typical network is found in the access network. It's in the access network where users are granted entry into the overall mobile network and where maintaining high security and access protocols become paramount.

The following diagram illustrates a simplified view of the Verizon Wireless CDMA2000 1x data network containing both 1xRTT and 1xEV-DO data structures. The Verizon Wireless mobile data network has two parts: the access network and the core network.

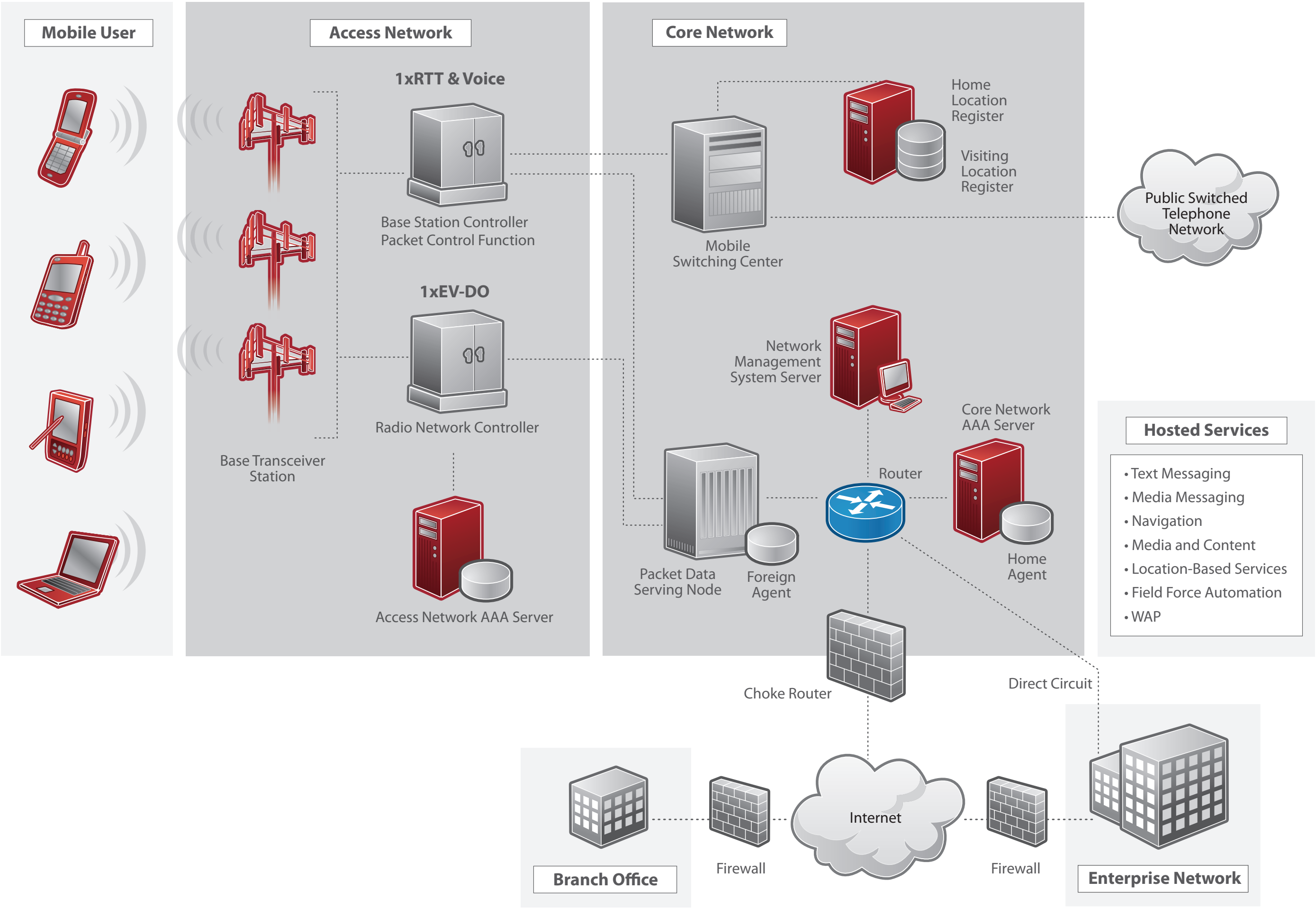

Figure 2: A simplified CDMA2000 1x data network showing 1xRTT and 1xEV-DO data structures.

3.1 CDMA2000 1xRTT and 1xEV-DO

Over time, more and more demands have been made on the capabilities of corporate networks. Workers want more mobility; secure, high-speed access; and an extension of applications across the enterprise, all of which can strain current IT capabilities.

Verizon Wireless understands these demands and has constantly improved its mobile data network to offer increased mobility, access, and applications. This process is ongoing, but it pays to see what's happened before to gain a greater appreciation of the capabilities of today's mobile data network.

Second-generation (2G) CDMA-based wireless networks, known as cdmaOne, have proved their effectiveness in delivering high-quality voice traffic to subscribers.

In response to subscriber growth and demand for data services that require high-speed access, the third-generation (3G) wireless networks, known as CDMA2000 and comprising 1xRTT and 1xEV-DO, were implemented.

The first phase of CDMA2000 is called 1xRTT. 1xRTT provides maximum theoretical data rates of 144 Kbps (downlink) and 144 Kbps (uplink), as well as twice the voice capacity of cdmaOne on a single 1.25-MHz CDMA channel.

1xEV-DO Revision 0 (Rev. 0) increases the downlink maximum theoretical data rate to 2.4 Mbps, with an average data rate between 400 and 700 Kbps. The average uplink data rate is between 60 and 80 Kbps.

1xEV-DO Revision A (Rev. A) supports Quality of Service (QoS), converges IP services and VoIP, reduces latency, increases the maximum theoretical downlink speed to 3.1 Mbps (average 600–1400 Kbps), and boosts the maximum theoretical uplink speed to 1.8 Mbps (average 500–800 Kbps). The entire Verizon Wireless EV-DO data network is now Rev.A-enabled.

3.2 Mobile Stations

Mobile subscribers access the CDMA2000 1x data network using a mobile station, such as a mobile phone, modem, a laptop with an embedded CDMA2000 chip, a broadband access wireless router, or PC Card on a laptop computer. Mobile stations allow mobile users to access Verizon Wireless-hosted services, the Internet, or enterprise services.

The mobile station interacts with the access network (AN) to obtain radio resources in order to exchange data packets. The mobile station, in tethered mode, can also act as a modem for a computer.

The mobile station automatically registers with the network upon power-up, and upon successful registration, it is ready for voice and data calls.

3.3 Access Network

There are two types of access networks: 1xRTT and 1xEV-DO. The AN is the mobile station's entry point into the mobile network and maintains the communications link between the mobile station and the core network. The access network facilitates security by allowing only authorized mobile stations to access the network. The AN is composed of the following elements:

Base Transceiver Station

The base transceiver station (BTS) is physically composed of antennas and towers. The BTS manages radio resources including radio channel assignment and transmit and receive power management and acts as the interface to mobile stations.

Packet Control Function

The packet control function (PCF) maintains the "connection state" between the access network and mobile stations, buffers packets when necessary, and relays packets between mobile stations and the PDSN.

Radio Network Controller/Base Station Controller

The radio network controller for 1xEV-DO and the base station controller for 1xRTT schedule packet transmission on the air interface and manage handoffs between BTSs. For 1xEV-DO, security functionality is maintained by the security sublayer in the RNC. Security functionality is performed by either the BTS or the RNC, or by both.

3.4 Core Network

The core network acts as the gateway between the access network and the Internet or enterprise private networks. It provides authentication, authorization, and accounting (AAA) services, provides access to network services, IP mobility, and manages IP addresses. The core network comprises the following elements:

PDSN/Foreign Agent

The PDSN is the gateway between the access network and the core network. The PDSN terminates PPP for mobile stations. The PDSN handles authentication and authorization for access to packet services and records packet billing information in conjunction with the AAA. The foreign agent handles packet routing and encryption (between the foreign agent and the home agent) for mobile IP subscribers.

AAA/Home Agent

The AAA and the home agent (HA) are used for authentication, authorization, and accounting for data services. The AAA/HA stores and records usage and access information for billing and invoicing purposes. The HA facilitates data roaming into other carrier networks by providing a mobile IP address for mobile stations, and by forwarding traffic to/from mobile stations. It maintains registration information and supports dynamic assignment IP addresses with the AAA.

Direct Circuit Connections

Verizon Wireless provides a direct circuit connection (a "private network") for business customers to directly connect between the company's enterprise network and the Verizon Wireless fixed end systems. This direct circuit lets companies communicate with their mobile workforces with increased data response times and lower latency, while reducing concerns over security and reliability. Overall connection reliability improves, because companies avoid having to traverse the Internet. As a result, security threats are more contained.

4. SECURITY IN CALL SETUP

This section briefly describes CDMA 1xRTT and 1xEV-DO. It introduces the idea of a call setup, procedures involved, and the differences in call setup for 1xRTT and 1xEV-DO. A mobile station is used to illustrate call setup.

4.1 1xRTT Autonomous Registration Authentication

Successful autonomous registration authentication is diagrammed in Figure 3. The authentication sequence comprises 15 steps and focuses on the major protocol exchanges that begin with authentication between the mobile station (MS) and the base station controller (BSC).

