Mobility Capability Package

March 26

2012

This document defines the 2nd release of earlier phases of the Enterprise Mobility Architecture and focuses on the architectural components of providing a Secure VoIP capability using commercial grade products.

Secure VoIP
Version 1.2

Table of Contents

Mobility Capability Package

Document Status: CSfC and Accreditation

The Mobility Capability Package is a product of the National Security Agency's Information Assurance Directorate (NSA/IAD) Mobility Program and the NSA/IAD Commercial Solutions for Classified (CSfC) process.

NSA/IAD is developing new ways to leverage emerging technologies to deliver more timely Information Assurance solutions for rapidly evolving customer requirements. To satisfy this new business objective, NSA/IAD's Commercial Solutions for Classified (CSfC) process was established to enable commercial products used in layered solutions to protect classified National Security System (NSS) data. This satisfies customers' urgent requirements to communicate securely with interoperable products based on commercial standards in a solution that can be fielded in months, not years.

This document is the second of a series of early releases of the Mobility Capability Package, and only partially implements a full Capability Package. The intent of the early release of these documents is to establish a partnership between system integrators and NSA/IAD experts via NSA/IAD's client processes to build secure Voice over IP systems while ensuring cryptographic commercially available mechanisms are properly implemented; and to establish the dialog with product developers to develop the necessary trusted, commercially available products that will enable those capabilities to be realized. Guidance in this document is not at the point where it can be used without consulting NSA for evaluation support prior to presenting a solution to the implementing organization's Authorizing Official. Customers interested in implementing solutions per this document need to submit a request for support to NSA/IAD Triage process. Future releases of this document (2.0 and higher) will build on the initial VoIP architecture and include additions for a secure interoperability architecture, mobile device management and data applications, and WiFi services with differing end devices. In the future, customers and their solution provider will be able to use this guidance to implement solutions without NSA involvement, and have the decision on allowing operation of a Secure Mobility capability made by their organization's Authorizing Official.

These earlier versions (1.x) of the Mobility (CSfC) Capability Package are the first steps in the development of a "how to" manual for a Secure Voice over IP generic architecture. The document outlines the security roles of the major components within the architecture and offers a broad-based set of capabilities and requirements to ultimately build a secure VoIP capability. In later versions, guidance will be provided for selecting products, setting rules for customers using this capability, configuring the devices, testing implementation, assessing risk of the implementation for certifiers and accreditors, managing key, and maintaining lifecycle support.

Please provide comments concerning the improvement of this document to mobility@nsa.gov. When submitting comments, please indicate whether you are claiming any intellectual property rights in the information you are providing and, if so, indicate which particular information you claim to be

intellectual property. For more information about the NSA/IAD Mobility Program, please visit: http://www.nsa.gov/ia/programs/mobility_program/index.shtml

For more information about the Commercial Solutions for Classified Program (CSfC) or the related National Information Assurance Program (NIAP), please visit the following web sites:
http://www.nsa.gov/ia/business_research/ia_bao/commercial_solutions_for_classified_program.shtml
http://www.niap-ccevs.org/pp
http://www.iad.gov

DISCLAIMER

This Capability Package is provided "as is." Any express or implied warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the United States Government be liable for any direct, indirect, incidental, special, exemplary or consequential damages (including, but not limited to, procurement of substitute goods or services, loss of use, data or profits, or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this Capabilities Package, even if advised of the possibility of such damage.

The User of this Capability Package agrees to hold harmless and indemnify the United States Government, its agents and employees from every claim or liability (whether in tort or in contract), including attorneys' fees, court costs, and expenses, arising in direct consequence of Recipient's use of the item, including, but not limited to, claims or liabilities made for injury to or death of personnel of User or third parties, damage to or destruction of property of User or third parties, and infringement or other violations of intellectual property or technical data rights.

Nothing in this Capability Package is intended to constitute an endorsement, explicit or implied, by the U.S. Government of any particular manufacturer's product or service.

Change Log

Version	Date	Change Description
1.1	02/29/12	Initial revision for public distribution.
1.2	03/26/12	Document is product neutral. Removed all references to products that were used as examples for emphasis.
		Added disclaimer statements and statements about intellectual property.
		Added improved discussion of how to use this document and how it relates to the Commercial Solutions for Classified Process.
		Edited the document improving readability and removing grammar issues.
		Removed un-necessary requirements. Expectation should be that other requirements will be removed or added in this and future releases based upon that maturity of those requirements in other documents.
		Statements regarding required approvals are being removed from current version, and will be added back in Version 2.0 for more clarity.

1 Overview of Enterprise Mobility

1.1 Goals

Enterprise Mobility will provide users with anytime, anywhere access to data, services, and other users to successfully and securely achieve their mission, whether it is warfighting, intelligence, or business. Given the increasing rate of change in technology and the need to control costs, except in rare cases, the government can no longer afford to develop its own expensive, and potentially untimely, security solutions. Instead, a new model, the Commercial Solutions for Classified (CSfC) process to protect National Security information will be used. The National Security Agency, working with its partners, customers, and industry will develop security solutions based upon commercially available products that will enable customers to layer and compose solutions that ensure that their systems and information are reliable, protected, and available. CSfC will rely on the National Information Assurance Partnership to convey the necessary security requirements to Commercial Off the Shelf (COTS) vendors by means of U.S Government Standard Protection Profiles that consistently promote the use of Suite B and the Cryptographic Interoperability Strategy.

The use of commercial mobile devices from laptop computers to the latest smartphones and tablets with mobile access is critical to achieving this goal. This release of Mobility Capability Package will describe the necessary steps for Securing Voice over IP and initiates the basis for the capabilities that need to be realized in cost effective, composed COTS-based solutions, using layered security approaches to achieve assured information sharing. Figure 1-1 is an operational view of secure anywhere, anytime access to the enterprise infrastructure.

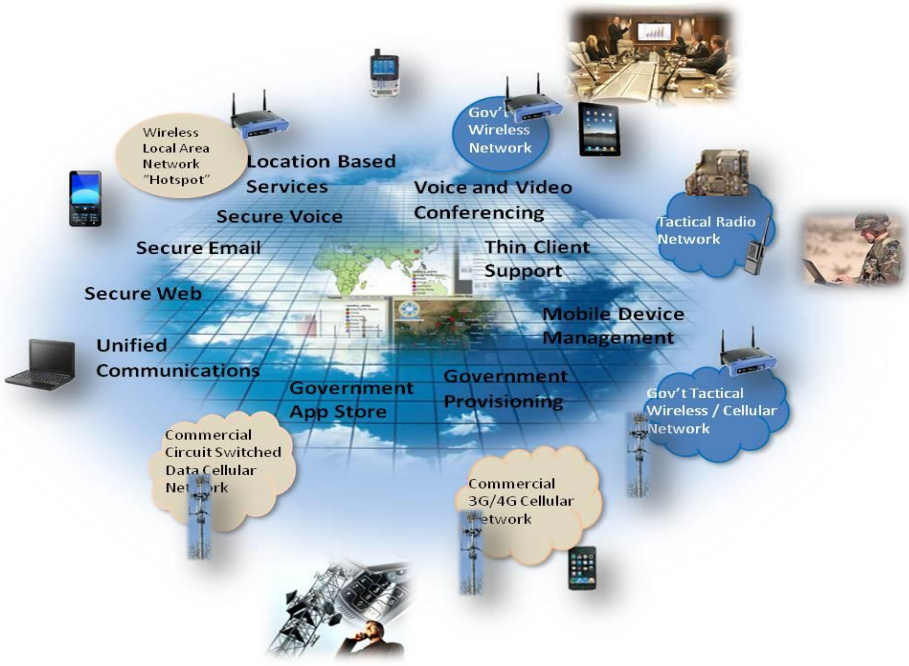

Figure 1-1 Enterprise Mobility

1.2 Description

Enterprise Mobility is supported by the use of commercial cellular and wireless devices to access classified data and voice services while minimizing the risk when interconnecting to existing enterprise services. Cellular 3G and 802.11 WiFi are currently the main access methods addressed but evolution to 4G technology, use of tactical radios, and wired use are also included. The commercial carriers and other unclassified access networks provide the controlled connectivity between end users and the Government enterprise. A Virtual Private Network (VPN) establishes a secured path between the user equipment and the secured access networks with a second layer of encryption required to access classified enterprise services. Figure 1-2 depicts the basic segments of the mobility architecture:

- User Equipment - includes commercially available mobile end user computing, display, input, and communications devices such as smartphones, tablets, netbooks, and laptops - with embedded communications or external MiFI/tethered modems.
- Access Networks - includes unclassified (commercial, public, and Government controlled) transport with limited control capabilities that allow user equipment to connect to the Enterprise Mobility Infrastructure. To cross unclassified access networks, two layers of approved commercial encryption will be required.
- Enterprise Mobility Infrastructure – includes Enterprise Networking Services and Enterprise Application Services.
    - Enterprise Networking Services provides the access point for all communications with User Equipment. It includes call control to establish data connections with authorized user equipment and a VPN endpoint to provide an outer security layer.
    - Enterprise Level Services includes unified communications (e.g. voice calling, conferencing, messaging, presence) virtualized desktop, and web services. Each application service includes an inner security layer at the network, transport, or application level.

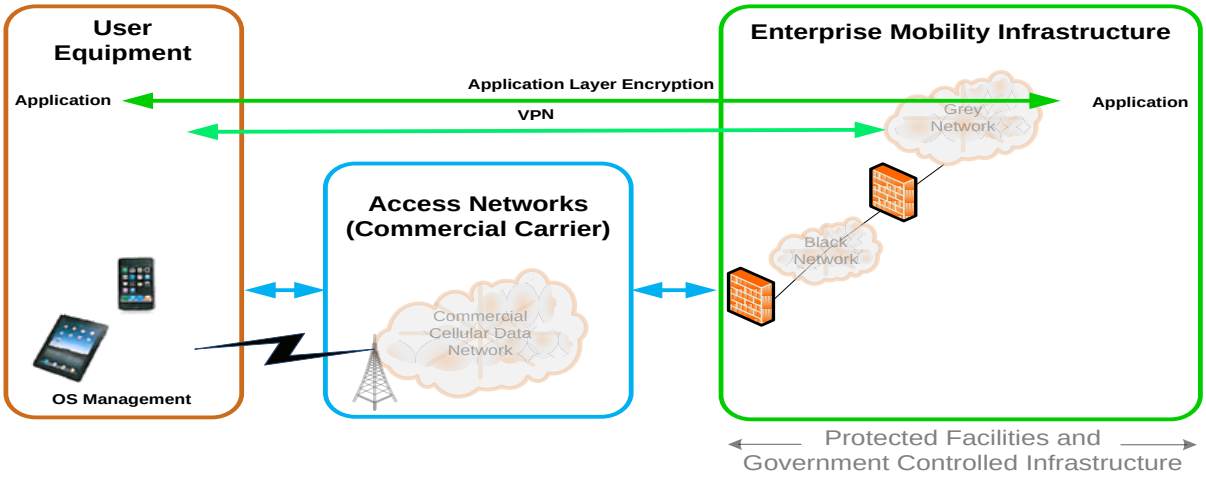

Figure 1-2 Basic Segments of the Mobility Architecture

Composed, layered solutions are the basis for the secure use of mobile devices and commercial components for access to classified enterprise services and data. Layers of commercial encryption, hardening of devices, Government provisioning (including keys and certificates), boundary protection (again layered), and controls within unclassified access networks all contribute to the overall security. Government controlled or managed devices and operations ensure ongoing policy compliance and responsiveness to lost and stolen devices.

1.3 Provisioning, Operations, and Management

A secure mobile device will not interact with the cellular carrier services in the same way as a comparable personal device but the capabilities can be similar and the user experience as close as practical. In some cases, security will require that the government own, control, or manage the enterprise mobility infrastructure, but services will emulate those available to commercial users. For example, all communications will be data packets and will be routed to the government infrastructure. Commercial application stores will not be directly accessible to users but government application stores within each security domain will be available and provide approved applications. Phone calls to commercial and private numbers may be allowed via telephone gateways in the government infrastructure. Figure 1-3 shows a more detailed view of the mobility architecture including the three major segments of user operations, the existing enterprise, plus a view of the overarching management and provisioning components.

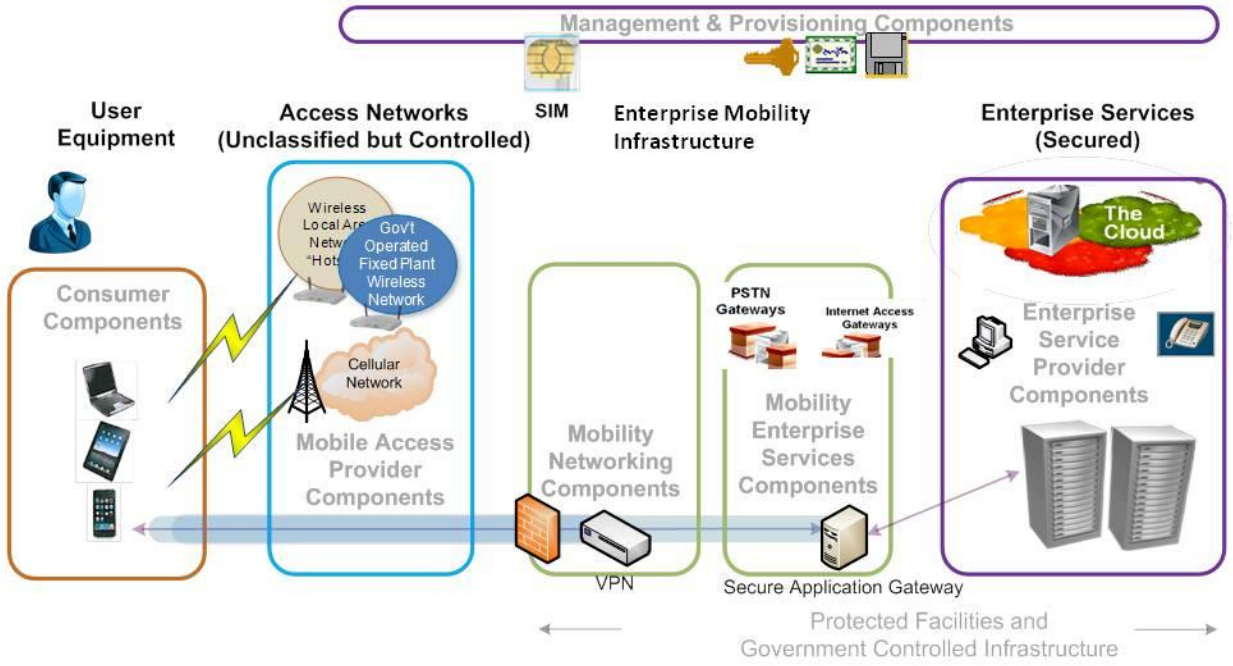

Figure 1-3 Major Areas of the Mobility Architecture

1.4 Component Requirements – Thresholds and Objectives

Each area of the Mobility Architecture will be explored with the security components identified and have an associated table of requirements. The requirement priorities are specified based on guidance contained in section 2.1.1 of the Defense Acquisition Handbook. Based on this guidance, the "Threshold or Objective" column in each table means the following:

- An objective (O) requirement specifies a feature or function that the Government desires and expects.
- A threshold (T) requirement specifies a minimum acceptable feature or function that, in the Government's judgment, still provides the needed capabilities if the corresponding objective requirement cannot reasonably be met (e.g., due to lack of technology maturity, cost or time constraints).

In many cases, the threshold requirement also serves as the objective requirement (T=O). Where both a Threshold requirement and a related Objective requirement exist, the Objective requirement complements the Threshold requirement rather than replaces it.

2 Overview of Smartphone Secure Voice over Internet Protocol (VoIP) on Cellular Networks

The remaining sections of this package (Sections 2 through Section 8) define the current knowledge and guidance available to create a secure Voice over IP system based upon commercially available components. Section 2 provides a high level view of the architecture and the subsequent sections explores each of those parts of the architecture. Each of the sections will provide a similar theme – how to use the current commercially available technology for secure use, what are the gaps with that technology and how to mitigate those gaps, and what risks still exist. The mobile user's equipment, specifically a smartphone in this particular instance, will be discussed in Section 3. Often the terms wireless provider, cellular network, or access networks are used to discuss the commercial carriers. Section 4 will address the commercial Carrier Services Connections. Section 5 will address the required controlled Enterprise Mobility Infrastructure. While each of the previous three mentioned sections describe the top level architecture – the device, the carrier, and the needed mobility infrastructure, Section 6 will take a horizontal view of the user application – Voice over IP. Section 7 – Secure Mobility Interoperability will be a growth area for new information and will be only introduced in the early releases. Section 8 covers the terms and acronyms used in the document.

2.1 Goals

The overall goal is to provide users with Secure VoIP calls while accessing the cellular network with a commercial smartphone as needed to perform their mission effectively and securely, whether it is warfighting, intelligence, or business. This capability is the crucial first step to achieving the goal of "anywhere/any way" mobile communications. The current design with a voice application is unencumbered by user data residing on the end user device to prove the concept that commercial components can be composed to protect classified information in a mobile environment. Figure 2-1 provides a functional view for Secure VoIP on a smartphone over to a Cellular Network.

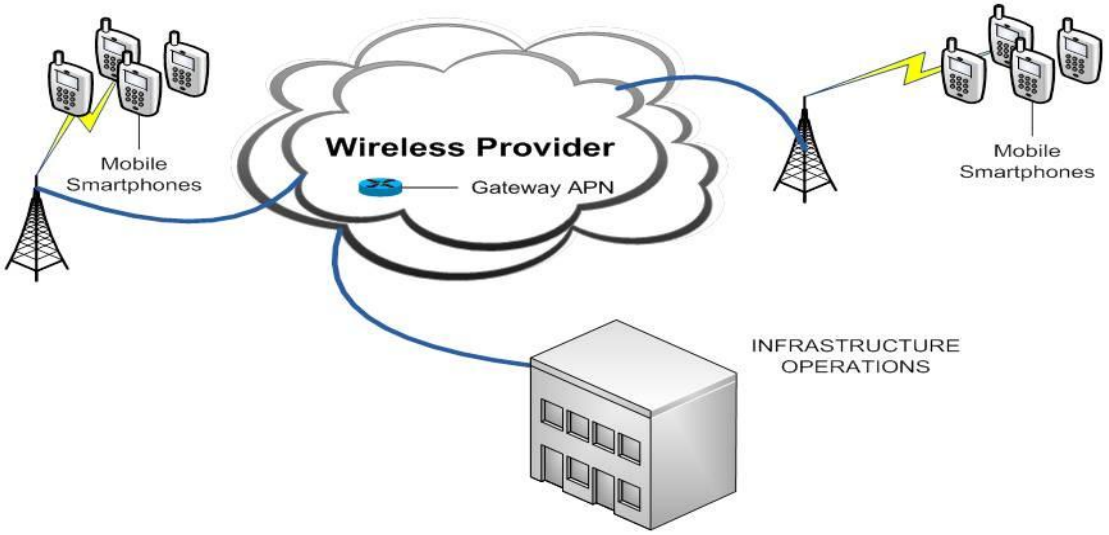

Figure 2-1 Major Areas of Secure VoIP

2.2 Description

The smartphone VoIP mobility goal is supported by the use of commercial cellular products that provide secure voice services while minimizing the risk and impact to existing enterprise services. Cellular 3G is the main access method discussed but evolution to 4G technology is also possible, and this package will be upgraded in the near future to provide guidance leveraging 4G technology. The commercial carriers and other unclassified access networks provide the controlled connectivity between end users and the Government enterprise. A VPN establishes a secured path between the user equipment and the secured access networks with a second layer of encryption required to access classified enterprise services. Figure 2-2 depicts the basic segments of Secure VoIP on a 3G smartphone.

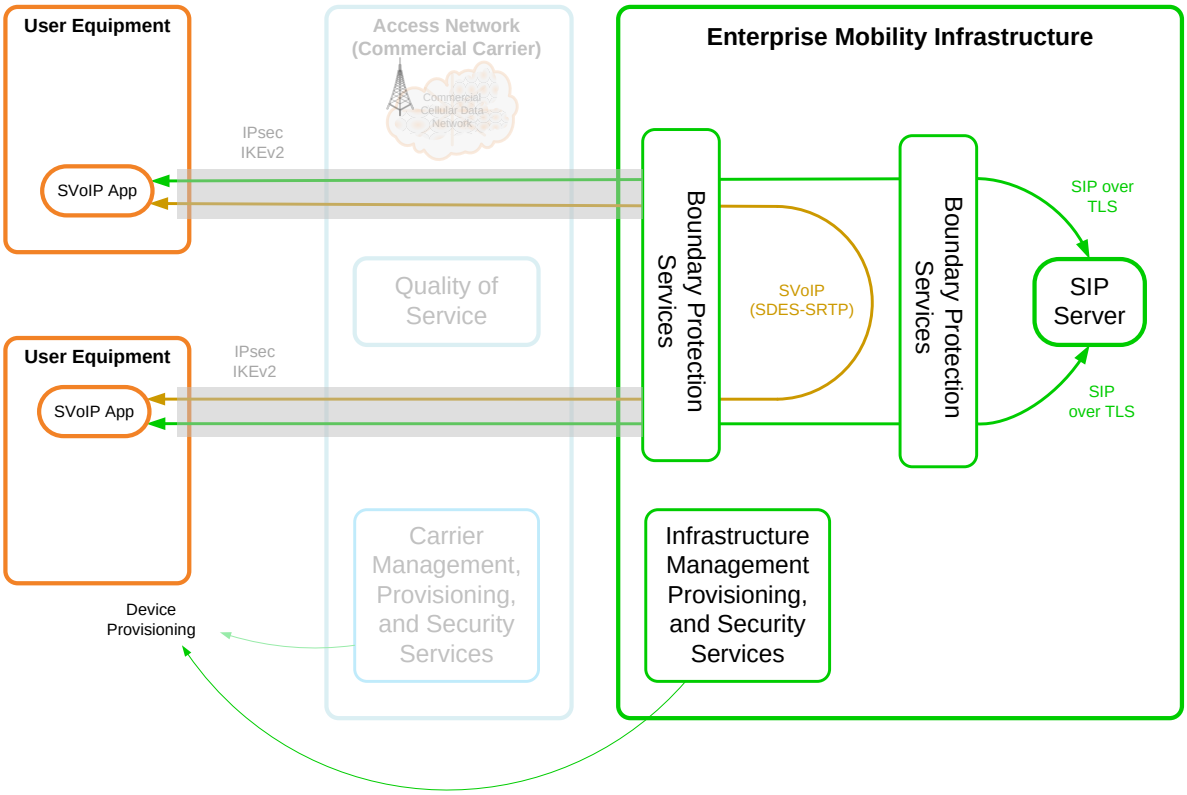

Figure 2-2 Basic Segments of Secure VoIP

Composed, layered solutions are the basis for the secure use of mobile devices and commercial capabilities for access to classified enterprise services and data. Layers of commercial encryption, hardening of devices, Government provisioning (including keys and certificates), boundary protection (again layered), and controls within unclassified access networks all contribute to the overall security. Government management of devices and operations ensures ongoing policy compliance and responsiveness to lost and stolen devices.

2.3 Threat Environment

With the growing use of mobile devices in the enterprise, new threats are emerging. Not only is there the need to worry about devices being lost or stolen, but malware on mobile products is becoming a growing issue. Rogue base stations and WiFi hotspots attempt to make unauthorized connections to mobile devices in order to steal data or services or to corrupt the device. The radio frequency transmissions used to connect to cell towers or WiFi access points are susceptible to intercept. Insiders within access network operations may also attempt to steal or modify information, corrupt the device, or deny service. This includes non-malicious attacks from software bugs, operator error, and system failures. Mobile devices often have weak user authentication, removable memory, and local interfaces such as Bluetooth than can be exploited if not secured or disabled. Internal to a mobile device, data may be susceptible to intentionally or inadvertently misrouting to bypass security functions. Without the appropriate security, mobile devices are extremely vulnerable to many attacks and errors.

2.4 Security Principles

The smartphone Secure VoIP mobility architecture is a secure system itself. It enables and secures the use of mobile devices and their access to enterprise resources. The architecture includes capabilities to protect resources (data – VoIP in this instance, and systems, mobile and enterprise), to detect suspicious activity, and to respond. This includes protection of management and control traffic and systems. The smartphone Secure VoIP architecture is based on a system versus component approach—the interactions and dependencies of infrastructure and devices, and of elements within the entire system are considered. In keeping with the CSfC approach, composed commercial technology is used. For instance, Data-In-Transit (DIT) protection for classified information is provided by two separate layers of Commercial-Off-the-Shelf (COTS) encryption. This does require understanding and analysis of the relationship of the two layers and how to maintain adequate separation. The emphasis on commercial solutions is intended to provide a more cost effective solution.

Use of COTS products to protect classified using layered encryption introduces new considerations: how many layers of protection are appropriate and what type of protection; determining the security domain of the intermediate zone between layers; interoperability with key and credential management infrastructures; and the ability to identify and control security levels with commercial equipment.

2.5 Mobile User and Wireless Access

Prior to requesting an application service or conversing with another user, a user's mobile device must connect with a mobile access provider, be connected to the Government mobility infrastructure, and establish a secured session. The first step is to access an authorized cellular carrier or wireless access point. A path is established through interconnecting networks to the Government mobility infrastructure in protected facilities that provides controlled connectivity and Data-in-Transit protection. Once this secured session is established, the mobile user can request access to application services or to other users. For example, a cellular smartphone connects to a cellular carrier. The cellular carrier routes the data to the Government network. Since the carrier is not collocated within the Government protected facilities, a commercial network may be used as the transport network to connect between the carrier and Government facilities. Within the protected facilities, mobility networking components establish a secure connection with the phone and route the data to the mobility enterprise services. This portion of user connection is common to all of the user potential services threads (access to application

services, connection to other mobile users, connection to non-mobile user devices, and access to unified communication services). Figure 2-3 illustrates the interactions and data flow across the components for cellular and wireless access.