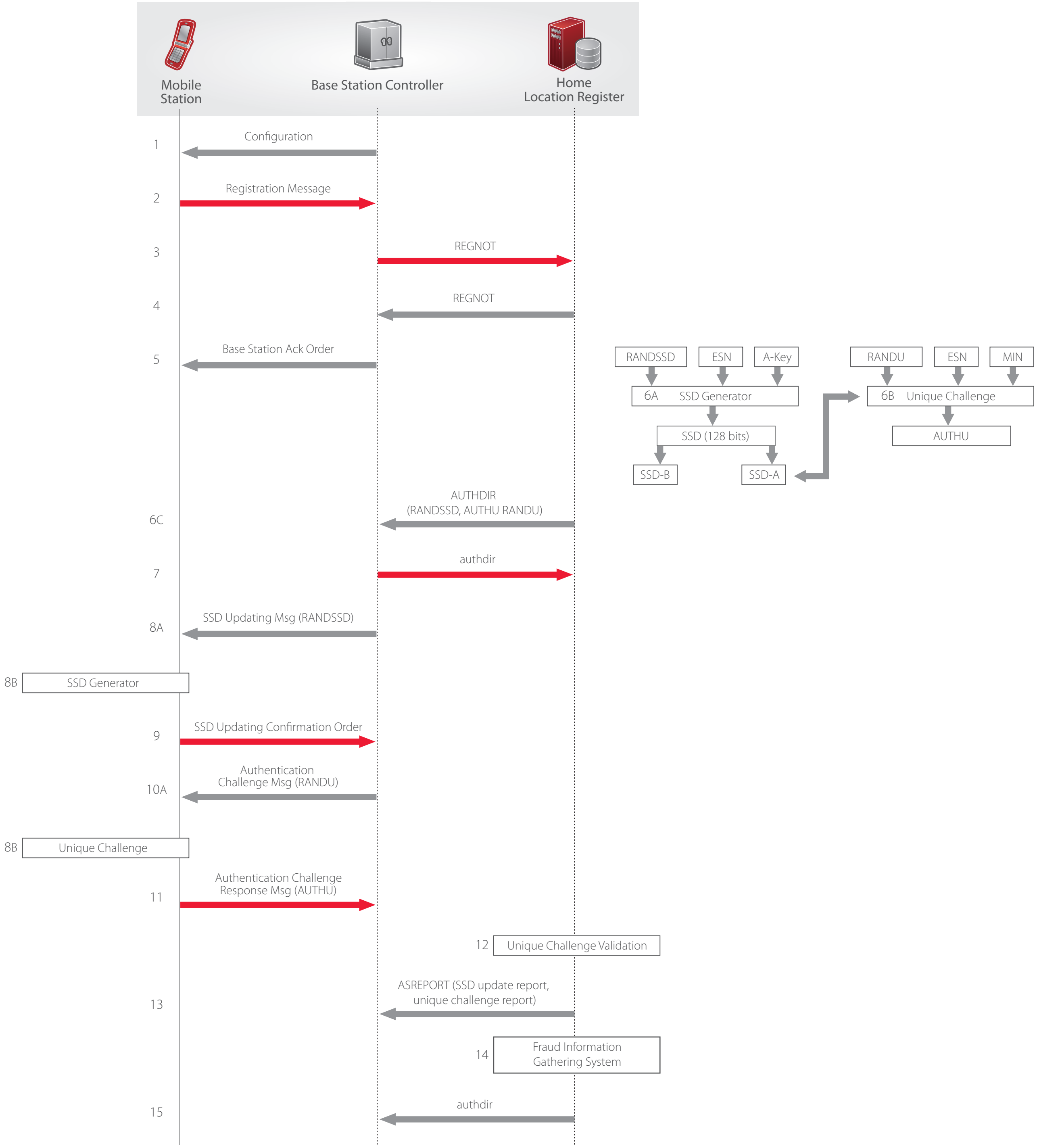

Figure 3: 1xRTT Autonomous Registration Authentication.

1. MS acquires the system, collecting a complete set of configuration messages before it is allowed to operate on the system. The BS tells all mobiles when they should register in the System Parameters Message (one of the messages in the set of configuration messages).

2. MS notices that it is obligated to register and so transmits a Registration Message.

3. The serving-system mobile switching center (MSC) or visitor location register (VLR) issues the ANSI-41 Registration Notification (REGNOT) Message for MS service qualification.

4. The home location register (HLR) responds with the REGNOT Result including the MS services profile.

5. Upon successful validation of service qualification in the REGNOT message, the BS confirms the MS's registration was successful with a Base Station Acknowledgment Message.

6.

   a. Upon receipt of REGNOT in step 3 above, the Authentication Center (AC), based on its internal authentication algorithms, initiates the SSD Update process. The first step is executing the Cellular Authentication and Voice Encryption (CAVE) algorithm using the MS's authentication key (A-Key), electronic serial number (ESN), and a random number, called the Random Variable SSD (RANDSSD). The result is the new, "pending' SSD subkey. The SSD has two parts: SSD-A (used for authentication) and SSD-B (used for session key derivation).

   b. The AC then selects RANDU (Unique Challenge) and calculates unique challenge authentication signature (AUTHU). AUTHU is calculated by executing the CAVE algorithm again using the SSD-A (lower 64 bits of the SSD) RANDU, ESN, and mobile identifier number (MIN). The SSD Update process occurs in parallel with the registration process.

   c. ANSI-41 AuthenticationDirective Invoke message (AUTHDIR) is used to transfer the [RANDSSD, RANDU, AUTHU] triplet from the AC to the VLR or serving MSC.

7. The serving system acknowledges the SSD update request by sending the ANSI-41 AUTHDIR to the AC.

8.

   a. The BS sends an SSD Update Message, including the RANDSSD, to the MS.

   b. The MS extracts the RANDSSD and independently computes the SSD.

9. The MS sends the SSD Update Confirmation Order confirming SSD update.

10. The BS executes a unique challenge by sending an Authentication Challenge Message including the RANDU.

    a. The MS extracts the RANDU and independently computes the AUTHU.

11. The MS returns the calculated AUTHU in the Authentication Challenge Response Message.

12. The serving system completes the unique challenge by validating whether the mobile station successfully completed the unique challenge.

13. Serving MSC/VLR sends a report, including the SSD update and unique challenge results, to the AC in the ANSI-41 ASREPORT message.

14. The HLR/AC verifies that the information in the ASREPORT is the expected result. If not, the HLR/AC forwards the information to a Fraud Information Gathering System (FIGS) for use in determining fraudulent activity.

15. The AC acknowledges the authentication report by sending the ANSI-41 ASREPORT to the VLR.

4.2 EV-DO Access Authentication

This section explains the process of how EV-DO access is granted and authenticated.

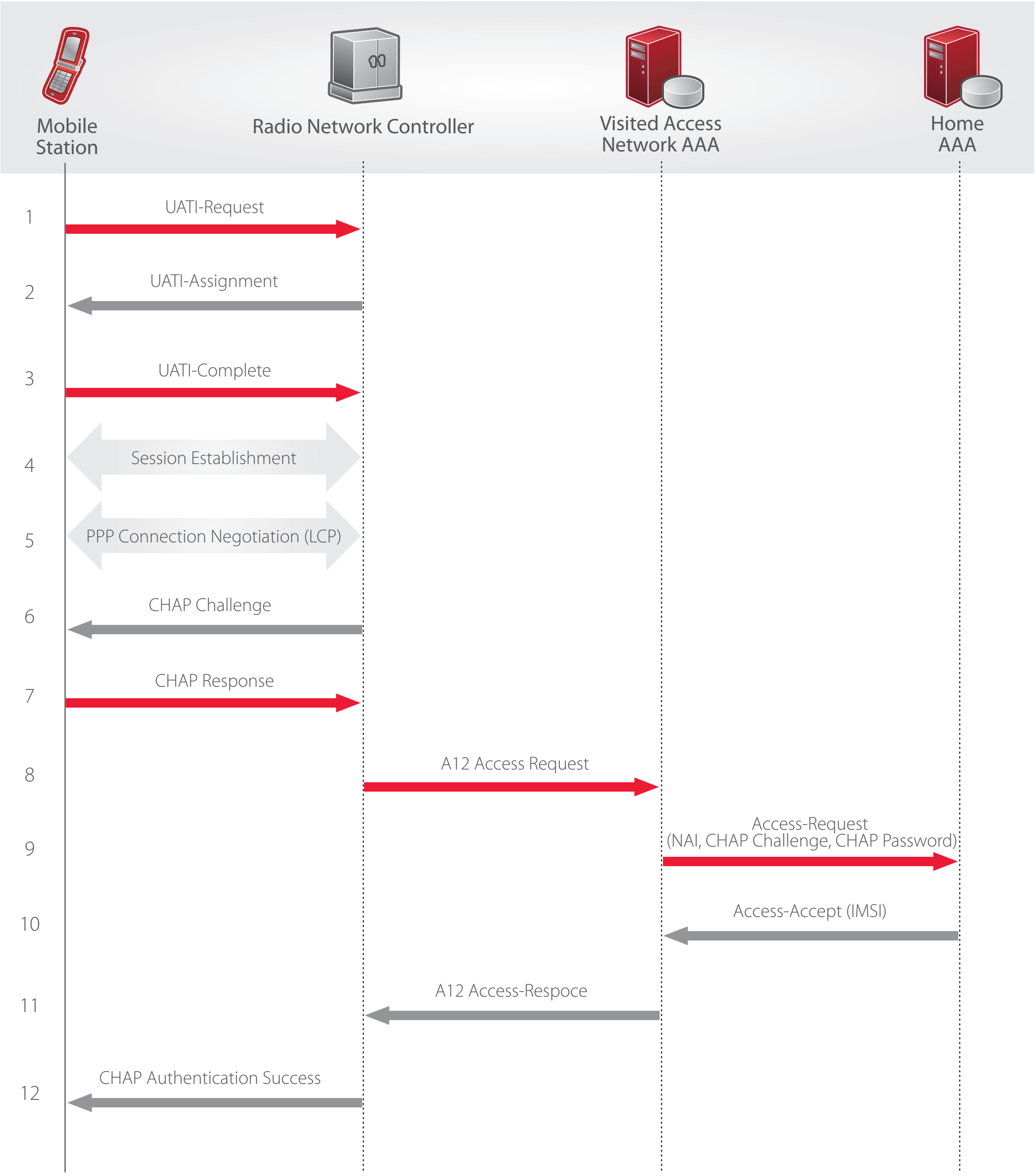

Figure 4: EVDO A12 Authentication.