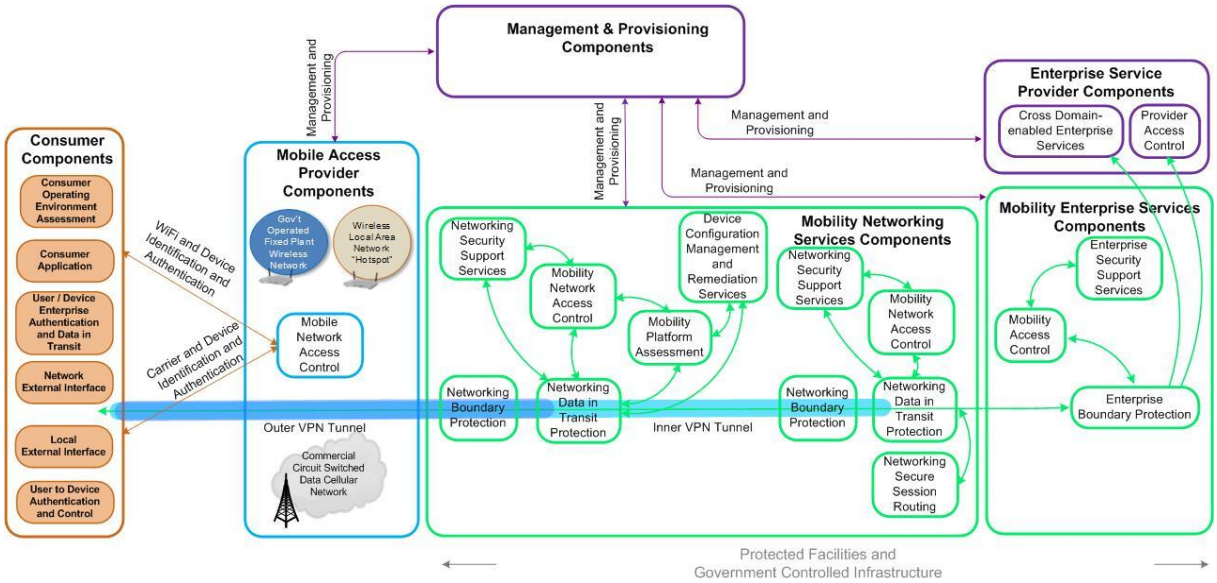

Figure 2-3 Mobile Cellular User and Wireless Access

2.6 Mobile User to Mobile User

To make a phone call to another mobile device with compatible protocols, the initial steps are the same as for accessing a service. The user's mobile equipment first accesses an authorized cellular carrier or wireless access point. A path is established through interconnecting networks to protected facilities that provide controlled connectivity and call management services. The cellular carrier routes the data to the Government network. Since the carrier is not collocated with the Government protected facilities, a commercial network may be used as the transport network to connect between the carrier and Government facilities. Within the protected facilities, mobility networking components establish a secure connection with the phone and route the call request to a call management service. From this point forward, the processing and paths differ from the service access interactions. The call control/management service identifies the called user device and attempts to communicate with it. Note that this device must have already established a secure VPN connection to be accessible. If the called device answers the call, the call control/management service completes the connection between the two users. The users now establish a secured call by exchanging credentials to form a session key for application level encryption. Figure 2-4 illustrates the data flow across components for cellular secure voice.

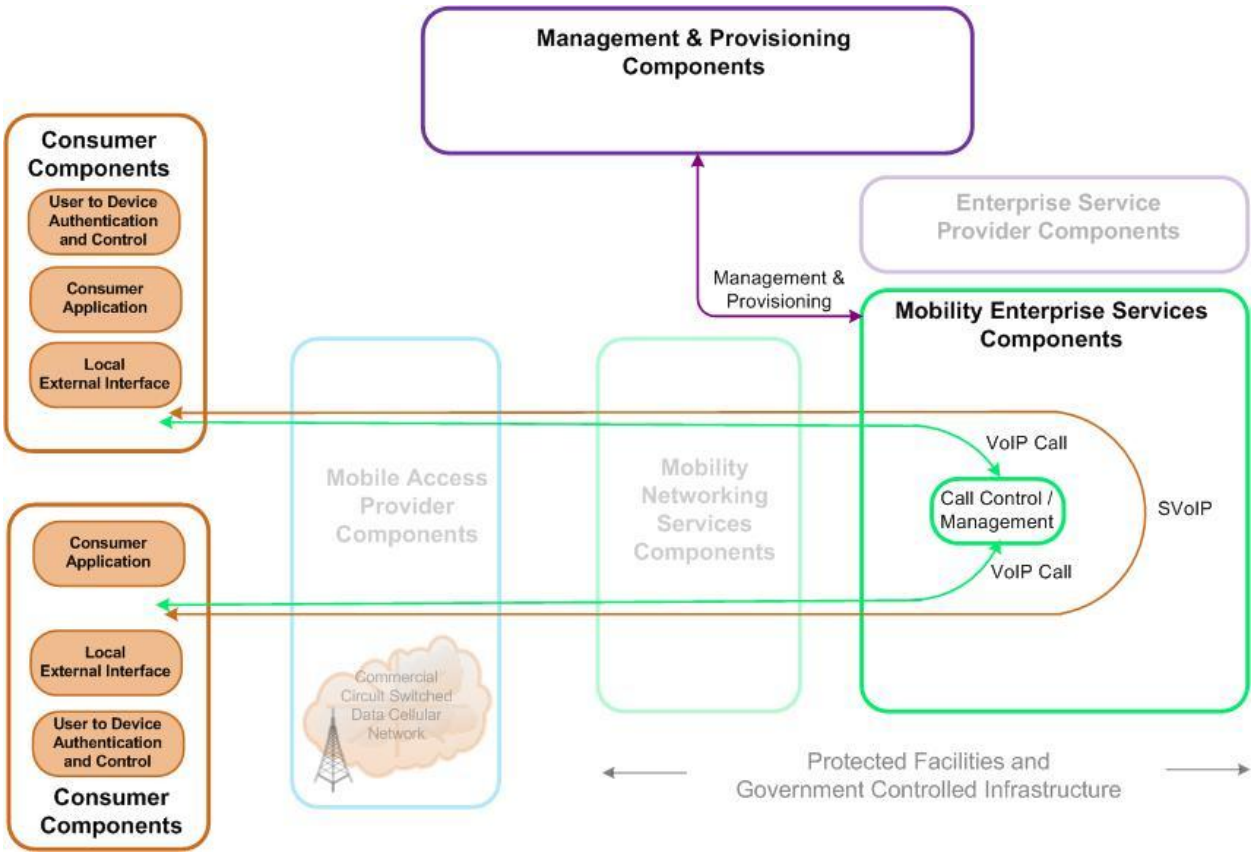

Figure 2-4 Secure Mobile to Secure Mobile (SVoIP)

3 Operating System and Applications Mobile Device Security

3.1 Overview

A commercial Mobile Device typically provides computing, displaying, inputting, and communication capabilities to a user. The associated capabilities are provided and managed by an Operating System (OS) platform running on the device. In order to protect these mobile capabilities, the operating system should be able to perform proper authentication, access control, data protection (at rest, in process, and in transit), health reporting, and accountability.

This section describes the security services and components needed on a mobile device and its resident operating system for classified usage. An operating system can provide multiple security features and functions, but only certain security critical components are highlighted in this section. This includes the resident VPN client, key storage and management (including protection of the authentication certificates and private keys), and device management including logging of health information, management of trusted processes (including the removal of unnecessary applications), and security monitoring.

A mobile device is typically composed of applications running on top of an operating system, which relies on its kernel and device drivers, and then the embedded firmware on a hardware architecture. Ideally, security critical components should be implemented on multiple independent layers such that an application layer security failure does not compromise the security upheld by the operating system layer. Securing a mobile device can be broken down into different strategies such that security critical services are protected by components inside each of the layers.

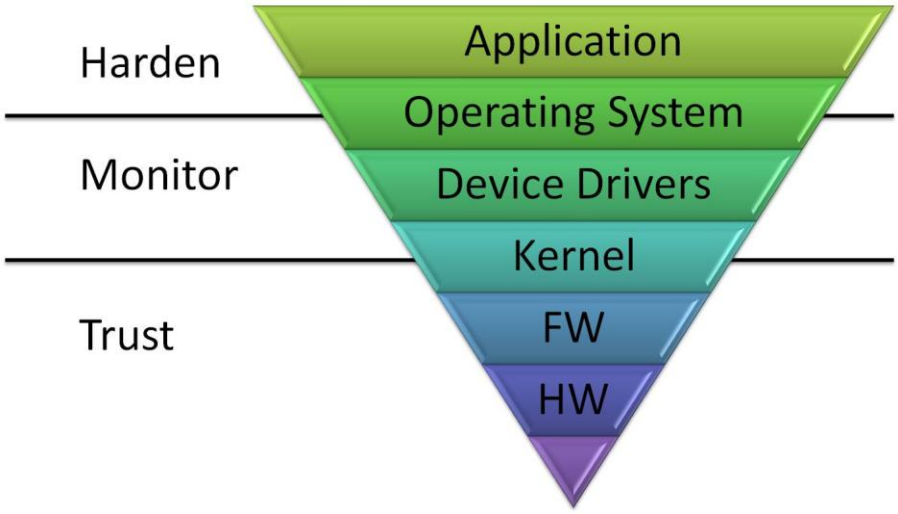

Figure 3-1 Mobile Device Protection

Figure 3-1 shows the practical mobile device protection breakdown. The strategy is to harden the layers that can be hardened (such as the applications and some areas of the operating system), monitor the layers that can't be hardened (when security critical), and trust the layers where security must be implemented at the hardware level.

3.2 Operation

The basics of the secure VoIP system operation from the point of view of the mobile device are as follows:

1. Device is powered on.
2. Monitoring service starts on device.
3. Configurable initialization program ensures that only authorized applications and operating system components are loaded, and that the system is in a known secure state.
4. Once the system is fully booted and in a secure state, the user can access the device by entering the required pin or passphrase to unlock the screen lock.
5. When the screen is unlocked, and before any other activities, a second passphrase or password is entered to decrypt the device's memory, which also stores any required keys or certificates.
6. The user starts the VPN, which establishes a tunnel from the device to the infrastructure.
7. Upon establishment of the VPN, the user registers to the Session Initiation Protocol (SIP) server via a Transport Layer Security (TLS) connection. This TLS connection is tunneled through the VPN connection.
8. Once the user is registered with the SIP server, they will be able to send or receive calls.

3.3 Approach

3.3.1 Architecture

The mobile smart phone or end user device is a commercial handset that is configured in order to provide secure communications with other approved mobile smartphones or with approved networks. For example, for secure voice communications, the end user device directly communicates with the commercial cellular network, the VPN gateway and SIP server in the organization's infrastructure, and finally with another end user device. Two layers of approved commercial encryption are used to protect communications across the untrusted commercial cellular network.

3.3.1.1 Architecture Overview

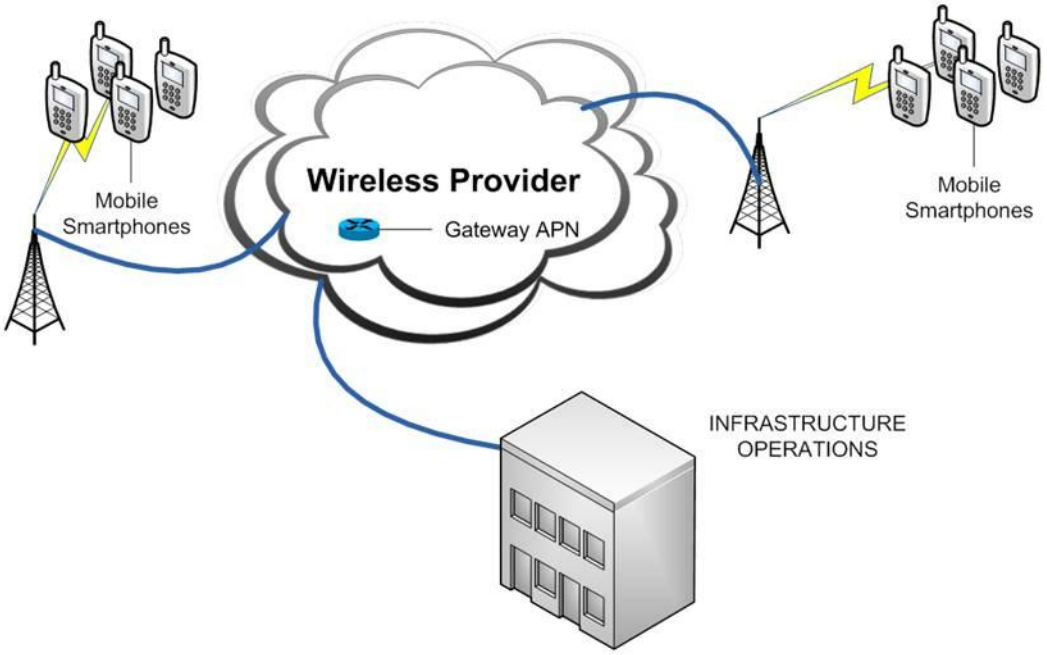

Figure 3-2 High Level Architecture

Internal to the end user device, there are several hardware/firmware components that provide external connectivity, hardware to support user interaction, software that controls the device, security related support, applications, and memory (which could possibly be shared by the application processor and the connectivity-related components). Some of these components can be managed via the operating system, some can be monitored via the operating system, and some can neither be managed nor monitored by the operating system.

3.3.1.2 Operating System Configuration

Organizations need to have the ability to disable features and functions in order to meet their mission needs. Disabling these features and functions should not impact the ability to make a secure voice call.

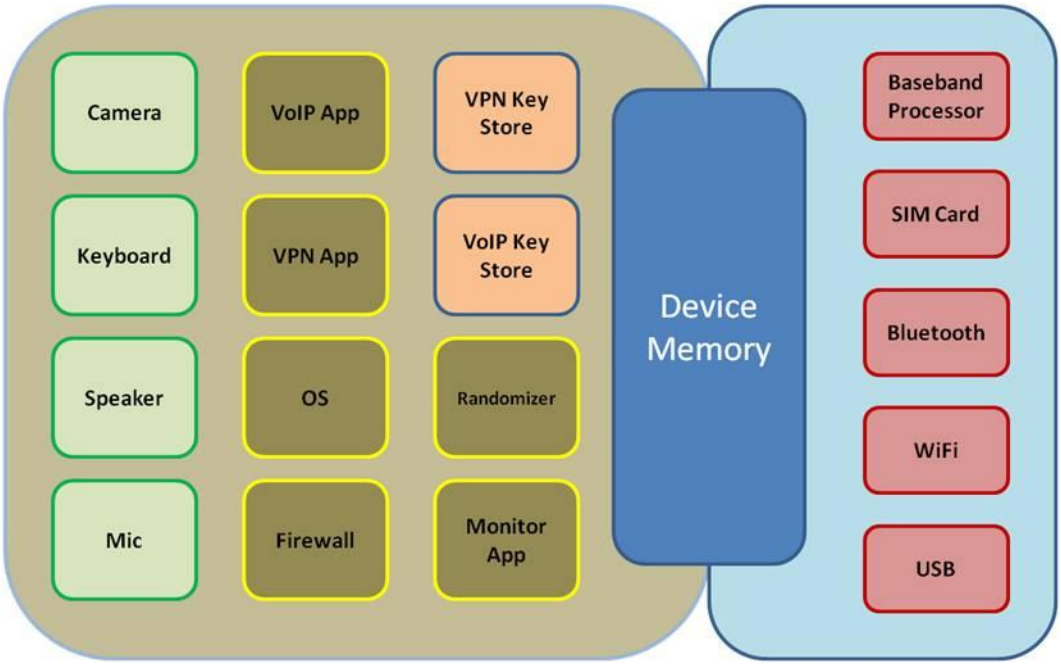

Figure 3-3 Mobile Device Components

3.3.1.3 System Settings

The following table describes various settings and features that are expected to be available in the end user device.

Table 3-1 Operating System Configuration Requirements

Req #	Requirement Description	Threshold / Objective
OSY.01	The system shall provide the capability to disable Bluetooth during initial provisioning and at system boot/initialization.	T=O
OSY.02	The system shall provide the ability to prevent users from enabling Bluetooth.	T=O
OSY.03	The system shall provide a mechanism to determine if the user has enabled Bluetooth.	T=O
OSY.04	The system shall provide a notification mechanism if the Bluetooth has been enabled by the user.	O
OSY.05	The system shall provide the capability to disable WiFi during initial provisioning and at system boot/initialization.	T=O
OSY.06	The system shall provide the ability to prevent users from enabling WiFi.	T=O
OSY.07	The system shall provide a mechanism to determine if the user has enabled WiFi.	T=O

Req #	Requirement Description	Threshold / Objective
OSY.08	The system shall provide a notification mechanism if the WiFi has been enabled by the user.	O
OSY.09	The system shall provide the capability to disable Auto Answer during initial provisioning and at system boot/initialization.	T=O
OSY.10	The system shall provide the ability to prevent users from enabling Auto Answer.	T=O
OSY.11	The system shall provide a mechanism to determine if the user has enabled Auto Answer.	O
OSY.12	The system shall provide a notification mechanism if the Auto Answer has been enabled by the user.	O
OSY.13	The system shall provide the capability to disable Voice Mail during initial provisioning and at system boot/initialization.	T=O
OSY.14	The system shall provide the ability to prevent users from enabling Voice Mail.	T=O
OSY.15	The system shall provide the capability to disable Automatic Redial during initial provisioning and at system boot/initialization.	T=O
OSY.16	The system shall provide the ability to prevent users from enabling Automatic Redial.	T=O
OSY.17	The system shall provide the ability to disable all GPS and location services except E911 during initial provisioning and at system boot/initialization.	T=O
OSY.18	The system shall provide the ability to prevent users from enabling Location Service.	T=O
OSY.19	The system shall provide a mechanism to determine if the user has enabled Location Services.	O
OSY.20	The system shall provide the capability to disable processing of Messaging (includes SMS, MMS, Chat, IM and any other messaging service) during initial provisioning and at system boot/initialization.	T=O
OSY.21	The system shall provide the ability to prevent users from enabling incoming Messaging (includes SMS, MMS, Chat, IM and any other messaging service).	T=O
OSY.22	The system shall provide the capability to disable outgoing Messaging (includes SMS, MMS, Chat, IM and any other messaging service) during initial provisioning and at system boot/initialization.	T=O
OSY.23	The system shall provide the ability to prevent users from enabling outgoing Messaging (includes SMS, MMS, Chat, IM and any other messaging service).	T=O
OSY.24	The system shall provide a mechanism to determine if the user has enabled incoming or outgoing messaging.	T=O
OSY.25	The system shall provide the capability to disable incoming calls during initial provisioning and at system boot/initialization.	T=O

Req #	Requirement Description	Threshold / Objective
OSY.26	The system shall provide the ability to prevent users from enabling incoming calls.	T=O
OSY.27	The system shall provide the capability to disable outgoing calls during initial provisioning and at system boot/initialization.	T=O
OSY.28	The system shall provide the ability to prevent users from enabling outgoing calls.	T=O
OSY.29	The system shall provide a mechanism to determine if the user has enabled incoming or outgoing calls.	T=O
OSY.30	The system shall provide the capability to disable dial-up modem or tethering capabilities during initial provisioning and at system boot/initialization.	T=O
OSY.31	The system shall provide the ability to prevent users from enabling dial-up modem or tethering capabilities.	T=O
OSY.32	The system shall provide a mechanism to determine if the user has enabled dial-up modem or tethering capabilities.	T=O
OSY.33	System shall provide Full Disk Encryption (FDE) or an equivalent capability.	O
OSY.34	The USB shall have the ability to be used only to charge the battery, and not allow for data connections.	T=O
OSY.35	The system shall allow for Over the Air (OTA) updates from the carrier to be disabled.	T=O
OSY.36	The system shall support encrypted SD cards for storage.	T=O
OSY.37	The OS shall have the ability to run a firewall.	O

3.3.2 Security Relevant Components

The smart phone device will include two layers of encryption. The first layer or outer layer will be provided by a Virtual Private Network (VPN). The second layer or inner layer will be a Secure Voice over Internet Protocol (SVoIP) layer.

Two Layers of Encryption: In order to protect data in transit two layers of commercial encryption will be used. This will provide security for data carried over the untrusted carrier network portion of the path between two end user devices. All data between end user devices and the trusted network is protected in a VPN tunnel. Within this tunnel, the call signaling information sent via the Session Initiation Protocol (SIP) between end user devices and the SIP server is additionally protected using Transport Layer Security (TLS), and the call data (voice) between two end user devices is additionally protected using SRTP.

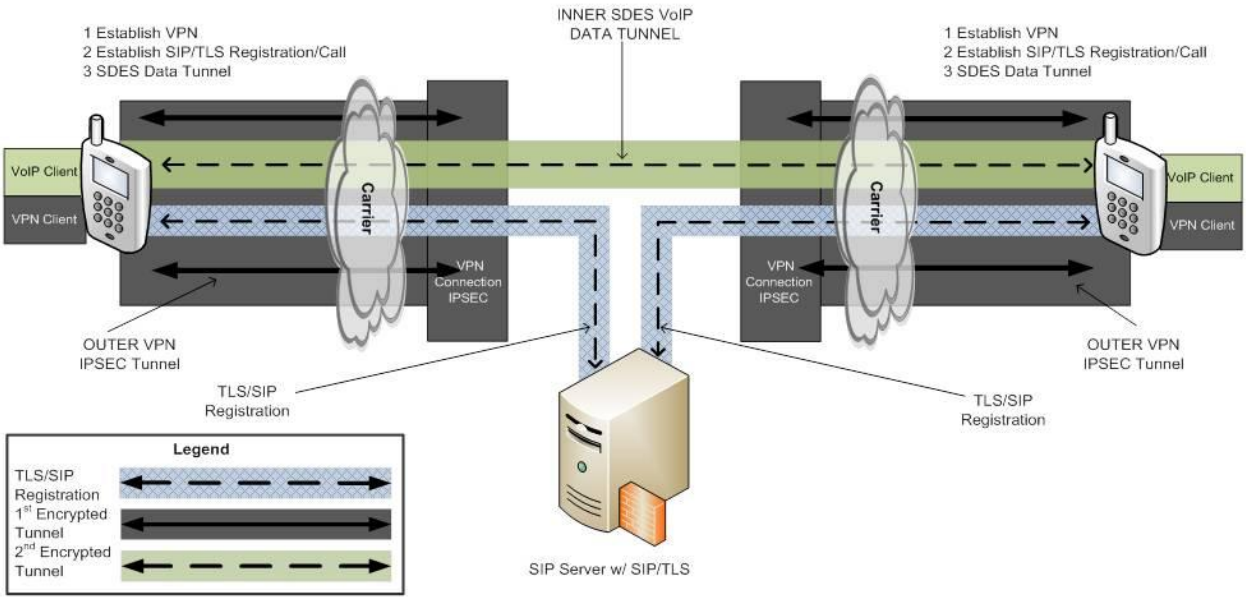

Figure 3-4 Two Layers of Encryption

Table 3-2 Virtual Private Network Requirements

Req #	Requirement Description	Threshold / Objective
OVP.1	The VPN shall have the ability to be configured so that split tunneling is prevented.	T=O
OVP.2	The VPN should run at the Operating System level, not as a separate application.	T=O
OVP.3	The VPN shall be configured to maintain the tunnel even if applications are not transmitting data.	O
OVP.4	The VPN shall authenticate in both directions.	T=O
OVP.5	The VPN shall be a non-proprietary standards based solution.	T=O
OVP.6	The VPN client and VoIP client shall be from different vendors.	T=O
OVP.7	The VPN client and VoIP client software shall not use the same software libraries or depend on the same services.	T=O
OVP.8	The VPN client and VoIP client shall not use the same randomizer.	T=O

3.3.2.1 Encryption Keys

Encryption keys are generated on a per-session basis by one or more of the communicating components for each of the two layers of encryption. No encryption keys are permanently stored on the mobile devices or in the network infrastructure.

Table 3-3 Encryption Key Requirements

Req #	Requirement Description	Threshold / Objective
OEK.1	The ephemeral session encryption key for the VPN encryption shall be generated on a per-session basis using a key exchange between the mobile device and the VPN concentrator.	T=O
OEK.3	The ephemeral session encryption key for the SRTP VoIP encryption shall be generated on a per-session basis by the mobile device, and sent through the SIP server to the other mobile device within a SIP message (using SDES).	T=O
OEK.4	The TLS encryption shall meet the requirement as defined in RFC 6460 “Suite B for TLS”, Annex A “A Transitional Suite B Profile for TLS 1.1 and 1.0”	T
OEK.5	All SIP messages between the phones and the SIP server shall use TLS.	T=O
OEK.7	The TLS encryption shall meet the requirement as defined in RFC 6460 “Suite B for TLS”.	O

3.3.2.2 Authentication Certificates and Keys

Public key certificates and their corresponding private keys are used to provide user and system authentication before establishing each of the two layers of encryption.