1. The mobile node (MN) sends a Unicast Access Terminal Identifier (UATI)-Request.

2. The RNC assigns UATI.

3. UATI assignment is completed.

4. The EV-DO session is set up between the MN and RNC.

5. PPP/Link Control Protocol (LCP) negotiation completes between the MN and the RNC.

6. The RNC sends a Challenge-Handshake Authentication Protocol (CHAP) challenge to the MN.

7. The MN calculates a response based on the A12 CHAP key and includes this along with the A12 Network Access Identifier (NAI) in a CHAP response to the RNC.

8. The RNC includes the challenge and response in a Radius Access Request to the local AN-AAA server.

9. The local AN-AAA server uses the NAI to forward the message to the proper home AN-AAA server, possibly via brokers.

10. The home AN-AAA server validates the CHAP response and responds with an authorization response that may be delivered using security between foreign (visited) and home networks. If the response is valid, the home AN-AAA server returns the IMSI in the Radius Access-Accept.

11. The local AN-AAA server forwards the response to the RNC.

12. The RNC informs the MN of the A12 authentication result. The PPP link is terminated after A12 authentication.

4.3 Mobile IP (Public Network) or Enterprise Home Agent (Private Network) Access

This section explains how access to a public or private network is granted and the process needed for authentication.

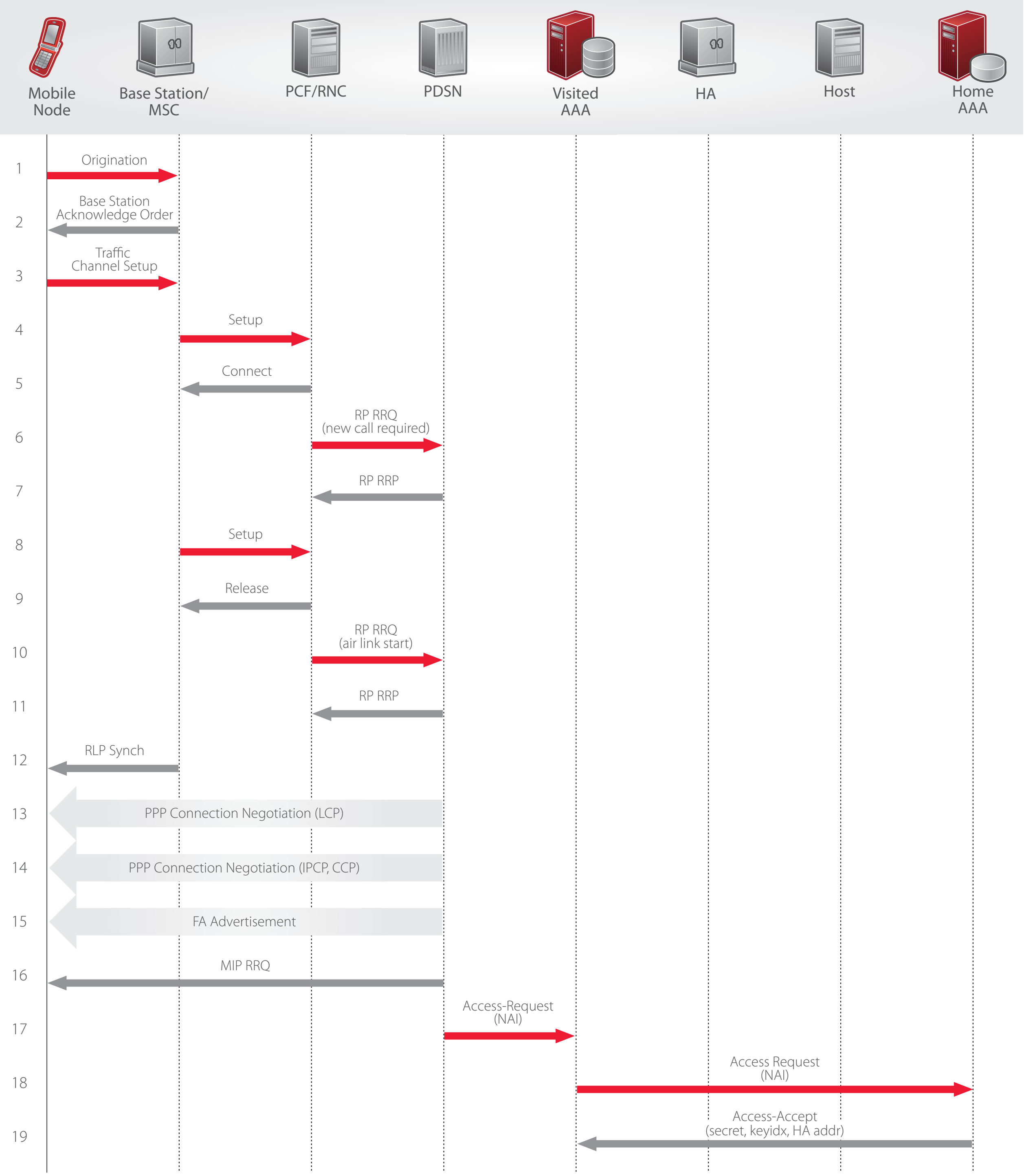

Figure 5: 3GMIPv4 Authentication.

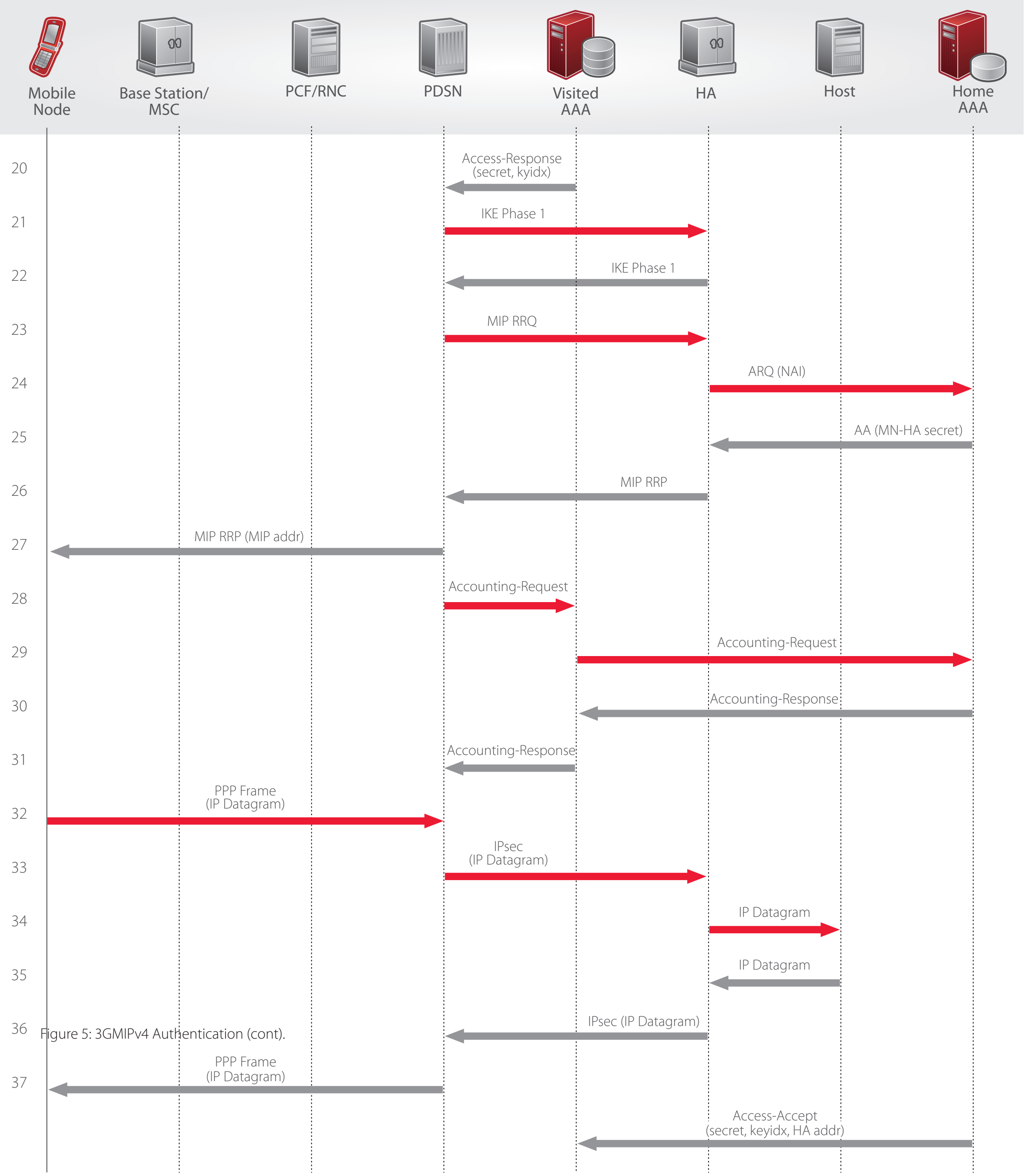

Figure 5: 3GMIPv4 Authentication (cont).