Table 3-4 Certificate and Key Requirements

Req #	Requirement Description	Threshold / Objective
OCK.1	The user authentication private key and the server certificates shall be stored on the end user device and encrypted using an auxiliary password.	T=O
OCK.2	The certificate protection password shall support a minimum of 8 characters long, and be allowed to consist of any combination of upper case letters, lower case letters, digits, and symbols.	T=O
OCK.3	The VPN authentication certificates and the SIP/TLS authentication certificates shall be issued by two different CAs.	T=O
OCK.4	Every device/component shall be issued different certificates and corresponding private keys.	T=O
OCK.5	The VPN component of each mobile device shall support the ability to securely contain a unique public key certificate and corresponding private key, used to provide authentication of the mobile device to the network infrastructure, in order to establish a secure communications channel (VPN) with the network infrastructure.	T=O

Req #	Requirement Description	Threshold / Objective
OCK.6	The SVoIP component of each mobile device shall support the ability to securely contain a unique public key certificate and corresponding private key, used to provide authentication of the mobile device to the SIP server, in order to establish a secure communications channel for sending and receiving SIP messages using TLS.	T=O
OCK.7	The client application shall support the storage of encrypted keys and certificates on the SD cards.	T=O
OCK.8	The SIP server shall support the ability to securely contain a unique public key certificate and corresponding private key, used to provide authentication of the SIP server to the mobile device, in order to establish the TLS channel for SIP messages.	T=O

3.3.2.3 Key Storage and Protection

As stated in the section above, public key certificates and their corresponding private keys are used to provide user and system authentication before establishing each of the two layers of encryption.

The private key and security critical profile protections are stored on the smart-phones. The requirements outlined below allow these keys to be protected, and by using a RAM disk temporary file mounting functionality, the keys are processed via volatile memory through a defined virtual path. Additionally, these requirements will also provide a level of key protection and will monitor the established VPN tunnel for the appropriate key protection events.

Table 3-5 Key Storage & Protection Requirements

Req #	Requirement Description	Threshold / Objective[1]
OKP.1	Each system shall have the ability to provide a level of security and key management for private keys and security critical profiles stored on the device.	T=O
OKP.2	The system shall provide the ability for the provisioning GUI to hash the contents of each of the unencrypted credentials and store the hash value in a separate plaintext file corresponding to that certificate.	T=O
OKP.3	Each hash file shall be stored in the VoIP or VPN data folder, read-only, directory of the phone.	T=O

Req #	Requirement Description	Threshold / Objective[1]
OKP.4	The system shall have the ability to prompt the handset user for the password assigned to them and used during the provisioning process to encrypt the private keys.	T=O
OKP.5	The system shall have the ability to run the password through a password based key derivation function (PBKDFv2) to generate an encryption key.	T=O
OKP.6	Once the key is generated, it shall be fed into AES-CTR to decrypt the encrypted private keys that are resident under the VoIP and VPN respective data folders.	T=O
OKP.7	The system shall have the ability to stream input data from the VoIP and VPN data folders to the virtual temporary file system of the handset that has been mounted in memory in order to allow the certificate decryption process to function.	T=O
OKP.8	The VPN client application shall be able to store the private keys unencrypted on volatile memory.	T=O
OKP.9	The VoIP client application shall be able to store the private keys unencrypted on volatile memory.	T=O

3.3.2.4 Client Device Monitoring

In order to ensure the handset operates under authorized or known conditions, a monitoring service must be available on the device. This service will be able to monitor the residing operating system, processes, applications, files, and I/O port activities. If a security fault is detected, the monitoring service will be able to write a log entry and notify the user of the unauthorized event. The monitoring service will also cease operation of the phone, and require the user to determine a course of action (reboot, shut down, or continue to operate in an un-trusted condition) for the detected event.

The following table outlines the requirements that make up the monitoring service.

Table 3-6 Device Monitoring Requirements

Req #	Requirement Description	Threshold / Objective
ODM.1	The monitoring services shall have the ability to monitor device activities such as the OS, i/o port activities, files, applications, and processes.	T=O
ODM.2	The monitoring services shall have the ability to log unauthorized events or security faults in the handset's system log.	T=O
ODM.3	The monitoring services shall have the ability to notify the user of an unauthorized event.	T=O

Req #	Requirement Description	Threshold / Objective
ODM.4	The monitoring services shall have the ability to cease operation of the phone and require the user to determine course of action (reboot, shut down, or continue to operate in an un-trusted condition).	T=O
ODM.5	The monitoring services shall have the ability to gain administrative access to the device using a custom file which provides administrative privileges to execute an initialization script.	T=O
ODM.6	The monitoring services shall have the ability to gain administrative access to the device using a custom file which provides administrative privileges to execute and perform certain OS level and file directory monitoring services.	T=O
ODM.7	The monitoring services shall have the ability to remove all functionalities, files, and applications that are not desirable on startup.	T=O
ODM.8	The system shall not have any feature that will be capable of "Phoning home" or reporting back to a centralized vendor-managed server.	T=O
ODM.9	The monitoring service shall have the ability to categorize unauthorized events into two classes: Major and Minor faults.	T=O
ODM.10	The monitoring services shall be able to detect and record to the system log in response to a Minor Fault.	T=O
ODM.11	In response to a Minor Fault, the monitoring service shall have the ability to notify the user unauthorized file system changes, unauthorized process detections, and SD card mounting or unmounting/removal.	T=O
ODM.12	The monitoring service shall have the ability to kick off a notification which shows up in the Notification Bar, accompanied by incessant vibration and an icon indicating that the monitoring application detected some event.	T=O
ODM.13	In response to a Major Fault, the monitoring service shall have the ability to remove any files containing encrypted or decrypted certificates or key material (thus rendering the device permanently unable to connect to the VPN until it is taken back to be re-provisioned).	T=O
ODM.14	In response to a Major Fault, the monitoring service shall have the ability to kill the VPN package manager utility.	T=O
ODM.15	In response to a Major Fault, the monitoring service shall have the ability to kill the VPN client process.	T=O

Req #	Requirement Description	Threshold / Objective
ODM.16	In response to a Major Fault, the monitoring service shall have the ability to unregister the phone call blockers to allow standard phone calls (until phone is power-cycled, after which the standard phone calls will again be blocked).	T=O
ODM.17	In response to a Major Fault, the monitoring service shall have the ability to log and generate a detailed notification to inform the user.	T=O
ODM.18	Major Faults will be classified when the following occur: "Enabled" WiFi State detected, "Enabled" Bluetooth adapter detected, USB data connection detected, and when 911 was dialed.	T=O
ODM.19	The monitoring service shall have the ability to allow 911 calls. 911 must be allowed, but a Major Fault response is necessary because the phone would be in an unsafe state.	T=O
ODM.20	The monitoring service shall have the ability to allow standard phone calls in the event a 911 responder needs to call the phone back.	T=O
ODM.21	In the event of a 911 call, the monitoring service shall not vibrate the phone, as the user will be attempting to talk to the 911 responder at that time.	T=O
ODM.22	The monitoring service shall have the ability to enable standard phone calls in response to a Major Fault	T=O
ODM.23	In response to a Major Fault the monitoring service shall only allow the phone to remain enabled until power cycle (device turned off and back on). Upon startup, ability to re-disable standard phone calls.	T=O
ODM.24	After a Major Fault the monitoring service shall upon startup re-disable standard phone calls.	T=O
ODM.25	The monitoring service shall have the ability to detect the removal and insertion of the SD card. .	T=O
ODM.26	The monitoring service shall have the ability to receive one or both of the broadcast messages in the event an SD card is unmounted through programmatics or physical removal.	T=O
ODM.27	The monitoring service shall have the ability to receive a broadcast message when the SD card is mounted, inserted, and no errors occur while mounting.	T=O
ODM.28	The monitoring service shall have the ability to generate a Minor Fault indicating which particular SD card event occurred.	T=O
ODM.29	The monitoring service shall have the ability to block incoming and outgoing phone calls that are not 911 related.	T=O

Req #	Requirement Description	Threshold / Objective
ODM.30	The monitoring service shall have the ability to dynamically register the phone call blockers.	T=O
ODM.31	The monitoring service shall have the ability to log incoming or outgoing phone calls if they are blocked and initiate a message to the user instead of a formal notification.	T=O
ODM.32	The monitoring service shall have the ability to monitor the OS file system to monitor different types of specified events that could take place in a directory or to a specific file.	T=O
ODM.33	The monitoring service shall have the ability to receive detected events written to the system log, and based on a priority level, initiate corresponding notifications to the user.	T=O
ODM.34	The monitoring service shall have the ability to re-disable the WiFi state if it is enabled, log the event, and generate a Major Fault response.	T=O
ODM.35	The monitoring service shall have the ability to periodically take a snapshot of which processes are running in memory to determine which processes are permitted to be running.	T=O
ODM.36	The monitoring service shall have the ability to compare processes from snapshots taken. The monitoring service shall have the ability to compare any new processes to a specified white-list, detect any differences, and generate a notification to the user if a process is not defined on the white-list.	T=O
ODM.37	The monitoring service shall have the ability to block the service which allows applications to run the camera resource.	T=O
ODM.38	The monitoring service shall have the ability to detect the mounting of USB as mass storage and generate a Major Fault.	T=O
ODM.39	The monitoring service shall have the ability to authenticate applications which request administrative user permissions.	T=O

3.3.2.5 Trusted Provisioning

Req #	Requirement Description	Threshold / Objective
ODP.1	During provisioning and updates the administrative user shall have the ability to remove and uninstall any applications, processes, and files that are not essential for operation of the handset.	T=O
ODP.2	During provisioning and updates the administrative user shall have the ability to run as administrator in order to perform most of its functions.	O

Req #	Requirement Description	Threshold / Objective
ODP.3	During provisioning and updates the administrative user shall have the ability to white-list applications that should not be removed from the handset	T=O
ODP.4	During provisioning and updates the administrative user shall have the ability to black-list miscellaneous files on the handset for removal including files to disable peripherals and other features on the handset	T=O
ODP.5	During provisioning and updates the administrative user shall have the ability to kill an identified list of processes each time the handset is provisioned or is booted	T=O
ODP.6	The system shall have the ability to notify the administrator during the provisioning process of the number of successful and unsuccessful application removals.	T=O
ODP.7	The system shall have the ability to notify the administrator during the provisioning process of the number of successful and unsuccessful miscellaneous file removals.	T=O
ODP.8	The system shall have the ability to notify the administrator during the provisioning process of the number of successful and unsuccessful process terminations.	T=O
ODP.9	During provisioning and updates the administrative user shall have the ability to remove the ability for ordinary users to attain administrative user privileges.	T=O
ODP.10	During provisioning and updates the administrative user shall have the ability to clear the contents of the cache. The cache is cleared to remove any data associated with the unwanted applications that were removed earlier. This allows a clean-slate of cache to begin operation after provisioning.	T=O
ODP.11	During provisioning and updates the administrative user shall have the ability to reboot the phone handset as its final action. The reboot will allow for a fresh initialization of the kernel and the applications remaining on the handset, as well as a fresh load of the boot image.	T=O

3.3.2.6 Password Protections

The user must first enter a password in order to unlock the end user device for use. The user must then enter another password in order to decrypt the certificates and private keys needed for the VPN and VoIP applications. Additionally, the VoIP application uses a username and password in order to register its location to the SIP server before any calls can be made.

Table 3-7 Password Protection Requirements

Req #	Requirement Description	Threshold / Objective
OPW.1	The screen lock password shall be at least four characters long.	T=O
OPW.2	The screen lock shall support locking the screen for a configurable amount of time after a configurable number of incorrect attempts.	T=O

3.3.2.7 SVoIP Requirements

The Secure Voice over IP Application (SVoIP) provides the inner layer of protection for mobility services and enterprise services required to enable calling to/from "unanticipated users"" and mobile-to-mobile secure calls. The SVoIP application also enables interaction with enterprise unified communications services (e.g., enterprise email, contacts, calendaring). TLS is used to protect SIP signaling messages against loss of integrity, confidentiality and against replay. It provides integrated key-management with mutual authentication and secure key distribution. TLS is applicable between mobile devices and SIP proxies, or between SIP proxies. The outer layer of protection is provided by using a VPN client that is integrated at the mobile device operating system level. The inner layer of protection between the SIP Server and VoIP clients is achieved through the use of a TLS protected channel for SIP signaling. The inner layer of protection between VoIP clients is achieved through the use of SRTP.

The Secure VoIP section describes the consumer components, mobility enterprise services components, management and provisioning components, and interactions required to enable a secure voice over secure IP call to/from 3G/4G mobile users. In addition to providing protection to disclosure of modification of communication, the TLS protocol described in this section offers mutual authentication between mobile devices and the SIP server in a cryptographically secure manner.

Figure 3-7 depicts the mobility components interactions in support of 3G/4G Secure Mobile to 3G/4G Secure Mobile (SVoIP).

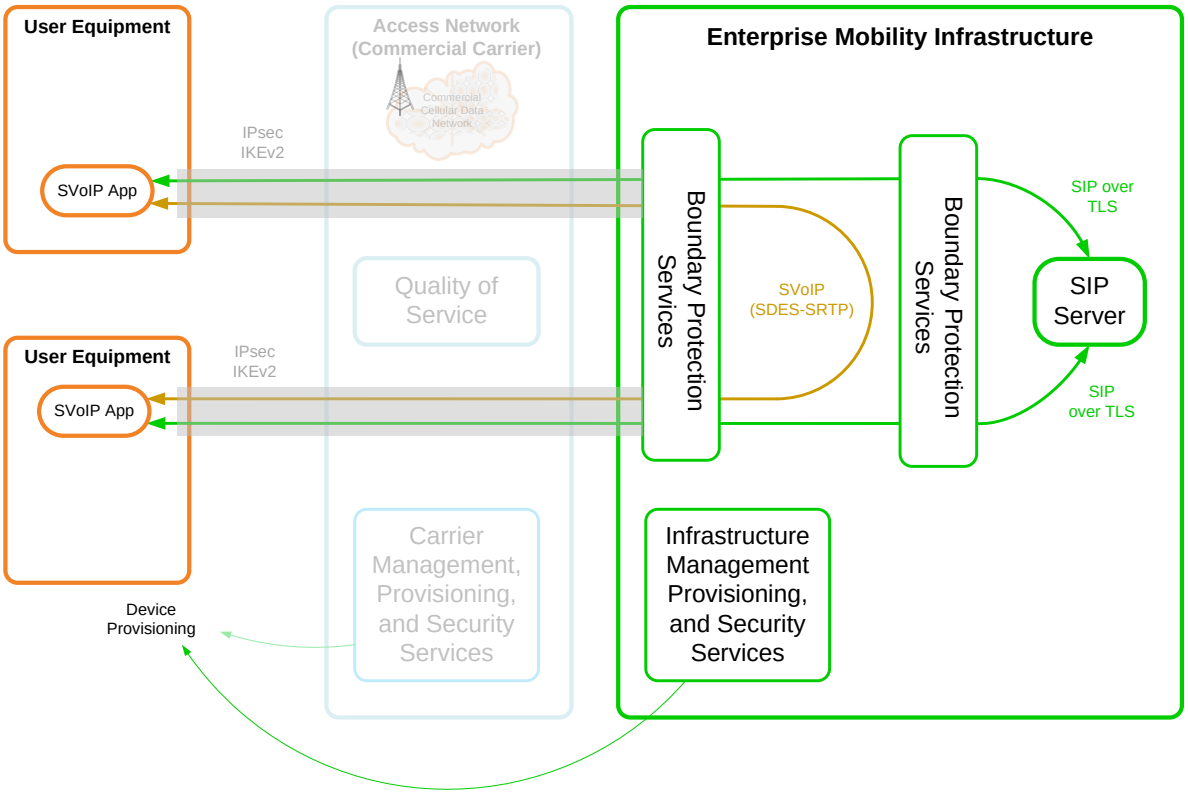

Figure 3-4 Basic SVoIP Architecture

In order to maximize the ability of the SVoIP clients to interoperate and provide the required levels of security, the client and server applications need to meet the following requirements.

Table 3-8 SVoIP Encryption Requirements

Req #	Requirement Description	Threshold / Objective
OSV.1	The mobility solution shall implement the Session Initiation Protocol (SIP) that complies with RFCs 3261, 4566, and 4568.	T=O
OSV.2	The mobility solution shall provide a password for client authentication for SIP REGISTER function requests.	T=O
OSV.3	The mobility solution shall protect the SIP communication channel using TLS.	T=O
OSV.4	The mobility solution shall implement the TLS 1.2 protocol (RFC 5246) supporting Suite B (RFC 6460) ciphersuites, using mutual authentication with certificates.	T=O

3.3.3 Inter-relationship to Other Elements of the Secure VoIP System

The phone must be a commercial device that supports the ability to pass data over a commercial cellular network. Standard voice phone calls, with the exception of emergency 911 calls, shall not be allowed. The phone must function on US CDMA & GSM networks and OCONUS on GSM networks with the same functionality.

All data communications to/from the mobile device must go through the VPN tunnel to the VPN gateway in the infrastructure; no other communications in or out of the mobile device are permitted.

Applications on the phone additionally encrypt their communications to servers in the infrastructure, or to other phones; all those communications must be tunneled through the VPN.

3.4 Gap Analysis

3.4.1 System Overview

Using Organization-Added Hardening and Monitoring: The configuration of the devices may be the only area where the using organization can make changes from a standard commercial device. In order to provide additional protection to the end user devices, some applications and services must be allowed to be removed, a monitoring application must be added, and tamper detection measures must be added. Hardening and monitoring can be achieved using applications installed during provisioning.

- Some applications and services removed – Certain applications and parts of the operating system can be security hardened. As part of the provisioning process, a system initialization script may be run to remove unwanted applications and turn off unneeded services.
- Monitoring service – Parts of the system kernel, the device drivers and part of the operating system cannot be security hardened, but can be monitored for unauthorized changes. Once the end user device is provisioned, it must have the ability to be monitored via a monitoring service. This application must start when the end user device is turned on, and continuously monitors the device to ensure it stays in a secure state. The system shall have a mechanism that executes at each boot to ensure that no new unauthorized software has been installed, and that all configuration settings are correct. The monitoring service shall be able to alert the user when issues are found, and logs the information locally to the end user device.
- Anti-tamper added – The device shall allow the using organization the ability to place tamper-evident seals and tape on key items such as the batteries and screw heads, and any removal able memory, such as an internal SD card, must have the possibility to be glued or otherwise permanently affixed into the device to prevent its removal or replacement. Anti-tamper measures do not have to prevent tampering, but to make any attempt to tamper with an end user device evident to a user.

3.5 Risk

3.5.1 Threats to the System

- An adversary updates software on an end user device using carrier Over-The-Air (OTA) update capability.

- An adversary establishes a rogue base station that can attack the end user device at the baseband level.
- An adversary sends AT commands to the end user device.
- An adversary installs malicious software (malware) on the end user device.
- An adversary physically tampers with the end user device.
- An adversary makes updates to the end user device or the user conducts activities that current monitoring systems are not able to detect or prevent.
- An adversary extracts the keys or certificates from the end user device.
- An adversary changes the hardware or software of the end user device while in the supply chain.

3.5.2 Risks to the System

End user devices provide a unique opportunity for an adversary to target individual users who are using mobile devices which are less mature (security-wise) than the other network technologies. Remote attacks against the end user device, other than via the carrier network, are limited by closing down a number of potential ingress paths (such as WiFi or Bluetooth) on the end user device via the monitoring services. Stealing or modifying an end user device would seem to be an attractive attack plan, particularly since user credentials are stored on the device, and both layers of encryption terminate on the device. However, the effort required by an adversary to attack a single end user device may not be worth it unless the targeted user is of particularly high value.

- It is important to note that the only security critical information stored on the end user device are the credentials used for authentication to the VPN gateway and SIP Server. An adversary who recovers a mobile device – even an active one – does not obtain any information that would help the attacker decrypt any past voice communications. Since the device is only used for voice communications, there is also no classified data (documents, email, etc.) stored on the end user device.
- In the event that an adversary acquires an active device that was lost or stolen, that adversary would be able access the organization's network or impersonate a user for some period of time (without modifying the mobile device in any way), until either the user reports the device as lost (at which time certificate revocation on the VPN will prevent any future network access), or the system requires re-authentication (which the adversary might not be able to provide). The credentials on the end user device would allow the adversary to connect to the VPN gateway in the network; this access into the network can allow the adversary to try to send traffic of his choosing further into the network in order to attempt to attack infrastructure components, or to send data to other phones in order to attempt to attack them. Again, the adversary would not obtain any information that would help the adversary decrypt any past voice communications.
- An adversary who obtains temporary possession of a device could attempt to modify it and return it to the user. Although government-added endpoint hardening (i.e., tamper detection) provides some assurance that a device has not been physically modified, some attempts by the adversary to modify the device may not be detected if the device were returned to the user. An adversary with physical access to the end user device may want to delete existing software and/or install malicious code on the device; however, the device is configured to disallow the installation of any software except at initial provisioning. If an adversary were to succeed, his

return could include exposing calls to and from that particular device, exfiltrating audio in the proximity of the device, or possibly using the end user device's VPN connection to the organization's infrastructure as a vehicle for attempting to attack the internal network (as above).

3.6 References

- RFC 2119 "Key words for use in RFCs to Indicate Requirement Levels"
- RFC 2543 "SIP: Session Initiation Protocol"
- RFC 4346 "The Transport Layer Security (TLS) Protocol Version 1.1"
- RFC 4492 "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)"
- RFC 6379 "Suite B Cryptographic Suites for IPsec"
- RFC 5246 "The Transport Layer Security (TLS) Protocol Version 1.2"
- RFC 6460 "Suite B Profile for Transport Layer Security (TLS)"
- RFC 3261 "SIP: Session Initiation Protocol"
- RFC 4566 "SDP: Session Description Protocol"
- RFC 4568 "Session Description Protocol (SDP) Security Descriptions for Media Streams"
- Security Requirements for Mobile Operating Systems, Protection Profile, Version 0.2, 9 December 2011
- Security Requirements for Voice Over IP Application, Protection Profile, Version 0.2, 9 December 2011

4 Carrier Services Connections

4.1 Overview

The Carrier Services portion of this document discusses the methods and features that enable the User Equipment – phones, laptops, tablets, etc -- to interface with the Government Controlled Infrastructure. Common access methods are cellular (2G, 3G, 4G, etc) and WiFi, though the scope of Section 4 for this release will focus exclusively on 3G cellular services.

4.2 Description

Because a carrier's job is to enable seamless communication between two User Equipments, the carrier must provide radio, mobility and policy control services.

Envision a time when you were outside with your cell phone and attempting to make a call, but could not, as you "had no service", or rather, your radio signal was too low. Being the most transparent aspect of the carrier services, the radio channel's existence, or non-existence, is felt by everybody. The radio channel, as the name implies, is the communication line comprised entirely of electromagnetic waves. Using different coding and modulation schemes, the User Equipment sends data through the radio channel to the base-station – the base-station being the tower-like structure with antennas frequently seen on the side of roads or on top of buildings. The base-station is the focal-point of a geographical area's radio-channel. The more base-stations that exist, the larger the area of coverage is for the carrier's radio channel. Coverage is the key here. An assumed aspect of the User Equipment to base-station interaction is the User Equipment's ability to process the signal – this happens in the baseband processor and will be covered in detail later. At the end of the day, a carrier is non-functional if the User Equipment has no radio channel to a carrier's base-station.

A carrier is also non-functional if the User Equipment is disconnected from a call session for moving out of range of the initial base-station's radio channel. A functional carrier should handle transferring the User Equipment's call path from one base-station to the next base-station; this is called mobility, and it is the second critical service a carrier provides. Assuming coverage exists, a User Equipment should be able to make a call in San Diego, CA and still be in the call when arriving in New York City, NY.

But, there's still the problem of the User Equipment being able to use the internet or other data services, or even worse from the carrier's perspective, there's the problem of identifying which User Equipment belongs to which carrier. The first problem is non-transparent as the typical user assumes that a decent radio signal means decent internet access, which is a reasonable expectation, but it disregards the routes and quality of service rules managed by the carrier to ensure an uninhibited user experience: 99% of users playing online games should not take precedence over the 1% opening a secure web-page. The second problem calls focus to the fact that the carrier should be able to manage who does and does not have access to their services. Typically, the User Equipment stores private credentials that are used to authenticate to the carrier, who contains the same private credentials. Exceptions exist, such as in the event the User Equipment wants to connect to a different carrier, but

even this “foreign carrier” knows the User Equipment is not one of their own, allowing the foreign carrier to make Quality of Service and charging rules. To summarize, the carrier must enforce quality of service and routing rules and provide an access control mechanism for User Equipments connecting to the carrier’s network.