1. The MN sends an Origination Message with the Data Ready to Send (DRS) bit set to the number (1), which indicates a request to establish a traffic channel to the BS/MSC to request packet data service.

2. The BS/MSC acknowledges the receipt of the Origination Message with a Base Station Acknowledgement Order to the Mobile Station.

3. The traffic channel is set up between the MN and BS/MSC.

4. The BS/MSC sends a SETUP message to the PCF.

5. The PCF sends back a CONNECT message to BS/MSC.

6. The PCF sends a R-P request to the PDSN to establish the R-P (i.e., A10/A11 interface) connection.

7. The PDSN responds to the PCF connection request and the A10/A11 connection is established.

8. The BS/MSC sends a second SETUP message to provide "airlink start" accounting information.

9. The second RELEASE message to the BS/MSC is required to acknowledge the above SETUP message. In this case the RELEASE message does not "release" any resources.

10. The PCF sends an R-P Registration Request RRQ message to the PDSN containing "airlink start" accounting information.

11. The PDSN records the accounting information and responds back to the PCF with the R-P Registration Response RRP message.

12. The BS/MSC sends a Radio Link Protocol RLP synchronization message to the MN.

13. A PPP session is established between the MN and the PDSN.

14. PPP negotiation completes. IP Control Protocol (IPCP) configures a simple IP address or rejects IPCP IP address configuration to indicate mobile IP service is requested (versus simple IP service).

15. After PPP initialization, the PDSN sends Foreign Agent Challenge (FAC) extension advertisements to the mobile station. The mobile station may send an agent solicitation message to the PDSN/foreign agent following PPP initialization.

16. The mobile station generates a mobile IP registration request containing four MIPv4 extensions: NAI, MN-HA Authentication, FAC, and MN-AAA Authentication Extension. In this example we assume the user is requesting a secure reverse tunnel (see steps 33 and 36) as part of the MIP RRQ message.

17. Using the NAI, the RADIUS protocol, the PDSN sends an authentication request to the local AAA. This request includes the MN NAI, MN-AAA authentication, and FAC/HA address (if any), as well as other information.

18. The local AAA server uses the NAI to forward the message to the proper home AAA server, possibly via brokers.

19. The home AAA responds with an authorization response that may be delivered using security between foreign (visited) and home networks. If the MN-AAA authenticator is valid, the home AAA returns the FA-HA secret key and key index in the Radius Access-Accept.

20. The local AAA forwards the response to the PDSN.

21. The PDSN sets up a security association with the HA (if one does not already exist) with an Internet Key Exchange (IKE) pre-shared secret. Note: The IKE pre-shared secret can be dynamically configured as per IS-835 (distributed by the Home RADIUS server) or statically configured.

22. The HA acknowledges and responds to the IKE exchange.

23. The PDSN sends the mobile IP RRQ to the HA. If the Mobile Station wants to use its static Home Address (or the Mobile Station already has a mobile IP address and the same mobile IP session is being continued), the Mobile includes the IP Address as the MIP RRQ (step 16) home address. If the Mobile Station wants a dynamic home address, it sets the home address to zero (0.0.0.0). Thus, in this case the HA field of the mobile IP RRQ is set to zero (0.0.0.0).

24. The HA requests the MN-HA key from the AAA.

25. The AAA returns the MN-HA secret key corresponding to the NAI in an Access-Accept (on a secure channel).

26. The HA validates the MN-HA authenticator. If valid, the HA responds with a mobile IP RRP Message, and if requested, provides a dynamic IP address for the MN. Otherwise, the supplied address offered in the MIPv4 RRQ is accepted.

27. The PDSN sends the RRP to the MS after recording the reply in the visitor entry list.

28. The PDSN sends an accounting start to the AAA server (which may forward the message to the AAA via optional brokers).

29. For roaming services, the local AAA server forwards the accounting start to the remote AAA server.

30. The remote AAA server records the accounting start and responds back to the local AAA server.

31. The local AAA server forwards the accounting response to the PDSN.

32. User data flows from the MS over the PPP link to the PDSN.

33. User data flows in the IPSec tunnel between the PDSN and the HA.

34. User data flows in an IP packet from the HA to the host.

35. User data flows in an IP packet from the host to the HA.

36. User data flows over the IPSec tunnel between the HA and the PDSN.

37. The PPP Packet flows from the PDSN to the MS.

The PPP link can be terminated at any time. The PPP link can be terminated by the user, authentication failure, or loss of carrier, etc., as described in the PPP protocol. In addition, the mobile station periodically refreshes the registration with the PDSN based on the lifetime value in the RRP message. The mobile station is allowed to periodically refresh or in effect extend the registration lifetime by sending agent solicitations.

5. AIR INTERFACE (PHYSICAL LAYER)

Mobile stations rely on radio technology to access the network. Security is of concern when using radio technology, but with the advances in radio technology, several air interface security mechanisms have been developed to keep signals secure while increasing access capability.

5.1 Air Interface Technologies

Modern radio systems typically divide their allotted radio spectrum by two factors—time or frequency—allowing multiple connections to occur. The different methods of dividing radio spectrum to accommodate lots of connections are called multiple-access schemes.

Dividing radio spectrum by time lets each connection (in all or part of the allotted spectrum) use a specific time slot and is called Time Division Multiple Access (TDMA). Using TDMA, multiple connections are separated from each other in time.

Dividing the radio spectrum by frequency allows each connection (in all or part of the allotted spectrum) to have access to the radio spectrum all of the time and is called Frequency Division Multiple Access (FDMA). Using FDMA, multiple connections are separated from each other by different frequencies.

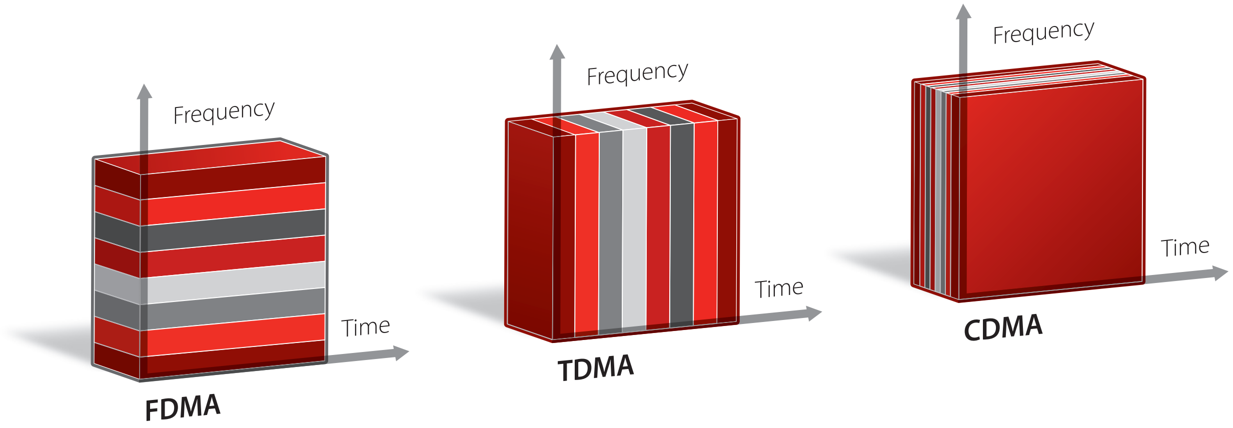

Figure 6: A comparison of radio spectrum division techniques.

Another way to give multiple access to radio spectrum is to divide the spectrum up using unique codes. Each connection has access to the radio spectrum all of the time, but uses a unique code to separate connections. This is called Code Division Multiple Access (CDMA). CDMA provides exclusive rights to a unique code for the duration of the connection, avoiding simultaneous connections from having the same code. This method grants greater network access while offering enhanced network security.

5.2 CDMA Air Interface Security Benefits

CDMA has inherent security benefits that TDMA and FDMA multiple-access schemes do not have. To understand the inherent security benefits of CDMA, it is necessary to understand how direct-sequence spread-spectrum (DSSS) technology works. DSSS technology employs techniques that deliberately distribute or "spread" data over a frequency domain.