4.3 Approach

4.3.1 Architecture

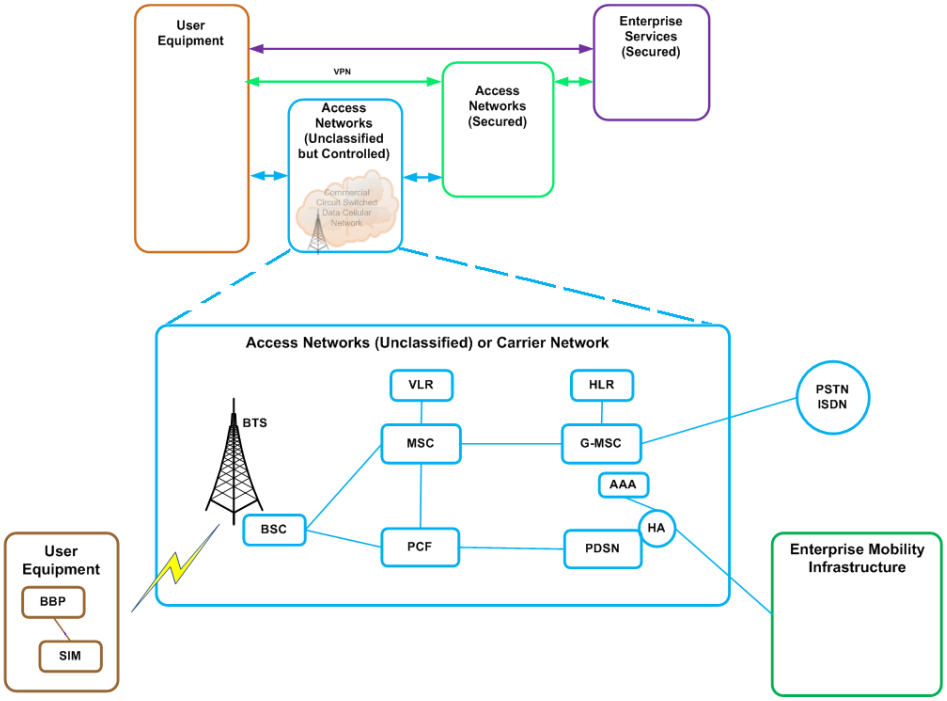

Figure 4-1 A Diagram of the Architecture with focus on the 3G Access Network

This architecture (Figure 4-1) represents the 3GPP2 specification for 3G access networks, and the following sections will describe each component. To get a broader picture, other 3G specification components will be described where necessary.

4.3.1.1 User Equipment – Identity Module

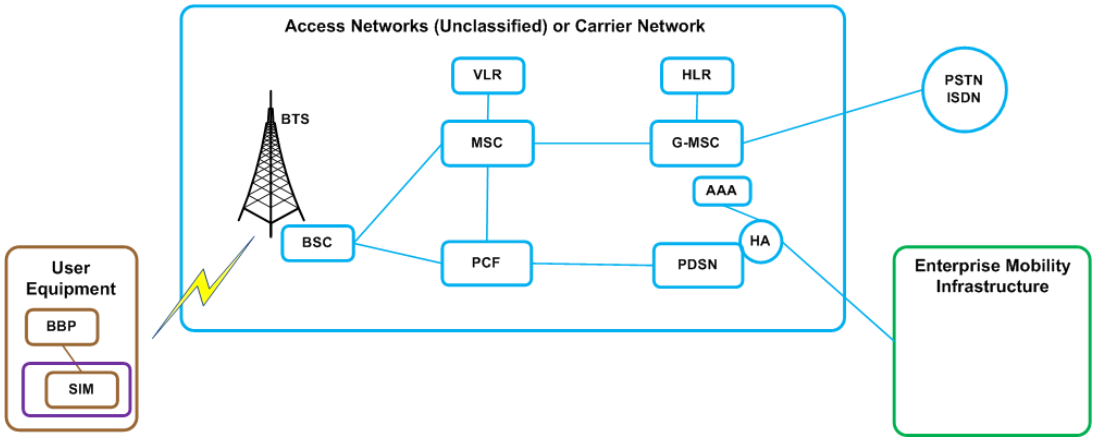

Figure 4-2 The 3G Access Network with focus on the Identity Module

The Identity Module (Figure 4-2) is the User Equipment's key to the carrier's network. There are two purposes the Identity Module serves: contain the subscriber ID and contain the private key to authenticate to a particular carrier service [1]. Generally, the subscriber ID will be the International Mobile Subscriber Identity which will be discussed in more depth later. The private key is a symmetric key stored on both the Identity Module and the carrier's authentication server; it is used in a challenge-response mechanism to authenticate the subscriber to the network. It is important to note that a private key will be stored for both voice and data. For instance, if the subscriber paid for both voice and data service, then two private keys will be stored, or derived, on the Identity Module: one for voice, one for data.

For 3G technologies, the Identity Module is known as the Subscriber Identity Module (SIM) card, UMTS Subscriber Identity Module (USIM) card [2], or Removable User Identity Module (R-UIM) [3].

4.3.1.2 User Equipment – Baseband processor

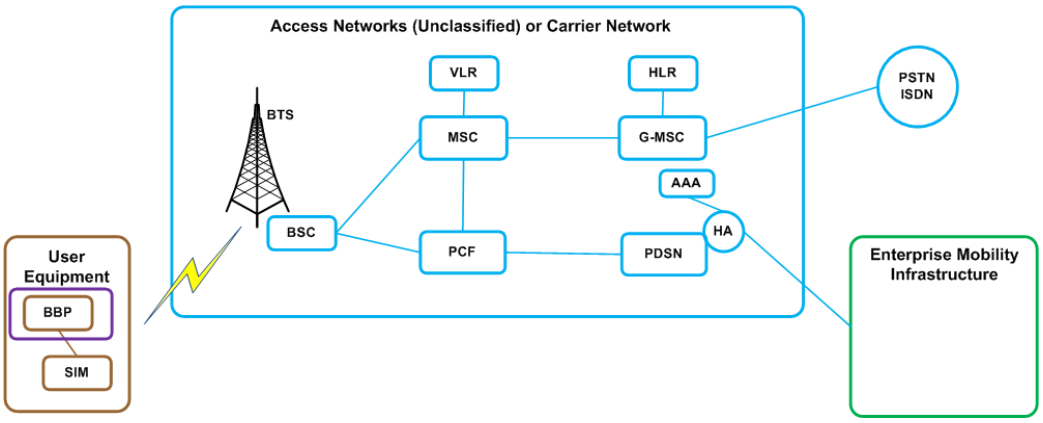

Figure 4-3 The 3G Access Network with focus on the Baseband Processor

The baseband processor (Figure 4-3) is the signal processor of the User Equipment – it handles the conversion of radio signals into digital messages that the application processor can use. The baseband processor was built according to a wireless standard, such as GSM, UMTS, and LTE etc. The relation between the baseband processor and the carrier is that the User Equipment is built according to the specifications set by the carriers. Tools inherent to the baseband processor, such as Attention (AT) commands, are standardized or built independent of the carrier's influence [4]. Certain carriers require that the baseband processor be provisioned with their public certificates and identity modules, but this is an agreement that would have happened post-manufacturing of the baseband processor.

4.3.1.3 Radio Access Network

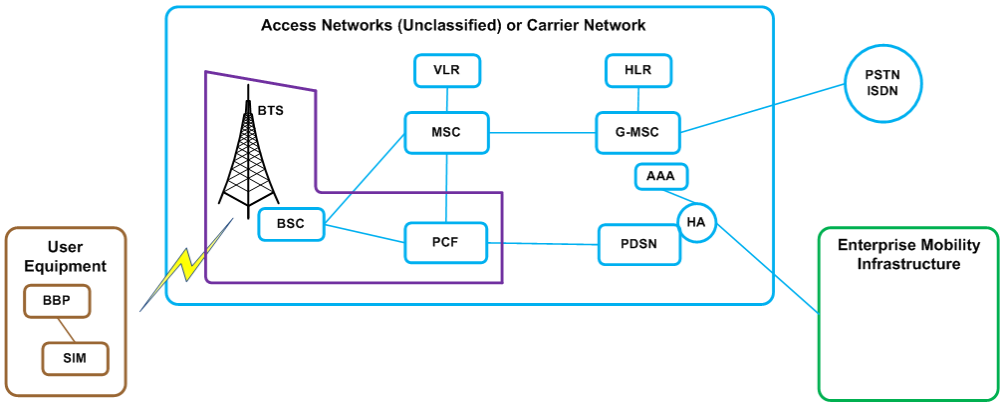

Figure 4-4 The 3G Access Network with focus on the Radio Access Network

The radio access network ((RAN) – Figure 4-4) encompasses the grid of base-stations – with their assumed radio channels – and the radio network controllers. Not much focus will be put on this area of the carrier, but it should be noted that the radio network controller is the device that splits the traffic between the voice and data paths. On CDMA networks, the Packet Control Function (PCF) is an additional technology required to handle the data services; it acts as a proxy for the core network with the added bonus of being aware of the User Equipment's location so that, if need be, it can reroute the data to another base-station assuming the User Equipment moves [5]. It is the User Equipment's anchor to the carrier's data infrastructure.

Depending on the 3G technology, The PCF may also be known as the Serving GPRS Support Node (SGSN) [6].

4.3.1.4 Core Network – Packet Data Serving Node

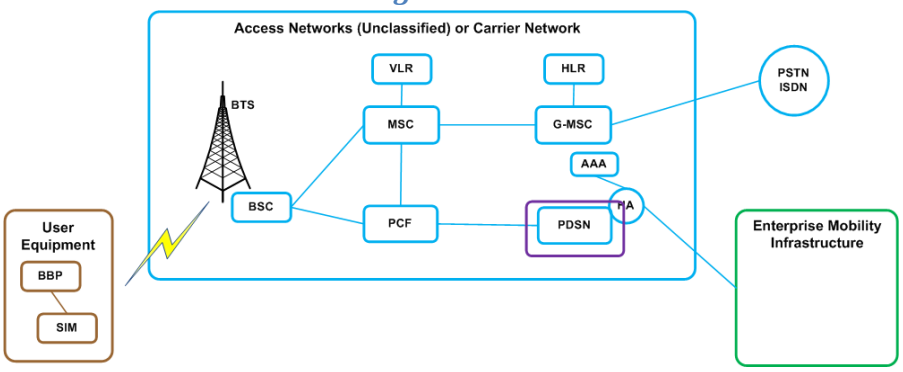

Figure 4.3.1.4 The 3G Access Network with focus on the Packet Data Serving Node

The Packet Data Serving Node (PDSN) is the entity within the carrier's infrastructure that handles the routing of data services and allocation of the User Equipment's IP address [5].

4.3.1.5 Core Network – Home Agent

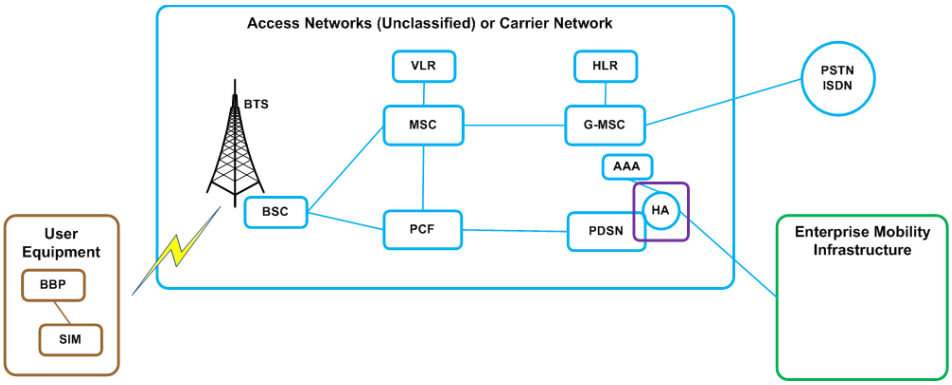

Figure 4-5 The 3G Access Network with focus on the Home Agent

The Home Agent (Figure 4-5), closely tied with the PDSN, is the carrier's gateway to the internet – it has a publicly routable IP address [5]. In addition, if control requests are received from the PDSN (if the phone is establishing a data path or trying to authenticate to the network), the Home Agent will forward on these requests to the appropriate server – most likely the Authentication, Authorization and Accounting server. Traffic originating from foreign agents destined for a User Equipment on the carrier's home network will be tunneled to the User Equipment via the home agent.

The combination between the Home Agent and the PDSN may be referred to as the Gateway GPRS Support Node (GGSN) [6].

4.3.1.6 Core Network – Authentication, Authorization and Accounting

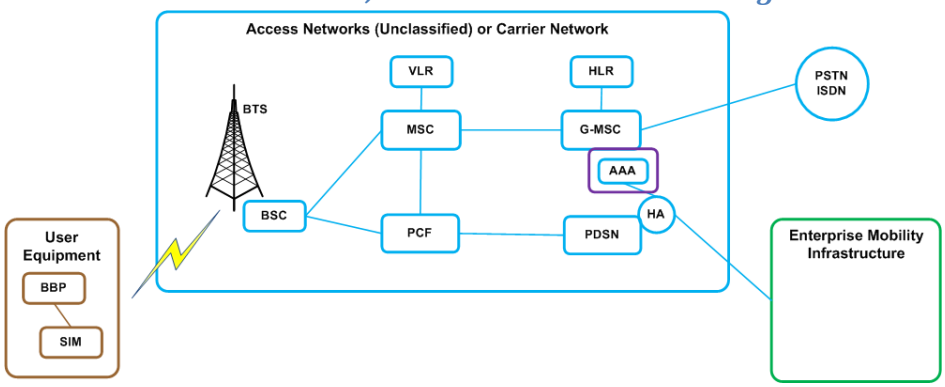

Figure 4-6 The 3G Access Network with focus on the Authentication, Authorization and Accounting server

Based on requests received from the PDSN, the Authentication, Authorization and Accounting (AAA) server (Figure 4-6) will perform the operations necessary to controlling what User Equipment uses the carrier's services [5]. Recall that during the User Equipment's provisioning process the Identity Module was given a private key: the same private key is stored on the AAA server. In this way, a Pre-Shared Key authentication mechanism is used to identify trusted and foreign carrier User Equipments.