DSSS works by multiplying user data by a pseudo-random noise (PN) sequence composed of 1 and -1 values. A PN sequence is a statistically random sequence that is multiplied at a much higher data rate or chip rate expressed in chips per second (cps), with the slower user data expressed in bits per second (bps). This multiplication is done at the radio baseband level prior to actual transmission over the air link. The output of these multiplied signals is a new signal that is randomly spread over a wide frequency band determined by the chip rate and PN sequence length.

The new signal resembles white noise when transmitted over the air link, except that it can be filtered out by the receiving radio. The receiver multiplies the received signal with the same synchronized PN sequence, yielding the original user data (1 x 1 = 1 and -1 x -1 = 1). This process completely separates the original user data from the received signal and is called "despreading."

Because the despread process is the same as the spread process, it is possible that jamming signals introduced into the radio channel will also be spread before despreading is performed. This reduces the susceptibility of CDMA to jamming and interference and makes it less likely a connection or call will be knocked off the air.

Because each connection or call is encoded with a unique PN sequence, multiple users can share a single frequency band or channel. Each connection or call is kept isolated from others via PN sequence codes. CDMA2000 uses different PN sequences or encoding types in the generation of both the uplink and downlink sides of each connection. There are over 4.4 trillion different PN code combinations, making it very difficult to intercept a specific connection's PN sequence. These PN codes also change regularly to make code interception very difficult. As an added benefit, PN sequences allow for increased network access while increasing overall network security.

The following diagram briefly describes how user data from the CDMA network is transmitted from a base station to a mobile station (the downlink side of a connection). A similar process occurs on the uplink side of the connection when the mobile station sends data to the network. The difference between downlink and uplink sides is that different PN sequences and codes are used for each half of the connection or call.

Within the mobile station, the process is reversed. The received signals are quantized into bits or chips by an analog-to-digital converter (ADC). The output of the ADC is run through the Walsh code and PN

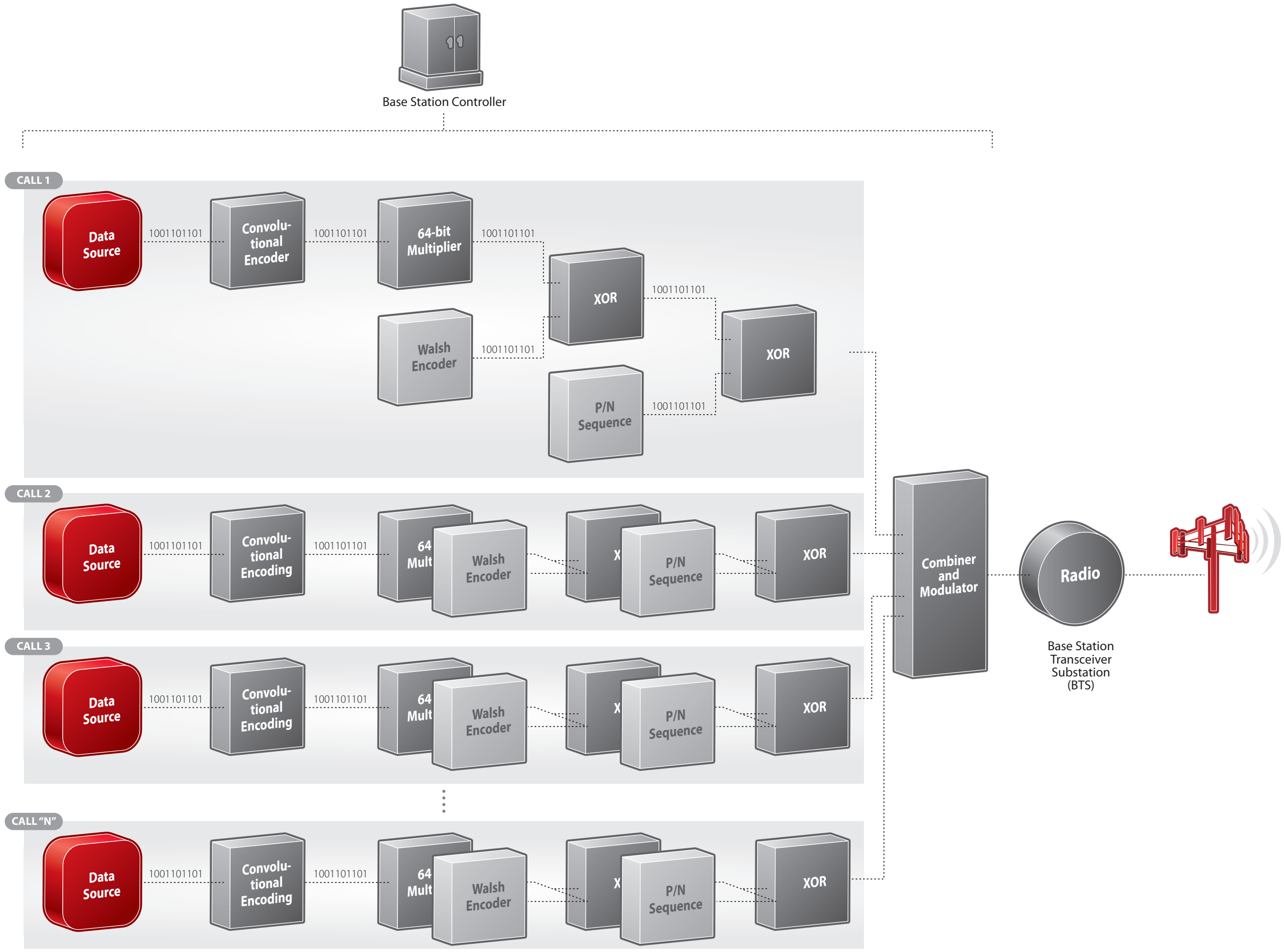

Figure 7: Base Station Controller encoding block diagram.

In the previous illustration, user-data output is doubled by a convolutional encoder that adds redundancy for error-checking purposes. Each bit from the output of the convolutional encoder is replicated 64 times and "exclusive or'd" (generally symbolized by XOR) with a Walsh code that is exclusive to that connection. The output of the Walsh code is then exclusive or'd with a PN sequence that is used to identify all of the connections or calls within a particular cell's sector. At this point, there are 128 times as many bits as there were in the original user data. All of the connections or calls for that cell's sector are then combined and modulated onto a carrier frequency.

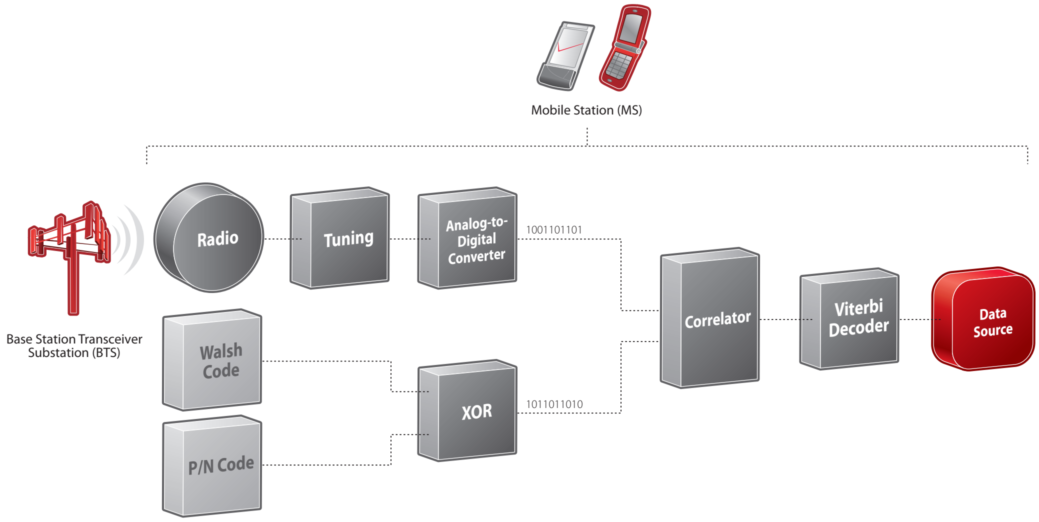

Figure 8: Mobile station decoding block diagram.

sequence correlation receiver to recover the transmitted bits of information from the original user data. Once about 20 ms of data is received, a Viterbi decoder is able to decode the convolutionally encoded data and correct any errors.

Because the uplink and downlink sides of a connection use different encoding methods, this encoding scheme makes it much more difficult to demodulate these already hard-to-detect, noise-like signals, thereby increasing overall network security.

The low probability of interception, demodulation difficulty, and anti-jamming/interference benefits of DSSS CDMA technologies are why the military has used it for so many years. This is also why CDMA technology is inherently more secure than competing wireless technologies.

The key inherent security benefits of CDMA technology can be summarized as:

- CDMA codes inherently spread the signals across the full channel bandwidth of 1.25 MHz.
- Soft handoff (multiple cells simultaneously supporting the call) typical for the CDMA operation make it very difficult to "follow" the CDMA cellular call.
- Long code mask (LCM) provides "built-in" security at the physical layer.
- CDMA signals are very difficult to intercept.
- CDMA attacks require sophisticated and expensive equipment.
- Access is only provided to authenticated mobile stations/subscribers.

6. ACCESS NETWORK (LAYER 2)

The access layer is critical for security because it is where access to the network is granted. Devices and users must be authenticated, creating a layer of security in accessing the wireless network.

6.1 1xRTT Device and Subscriber Authentication

1xRTT authenticates device identity and subscriber identity using three components: A-key (secret value), MIN, and ESN. For example, if someone tries to steal a mobile station and sell it, Verizon Wireless can track the subsequent usage of this mobile station, reducing the incentive to steal devices.

To authenticate, the MSC sends a random binary number (RANDSSD) to all the mobile stations in its service area. Mobile stations use the CAVE algorithm, A-Key, ESN, and MIN to generate SSD and forward it to the MSC. The network authentication center generates SSD using the same set of authentication inputs.

If the signatures of the authentication center and the mobile station match, the MSC is informed of the successful authentication and both the ESN (device) and MIN/IMSI (subscriber) are authenticated. If they do not match, then access to the mobile station is denied and its user is shut off from network access.

In CDMA, identity information is sent on the access channel. Test equipment may be available that is capable of monitoring the CDMA access channel, thereby obtaining the phone identity information.

To deter this, the CDMA standards provide a mechanism for eliminating the transmission of phone identification data over the air. This mechanism involves the assignment of a Temporary Mobile Station Identifier (TMSI) to the mobile station that is used, instead of the permanent mobile station identifiers. Because the mobile station does not transmit permanent identifiers, they cannot be obtained by intercepting transmissions.

6.2 1xEV-DO Access Authentication

Subscriber authentication grants users access to common network services and prevents unwanted intrusions from taking place.

Access authentication between an EV-DO mobile station and RNC takes place when the AT initiates the PPP connection. Access authentication does not require any user interactions and uses CHAP and MD5. It requires that the AT supports the MD5 algorithm and saves the A12 NAI and authentication keys. The RNC obtains the subscriber-specific NAI, authentication keys (passwords), and IMSI from the AAA via the A12 interface.

7. CORE NETWORK

The Verizon Wireless mobile data network uses authentication protocols to establish a user's identity before network access is granted. Verizon Wireless follows many of the established security and access procedures implemented by many IT organizations. This section will cover those topics, plus common network services such as IP addresses, and roaming.

7.1 User Authentication and Authorization

Once a subscriber is authenticated on the access network, he or she is authenticated for IP services using CHAP with the PDSN, during PPP establishment between the mobile station and the PDSN. The reason for authenticating subscribers at the packet data level (e.g., core network) is to provide differentiated services to Internet users and mobile subscribers. The subscriber profile in the AAA defines which services the subscriber is authorized to access.

7.2 IP Management

Verizon Wireless offers a variety of IP addressing options that provide differing levels of accessibility, protection, and manageability. These options are designed to provide customers with a variety of choices, so that customers can choose an IP addressing scheme that is appropriate for their needs.

For example, a mobile user who needs to access the Internet or connect to the enterprise network via VPN from the mobile station (i.e., mobile-originated data connection) would need an Internet accessible or unrestricted IP address (e.g., a dynamic or static public IP address).

Connectivity Options

Options	Benefit	Consideration
VPN	▪ Low cost ▪ Secure ▪ Low redundancy	Not all VPN vendors are supported.
Single-frame relay	▪ Secure ▪ Full routing control	Requires static or BGP routing. Verizon Wireless strongly suggests that customers implement access control policies to protect their networks.
Dual-frame relay (to different Verizon Wireless locations)	▪ Secure ▪ Redundant ▪ Full routing control	Requires static or BGP routing. Verizon Wireless strongly suggests that customers implement access control policies to protect their networks.
Multiple direct circuits	▪ Secure ▪ Some redundancy ▪ MLPPP (required if static)	Requires static or BGP routing. Verizon Wireless strongly suggests that customers implement access control policies to protect their networks.

Note: Please contact a Verizon Wireless sales representative for pricing options.

Dynamic Public IP Address

With a dynamic public IP address, a mobile station has access to the Internet. Because the IP address is public, there is no need to NAT or proxy data to/from the mobile station. Push applications, or mobile-terminated data, are supported. Mobile stations in the "general dynamic protected IP address" pool are protected from unsolicited Internet traffic, but allow traffic from Verizon Wireless push applications such as **VZ**Email®.

Static Public IP Address

With a static public IP address, a mobile station gets the same IP address each time it registers with the network. Mobile stations with unrestricted static public IP addresses have full Internet access, while mobile stations with Internet-restricted static public IP addresses cannot access the Internet. The latter alternative is important for customers looking for mobile-terminated and mobile-initiated data through a direct circuit connection.

Customer-provided IP Address

With direct circuit connections, mobile stations can be assigned customer-provided private or public IP addresses. This virtually extends the corporate LAN addressing to mobile stations, allowing IT administrators to manage mobile stations and LAN devices using the same tools and techniques. For example, the same firewall and routing schemes can be used. Traffic to/from mobile stations are tunneled securely to the enterprise network, and Internet access can be provided via the enterprise network. This makes it easier for enterprise IT administrators to manage and monitor network usage and enforce IT policies.

7.3 Dynamic Mobile IP Update

The CDMA2000 mobile IP standard was designed to incorporate cryptographic keys for MIP security. However, the standard didn't provide a secure and efficient means to distribute MIP keys to mobile stations. To that end, Verizon Wireless developed the Dynamic Mobile IP Update (DMU) standard to prevent hackers from intercepting or rerouting packets sent to legitimate users, stopping "man-in-the-middle" attacks.

The DMU standard allows manufacturers to embed public RSA encryption keys into mobile stations to enable secure distribution of mobile IP keys. The DMU standard enables stronger cryptographic keys—128-bit authentication—and stronger authentication of MIP registration messages. DMU is used to provision simple IP and mobile IP credentials, where it is used to enforce key lifetimes and establish security policies on the keys such as key length, etc. Security and protection continue even as the subscriber moves through the service area. Overall, the DMU standard adds another layer of device authentication.

7.4 Roaming

Roaming allows greater mobility through mobile access from different networks. Verizon Wireless allows its subscribers to roam on other networks operated by carriers with whom Verizon Wireless has roaming agreements without compromising security by using the same authentication mechanisms even for roaming users.

For roaming authentication, Verizon Wireless securely stores the authentication credentials on its network and doesn't share them with any network. This prevents operator fraud. In addition, authentication happens between Verizon Wireless and the mobile station, with the roaming network as a pass-through for authentication information.

8. NETWORK AVAILABILITY

Verizon Wireless has designed its wireless network to deliver America's most reliable wireless service using smart network design, networking best practices (policies, procedures and maintenance), and continuity of operations.

COOP

As part of its overall security policy, Verizon Wireless maintains a system to ensure continuity of operations (COOP) in the event of disasters or other service interruptions. This COOP system involves using back-up and redundant servers, cellular towers, and other equipment to ensure that connectivity and security are maintained throughout the network. Verizon Wireless has redundancy and automatic fail-over throughout the network such as at the BSC/RNC, PDSN, home agent, and AAA levels. The Verizon Wireless network is built for reliability, with battery back-up power at all facilities. In addition, generators are installed at all switching facilities and many cell-site locations. Portable generators can also be deployed to provide power during extended power outages.

Rapid Disaster Response

For rapid disaster response and to handle special events with large gatherings, Verizon Wireless has "Cell on Light Trucks" (COLTs) and "Cell on Wheels" (COWs) that handle voice and data services. A COLT is a 25,000-pound vehicle with two retractable masts, a microwave antenna to link network components, an emergency power generator, and a small office. COLTs are also fully equipped with emergency resources such as equipment, fuel, electrical generators, food, water, and cots. COWs are fully functional, generator-powered mobile cell sites that enhance coverage and capacity in a given area.

24/7 Network Operations Centers

Verizon Wireless has two network operations centers to monitor its nationwide network. These operations centers are in service 24 hours a day, 7 days a week. Verizon Wireless also has network and file system intrusion detection systems (IDS) in place to manage, monitor, and prevent break-ins on a 24/7 basis.

9. TRANSPORT/PERIMETER

Data communications require stringent security measures to prevent breaches and attacks. Firewalls are put into place to secure data, cryptographic measures are taken to prevent hacking or corrupting data, and direct connections such as VPNs are used to control data flow. The Verizon Wireless mobile data network uses these techniques to enhance security on its network.

9.1 Traffic Separation

Verizon Wireless uses traffic separation to keep apart operations, administration, and management (OAM); billing; and subscriber data. The network is partitioned into multiple domains to separate data traffic. Traffic separation is available for both network links and network nodes. In addition, mobile IP uses tunneling as an additional measure of traffic separation.

9.2 Direct Circuit Connection

The Verizon Wireless allows business customers to extend the enterprise network to mobile stations via direct circuit connection. In addition, mobile stations can be connected to the customer's managed services provider as well.

Enterprise networks can connect to the Verizon Wireless FES through a direct circuit connection using Frame Relay, T1, DS3, and Metro Ethernet connections. FES also supports IPSec and MPLS VPN technology. VPN services from the mobile station are also provided as needed.

A customer's mobile stations can be assigned private and public IP addresses belonging to a customer, creating a virtual extension of customer network. For example, this allows an enterprise network to reach mobile stations as if they were part of the local enterprise network.

Because these mobile stations have customer-specific IP addresses, their traffic is tunneled through Verizon Wireless's core network to an enterprise home agent (EHA) (rather than to a HA), and then forwarded to the enterprise network via the FES that is connected to the direct circuit. Thus, traffic is segregated from other wireless traffic.

Overall, direct circuit connection improves reliability and security because customer traffic is segregated and is directly transferred without having to traverse the Internet. Direct circuit connections also support roaming mobile stations.

9.3 SSL/TLS

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are standards-based protocols that allow mutual authentication between a client and server, and establishes an authenticated and encrypted connection between the client and the server. Verizon Wireless supports SSL/TLS through iBAS and MyBusiness portals and for customers using transports that use service oriented architecture, a secure environment for business process integration.

9.4 Firewalls and Choke Routers

Firewalls are a key factor in maintaining the overall security of the mobile data network. As part of a security best-practices plan, Verizon Wireless uses firewalls to partition the network into easily controllable security domains. Verizon Wireless also has firewalls on the direct circuit to enterprise networks and has choke routers to protect its Internet interface. Verizon Wireless also has application-level gateways within its network.

10. DEVICE ENDPOINT

Verizon Wireless uses a variety of techniques to provide a secure environment for mobile stations, including licensing and reselling certified third-party applications to secure smartphone and BlackBerry®-based mobile stations. These tools allow an enterprise's IT personnel to establish security policies to fit the needs of the enterprise and form a cohesive solution to protect an enterprise's data from being compromised by a noncompliant mobile station.

10.1 Initial Provisioning

Provisioning makes a mobile station functional for a subscriber. This process involves activating the mobile station, subscribing to services, and loading necessary software and applications.

To begin the process, the mobile station and subscriber credentials are authenticated. Once authenticated, software and applications can be sent OTA to the mobile station to make it compliant with the enterprise IT policy. Only services and applications allowed per the subscriber profile can be provisioned.

10.2 Device Management

Device management takes security beyond the initial setup. New applications can be sent OTA to the mobile station to keep it current with IT policies. As a mobile station is subscribed to new services, or as IT policy changes, device management allows mobile stations to be brought up to date.

On a basic level, advanced mobile stations can be fitted with a firewall and an enterprise's firewall policies can be extended out to the mobile station to prevent attacks through the mobile station. In addition, an IT administrator can enable software installation protection through on-device-maintained blacklists and whitelists. Anti-virus, anti-spam, and anti-spyware capabilities are also available on mobile stations.

10.3 Device Compliance

Device compliance allows an IT administrator to remotely monitor a mobile station to ensure that it maintains integrity. As new software applications become available, or as an enterprise's IT policy changes, an IT administrator can update the mobile station OTA to maintain compliance.

If a mobile station has been compromised, an IT administrator can lock a mobile station by sending a message to the mobile station. The IT administrator can also erase the contents of the mobile station, rendering it useless until it is re-provisioned. Mobile stations can also be backed up and restored OTA.

11. HOSTED SERVICES SECURITY

Verizon Wireless offers secure, hosted, wireless data services for its subscribers. These hosted services are designed to enhance the mobile experience while maintaining security.

11.1 BREW

BREW is a runtime environment that allows Verizon Wireless to control which applications can run on a mobile station to access its network. For example, V CAST and Get It Now® use BREW. Mobile stations require a BREW signature to run applications. Non-BREW-based applications cannot read, write, or delete a target application's data, ensuring that no data breach or corruption occurs. BREW-based applications can grant access to non-BREW applications only after these applications have been authenticated. Non-BREW applications are verified via a digital signature from a trusted certificate authority to minimize the risk of virus infection.

11.2 SMS

SMS allows subscribers to send and receive short text messages between mobile stations. To combat flooding the network with SMS messages, Verizon Wireless has the ability to limit the number of messages and users accessing the network. If there are too many messages coming from one person or broadcast behavior is detected, this behavior, also known as "spamming," can be prevented by blocking these messages.

11.3 MMS

MMS allows for the transmission of images, audio, video, and rich text using WAP technology and an MMS-capable mobile station. Communication between the mobile station and the WAP server is handled through WTLS security. In addition, the Verizon Wireless MMSC implements message throttling to mitigate denial-of-service attacks. Standard best operating practices, such as firewalls and access control lists, are implemented to provide security for MMS.

11.4 Content and Media

V CAST™ provides OTA multimedia content including video, games, and music. Downloads are tested and authenticated as being from a reliable source before being made available to the end user. In addition to CDMA security, V CAST is made secure through the use of BREW.

11.5 Navigation and Location-Based Services (LBS)

VZ Navigator℠ provides subscribers with navigation, including turn-by-turn directions, via their mobile stations. Navigation and LBS are made secure by maintaining location/position information within Verizon Wireless and providing that only to authenticated applications.

11.6 Verizon Wireless Field Force Manager

Field Force Manager provides companies with resource tracking and management tools that help reduce operating costs, increase worker productivity, and streamline business processes. Field Force Manager allows managers to track worker locations, job lists, and timecards; validate job details; and dispatch personnel to needed locations—all of which is kept secure through LBS security features from Verizon Wireless.

12. SUMMARY

To secure its own wireless network, Verizon Wireless has developed and implemented the security best practices found in this document, enabling the company to offer a secure wireless environment to access mobile enterprise applications and data. Verizon Wireless combines technology, access policies, and services to help ensure that its customers' mobile workers have secure access to the data and applications they need, while minimizing outside security threats and possible attacks.

13. GLOSSARY OF TERMS

1xEV-DO (One times Evolution Data Optimized)—A CDMA2000 technology optimized for packet data services.

1xRTT (One times Radio Transmission Technology)—A CDMA2000 technology with traditional circuit voice and data support that has maximum downlink speeds of 307 Kbps and uplink speeds of 144 Kbps.

2G (second generation)—The second generation of cell-phone technology introduced during the 1990s. This generation added data capabilities to cell phones, including Internet and email access.

3G (third generation)—Third-generation cell-phone technology appeared in the 2000s and forms the foundation of our current cell-phone capabilities. 3G technology offers even faster Internet access, plus enables worldwide roaming capabilities.

AAA (authentication, authorization, and accounting)—A network server used for access control. Authentication identifies the user. Authorization implements policies that determine which resources and services a valid user may access. Accounting keeps track of time and data resources used for billing and analysis.

AC (Authentication Center)—A system that authenticates a mobile station that attempts to gain access to the cellular network.

ADC (analog-to-digital converter)—The device that converts analog signals into digital signals.

A-Key (authentication key)—A digital key used during an electronic transaction to ensure that the contents of the transaction remain unchanged when traveling from sender to receiver.

AN (access network)—A network that grants end user access to the network core and network services.

ASREPORT—A report sent by the MSC to the VLR indicating the status of a unique challenge.

AT (access terminal)—A 1xEV-DO mobile station.

AUTHDIR (Authentication Directive)—A unique challenge and update operation between an Authentication Center and a Mobile Switching Center in a cellular network.

AUTHU (Authentication response for a unique challenge)—A response to a unique challenge by the cellular network to prove the authenticity of a mobile station.

Base station (BS)—A terrestrial station in a cellular network that communicates with mobile terminals.

BREW (Binary Runtime Environment for Wireless)—A runtime environment that allows applications to run on a mobile station.

BSC (base station controller)—A distributed computing structure of the access network that manages multiple base transceiver stations (BTSs), radio resources, and handoffs between BTSs within its domain. BSC-to-BSC handoffs are handled by the mobile switching station.

BTS (base transceiver station)—A structure of the access network that contains antennas, transmitting and receiving radio systems, encoding/decoding systems, and encryption/decryption equipment. Multiple BTSs are controlled by a BSC.

CAVE (Cellular Authentication and Voice Encryption) algorithm—A cryptographic hash function used in CDMA mobile systems for authentication, data protection, anonymity, and key derivation.

CDMA (Code Division Multiple Access)—A method for sending multiple voice and/or data signals simultaneously across the radio spectrum.

CDMA2000—The brand name for telecommunications Interim Standard-2000 (IS-2000) that supports 3G CDMA-based cellular networks .

cdmaOne—The brand name for telecommunications Interim Standard-95 (IS-95) that support 2G CDMA-based cellular networks.

CHAP (Challenge-Handshake Authentication Protocol)—The protocol used to authenticate remote users to an Internet access provider.

COOP (continuity of operations)—Technology used to ensure continuous operation of services in the event of a disaster or crisis.

DMU (Dynamic Mobile IP Update)—A procedure used to distribute and update mobile IP cryptographic keys in CDMA, 1xRTT, and 1xEV-DO networks.

DRS (Data Ready to Send) —A code or bit that signals that a system is ready to send data.

DSSS (direct-sequence spread-spectrum)—A technology technique that deliberately distributes or “spreads” data over a frequency domain.

ESN (electronic serial number)—The unique identification number found in mobile stations.

FA (foreign agent)—A network device that acts as a mobility agent for a mobility node. Foreign agents work in conjunction with a home agent to support IP traffic forwarding for a device connecting to the network from somewhere other than its home network.

FAC (Foreign Agent Challenge) —A challenge issued by the foreign agent to a verify the authenticity of a device connection to the network.

FDMA (Frequency Division Multiple Access)—In FDMA, multiple connections on the radio spectrum are separated from each other by using different frequencies.

FIGS (Fraud Information Gathering System)—A system that monitors the activities of cellular network subscribers and looks for fraudulent activities.

GPS (global positioning system)—Navigation technology that pinpoints the exact location of the device containing the GPS.

GRE (Generic Routing Encapsulation)—A tunneling protocol that allows network layer packets to contain packets from a different protocol. It is widely used to tunnel protocols inside IP packets for virtual private networks.

HA (home agent)—A core network device that stores and forwards location and IP address information about a mobile station when it is away from the mobile station's home network. The home agent is used in conjunction with one or more foreign agents to manage mobile stations as they roam.

HDLC (High-level Data Link Control)—A synchronous data link layer protocol developed by the International Standards Organization (ISO) that manages PPP and MLPP connections.

HLR (home location register)—A database in a cellular system that contains all the subscribers within the provider's home service area.

HTTP (Hypertext Transfer Protocol)—The method used to convey information on the World Wide Web.

IDS (intrusion detection system)—A software system that detects attacks on the network.

IETF (Internet Engineering Task Force)—The governing body responsible for establishing standards for the Internet.

IKE (Internet Key Exchange)—A protocol whose purpose is to negotiate and provide authenticated keying for protected security associations.

IMAP (Internet Message Access Protocol)—The protocol that allows remote devices to access email messages from the Internet.

IMSI (International Mobile Subscriber Identifier)—A unique 15-digit number assigned to a mobile station issued at the time of service subscription containing subscriber identification information.

IP (Internet Protocol)—The network layer protocol in the TCP/IP communications protocol suite (the "IP" in TCP/IP). Also references IP address, the four-element number with three decimal points that is the numeric identification of every node in a TCP/IP network.

IPCP (Internet Protocol Control Protocol)—A network control protocol for establishing and configuring an IP over PPP connection.

IPSec (IP Security)—A suite of protocols used to secure IP communications through authentication and encryption technology.

ITU (International Telecommunications Union)—An international governing body that develops standards recommendations for telecommunications, consumer electronics, broadcasting, and multimedia communications. The ITU's main responsibilities governing the mobile telecommunications industry is standardization, radio spectrum allocation, and the facilitation of arrangements between countries allowing for international phone calls.

L2TP (Layer 2 Tunneling Protocol)—A tunneling protocol that is used to support VPNs. L2TPv3 provides additional security features, improved encapsulation, and the ability to carry data links other than PPP over an IP network.

LCM (long code mask)—A 42-bit binary number that creates the unique identity for a long-code generator whose output is used in the CDMA coding and spreading process.

LCP (Link Control Protocol)—Used by PPP to establish a link between a user's computer and the Internet service provider.

LBS (location-based services)—LBS are used by wireless companies to send advertising and promotional messages to the user, based on his or her location.

LDAP (Lightweight Directory Access Protocol)—A network protocol used for querying and modifying directory services on TCP/IP connections.

MAC (medium access control)—The process that allows multiple connected terminals to broadcast over the same physical medium.

MD5 —a widely used cryptographic hash function with a 128-bit hash value. MD5 is an Internet standard (RFC 1321) that is deployed in a wide variety of security applications.

MIN (mobile identifier number)—The unique 10-digit number used to identify a mobile phone.

MLPPP (Multi-link Point-to-Point Protocol)—An extension to PPP that enables two channels to be linked together to double the throughput. It is used for ISDN transmission and channel bonding.

MMS (Multimedia Messaging Service)—A messaging system that allows video, pictures, audio clips, and other multimedia to be distributed wirelessly.

Mobile IP (MIP)—In MIP, the packet data session is not dropped each time the user changes location. The session continues as long as mobility is still connected to the home agent.

Mobile node (MN)—Same as Mobile Station.

Mobile station (MS)—An end terminal such as a mobile phone, a laptop with an embedded modem, a broadband wireless router, or a PCMCIA modem that can access the CDMA network.

MPLS (Multiprotocol Label Switching)—A datagram transport service designed to emulate circuit-switched network characteristics over a packet-switched network. It can be used to carry many different types of traffic, such as IP packets, ATM frames, and Ethernet frames.

MPN (mobile private network)—MPNs allow mobile users to communicate securely across public networks.

MSC (mobile switching center)—A core-network switching structure that bridges the mobile telephone access network with another telephone network such as the public switched telephone network (PSTN).

NAI (Network Access Identifier)—The user identification submitted by the mobile station during network access authentication.

NAS (network access server)—A device that functions as an access control point for users in remote locations, connecting users to their company's internal network or to an Internet service provider.

NNTP (Network News Transfer Protocol)—The protocol used to post and receive information from Usenet and news servers.

OAM (operations, administration, and management)—The process by which wireless networks and mobile devices are maintained.

OSI (Open Systems Interconnection)—The standard reference model for how messages are transmitted between any two points in a network.

OTA (over the air)—The process by which mobile stations are updated with new software or monitored for security.

PCF (packet control function)—Routes IP packets between the mobile stations connected to its associated BTSes and PDSN.

PDSN (Packet Data Serving Node)—A PDSN establishes, maintains, and terminates a PPP session to an MS.

PN (pseudo-random noise) sequence— A set of bits intended to simulate the statistical randomness of noise. A PN sequence is generated by a deterministic process and will repeat; therefore, it is "pseudo"-random.

PPP (Point-to-Point Protocol)—A common method to establish a direct connection between two points. PPP is link layer-agnostic and is commonly used to establish a connection between a networked device and the Internet.

PTT (push-to-talk)—Services made available by pressing a button on a mobile station to communicate.

QoS (quality of service)—The measure of performance in a telecommunications system. QoS refers to the mechanisms in the network software that make the actual determination of which packets have priority.

RADIUS (Remote Authentication Dial-In User Service)—A client/server protocol enabling remote access servers to communicate with a central server to authenticate users and authorize network access.

RANDSSD (Random Variable Shared Secret Data)—A 56-bit random number generated by the mobile station's home station.

RANDU (Unique Random Number)—A 24-bit random number generated by a base station in support of the AUTHU challenge.

RLP (Radio Link Protocol)—A link layer protocol used to correct network-based errors.

RNC (radio network controller)—A network element that controls and manages a group of connected base station controllers.

R-P (Radio Network-Packet Network)—A radio system and methodology for handling packetized communications within a CDMA network.

RRP (Registration Reply)—A message reply from a home agent regarding the state of a subscriber.

RRQ (Registration Request)—A message request sent to a home agent regarding the state of a subscriber.

RSA (Rivest, Shamir, Adelman)—An encryption and authentication system that uses an algorithm developed by Ron Rivest, Adi Shamir, and Leonard Adleman.

Simple IP (SIP)— Simple IP is an IP address that is valid within a PDSN coverage area. A mobile station must obtain a new IP address (and lose existing connections) when it moves from one PDSN coverage area to another.

SMS (Short Message Service)—A feature of the cellular network allowing text messages of up to 160 characters to be sent and received.

SSD (Shared Secret Data)—SSD is used to respond to authentication challenges. SSD is a 128-bit number derived from the A-Key and random numbers.

SSL (Secure Sockets Layer)—Cryptographic protocols that provide security over the Internet.

TDMA (Time Division Multiple Access)—The process of dividing the radio spectrum by time. Using TDMA, multiple connections are separated by time.

TIA (Telecommunications Industry Association)—A non-profit trade association serving the telecommunications and information technology industries.

TMSI (Temporary Mobile Station Identifier)—A temporary number assigned to a mobile station at the moment it's turned on. The number changes when the mobile station changes locations.

UATI (Unicast Access Terminal Identifier)—An over-the-air signaling identifier that associates a mobile terminal with the access network's radio resources used during the connection and call setup procedure.

VLR (visitor location register)—The database in a cellular network that contains the list of subscribers registered in a service area.

VoIP (Voice over Internet Protocol)—Telephone services that use the Internet to make and receive calls.

VPN (virtual private network)— A private network that uses a public network such as the Internet to connect users or remote sites together in a secure manner. VPN direct-connect solutions are extremely popular due to their low cost to deploy. Instead of using a dedicated connection such as leased-line direct circuits, the VPN option uses tunnels routed over the Internet from the company's private network to the Verizon Wireless network operations center.

WAP (Wireless Application Protocol)—The protocol that allows mobile stations to wirelessly access the Internet and email applications.

14. CONTACT INFORMATION

For more information about Verizon Wireless, speak with a Verizon Wireless sales representative, visit www.verizonwireless.com, or call 1.800.VZW.4BIZ.

15. LEGAL DISCLAIMER

This document and the information contained herein (collectively, the "**Information**") is provided by Verizon Wireless, on behalf of itself and its affiliates for informational purposes only. Verizon Wireless is providing the Information because Verizon Wireless believes the Information may be useful. The Information is provided solely on the basis that each business will be responsible for making its own assessments of the Information and are advised to verify all representations, statements, and information before using or relying upon any of the Information. Although Verizon Wireless has exercised reasonable care in providing the Information, Verizon Wireless does not warrant the accuracy of the Information and is not responsible for any damages arising from the use of or reliance upon the Information. Verizon Wireless in no way represents, and no reliance should be placed on any belief, that Verizon Wireless is providing the Information in accordance with any standard or service (routine, customary or otherwise) related to the consulting, services, hardware, software, or other industries.

Network details, coverage limitations, and maps are available at www.verizonwireless.com.