Another important feature of the AAA server is the handling of the subscriber's profile. The profile contains the subscription status and Quality of Service parameters (examples: Are they a premium member? Do they have video enabled?). Upon successful authentication of the subscriber, the profile will get sent to the PDSN and PCF for Quality of Service enforcement.

4.3.1.7 Core Network – Mobile Switching Center/Gateway-Mobile Switching Center

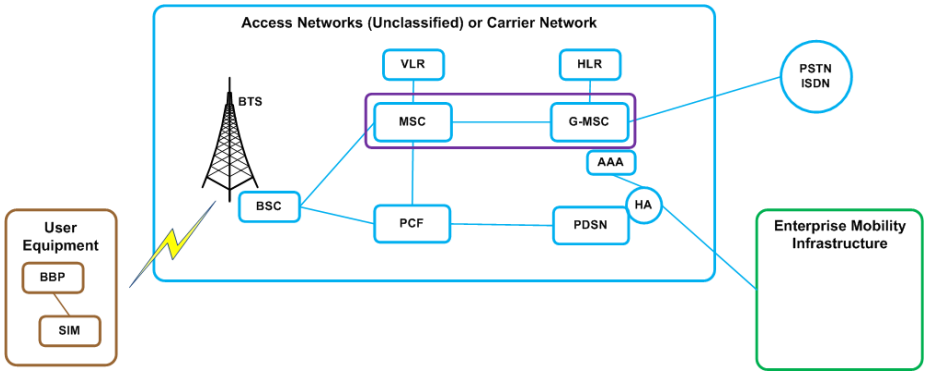

Figure 4-7 The 3G Access Network with focus on the Mobile Switching Center and its respective Gateway

The Mobile Switching Center (MSC) is the "routing" function for closed-circuit connections (Figure 4-7), aka voice [5]. The MSC acts as the User Equipment's anchor to the carrier's circuit-switched network and handles the forwarding of traffic to the Gateway-MSC. The Gateway-MSC translates the signaling mechanisms used in the circuit-switch network to PSTN traffic formats and acts as the gateway to the PSTN cloud.

Because the MSC/G-MSC operates in the circuit-switched domain, it is not applicable to the functioning of a secure Voice over IP solution (since VoIP is data traffic).

4.3.1.8 Core Network – Home Location Registry/Visitor Location Registry

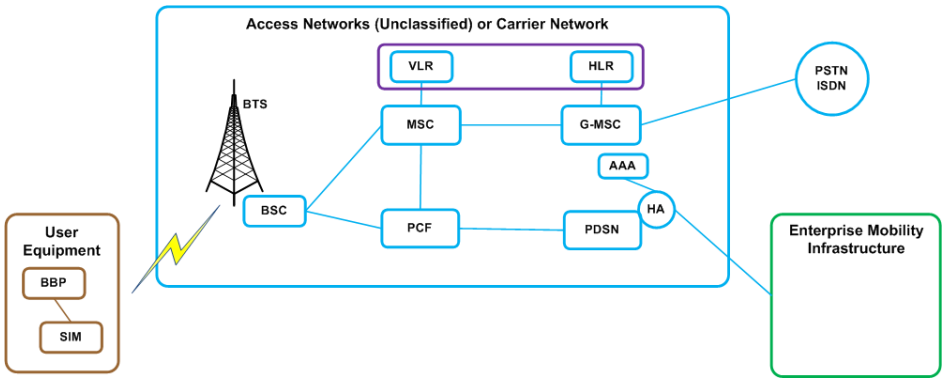

Figure 4-8 The 3G Access Network with focus on the Visitor Location Registry and Home Location Registry

The Home Location Registry (HLR- Figure 4-8) acts as the primary database for all the subscribers to the carrier's circuit-switched services [5]. Generally, the HLR will store the subscriber's identity, key, status and location information. The VLR is the same as the HLR but tendered towards the localized MSC. As an example, an MSC may serve a resident of San Diego. So when said resident attempts to connect to the network, the MSC will poll the VLR for their information. If a non-resident were to attempt to connect, the MSC would poll the VLR, find that this subscriber does not exist, and then poll the HLR to get the information.

Because the HLR/VLR operates within the circuit-switched domain, it is not applicable to the functioning of a secure Voice over IP solution.

4.3.1.9 Core Network – Policy and Charging Rule Function

The Policy and Charging Rule Function node seeks to monitor a subscriber's data usage in order to charge the subscriber [7].

4.3.1.10 Core Network – Emergency 9-1-1

Emergency 9-1-1 is a service in the United States required by law to be implemented and functional on a User Equipment. Emergency 9-1-1 will work on all User Equipment's whether or not a connection to the carrier was established, though a radio channel is still required [8]. A feature of 9-1-1 is the User Equipment uses geo-location to determine the nearest dispatcher.

4.3.1.11 Core Network – Location Based Services

There are certain third-party services or technologies that may require the User Equipment's location to be known at all times; it is for this business case that carriers will often provide Location Based Services on behalf of the User Equipment or third-party. For Enhanced 9-1-1, it will be a requirement for the calling User Equipment's location to be known so that geo-coordinates may be provided to the EMT for faster service [9].

4.3.1.12 Over-the-Air Update

Several standards have been established that enable the carriers to silently push updates to the User Equipment via the radio channel [10]. This may happen through either the voice or data paths and are processed on the User Equipment's baseband or application processor. The security mechanisms of the updating procedure will be discussed later.

4.3.1.13 Roaming Services

In the event the User Equipment traverses to a foreign network, SMS procedures may be pushed to the User Equipment to initiate a roaming agreement. This happens with or without the subscriber's acknowledgement, though most phones have an option to enable or disable roaming.

4.3.1.14 Lawful Intercept

A feature common to most PDSN/GGSN/P-GWs is the ability to intercept traffic for government agencies and law enforcement's use.

4.3.2 Security Components

These are the components inherent to the carrier's services that protect the User Equipment from unauthorized behavior or data leakage.

4.3.2.1 Subscriber Identity

The User Equipment provides the subscriber identity to the carrier to enable the carrier to initiate the authentication procedure; in this way, the subscriber identity is the value in the AAA or HLR to look up to determine what private key to use for which service. The subscriber identity being provided ensures that no passive collection technologies may intercept the private key; without knowledge of the User Equipment's private key, authentication and encryption would be impossible.

Depending on the technology, the subscriber identity may be referred to as the International Mobile Subscriber Identity (IMSI) or the combined Mobile Identification Number (MIN) and Electronic Serial Number (ESN).

4.3.2.2 Packet Temporary Mobile Subscriber Identity

The Subscriber Identity's security fails due to the fact that it can be tracked. If knowledge of the subscriber's identity is gained, it is possible to track all services rendered, though they may be encrypted. Thus, certain 3G technologies use temporary subscriber identities in place of the subscriber identity when authenticating to the carrier's network. This obfuscates the subscriber's voice/data usage for a time – either until a new temporary identity is assigned or a passive collector associates the temporary identity with the subscriber.

4.3.2.3 Identity Module Protection

As much of the security of the carrier relies on the private key stored in the identity module, measures exist that prevent unauthorized disclosure of the private key to the application or baseband processor. GSM 11.11 defines the different read/write/update mechanisms that allow the baseband/application processor to talk to the identity module, and ISO/IEC 7816-4 further specifies the Application Protocol

Data Unit as the standard communication method between the User Equipment's processors and the identity module [1][11]. The data on the identity module is held in a hierarchical file system where the core data is stored in units called Elementary Files; the keys would be stored in their own Elementary Files. The Elementary Files have specific permissions, so if a rogue request were to come from the baseband/application processor without proper permissions, the identity module would send back a failure message without compromising any data.

The standards do not define a mechanism to protect the private keys from forensics analysis. The keys are presumably stored in the identity module's memory unencrypted.

4.3.2.4 Quality of Service

The ability to prioritize traffic based on need and bandwidth constraints would place Quality of Service (QoS) functionality under the availability umbrella of security. Quality of Service was included in this section as there are limited 3G technologies that properly handle QoS enforcement for data usage, but it is not widespread. A properly functioning QoS mechanism would enable a leader in an emergency to have uninhibited carrier service using a commercial User Equipment.

4.3.2.5 Encryption

An optional feature for most 3G carriers is encryption on the radio channel [5]. This prevents passive collection units from sniffing the radio channel and siphoning off a subscriber's traffic. As was discussed earlier, the identity module contains a key for either voice or data; this means there will be two independent encryption sessions depending on which carrier service is being used by the User Equipment. It needs to be stressed that encryption is only between the User Equipment and the base-station; once the subscriber's traffic touches the core network, it is unencrypted.

4.3.2.6 Integrity Protection

An optional feature for most 3G carrier's is integrity protection on the radio channel, and to that end, it tends to only affect signaling/control traffic [5] [12]. Integrity ensures that no data is modified or subverted while in transit. The key used for integrity protection would be separate from the key used for encryption. This key would be stored in the identity module.

4.3.2.7 Firmware Updates Over-the-Air

There are two security mechanisms associated with firmware updates: validating the connection to the carrier's update server and validating the authenticity of the update package. Ownership of the update package is claimed by the manufacturer; the carrier only provides a means to receive the package, over-the-air. A commonly accepted phrase for this process is Over-the-Air updating.

In order to validate the connection to the carrier's update server, the carrier's public certificate must be present on every User Equipment; this provides the User Equipment with a trust anchor. Typically, the carrier's public certificate is stored in non-volatile memory with root permissions. In the event the User Equipment was to connect to a malicious update server, the carrier's public certificate on the User Equipment would invalidate the connection, halting the download. It should be noted that validation to

the carrier's update server is not always required. There are instances where carrier's have no control over the update package, and thus, provide a direct link to the manufacturer.

The update package is controlled by the manufacturer. Even if a carrier were to maliciously modify an update package provided by the manufacturer, certificates burned into hardware fuse-arrays on the User Equipment would prevent installation of a modified update package.

4.3.2.8 Identity Module Provisioning Over-the-Air

Similar to Firmware updating, Identity Module Provisioning pertains to the updating of the User Equipment's identity module, settings and applications through SMS. This process is exclusively handled by the carrier [10].

The User Equipment's identity module contains a set of keys associated with a particular security domain; similar to the secure partitioning between voice and data services. The set of keys allow for integrity and confidentiality of the keys to be assured. The SMS that is sent to the phone contains a security session profile, used to tell the identity module how the provisioning session will be protected (examples: What encryption algorithm? What key will be used for integrity?). If the SMS is requesting an unsupported feature from the identity module, the provisioning request will be ignored by the identity module.

In some instances, the connection to the carrier's provisioning server is secured through a one-way authentication scheme. This assures the User Equipment that it is connecting to a trusted entity and not a rogue provisioning server.

4.3.3 Inter-relationship to Other Elements of the Secure VoIP System

This section provides context for how the carrier services interface with the rest of the secure VoIP architecture.

4.3.3.1 Identity Module to Baseband/Application Processor

This section details the communication channel between the identity module, owned by the carrier, and the baseband/application processor, owned by the manufacturer.

4.3.3.1.1 Application Protocol Data Unit

The Application Protocol Data Unit (APDU), as mentioned in section 4.3.2.1, is the message that enables the User Equipment to select, read or update files on the identity module. The identity module may optionally return data requested by the User Equipment but is required to provide a status response of the message request, be it success or failure. It is important to recognize that APDUs originate from the User Equipment.

4.3.3.1.2 Proactive Commands

3G enabled the feature of allowing the identity module to issue commands to the User Equipment – these are called proactive commands [13]. The User Equipment will poll the identity module for a

command; if one exists, the User Equipment will act upon the command given. The following is an arbitrary sampling of some of the available proactive commands:

- Display Text: Displays text to the User Equipment's screen
- Provide local information: The identity module requests location information from the User Equipment
- Send Short Message: The User Equipment is to send an SMS message
- Set up call: The User Equipment is to make a voice call

4.3.3.2 Baseband to Application Processor

As the channel is dependent on the manufacturer, not much detail will be provided here, suffice it to say the communication that happens between the baseband and application processors is two-fold: serial and shared-memory. In the former case, commands and data are sent between the processors, originating from either, with the volatile memory being physically partitioned from the other – the memory is not shared. In the shared-memory case, the data stored in volatile memory is addressable by both the application and baseband processors.

4.3.3.3 Home Agent to Government Infrastructure

As mentioned in section 4.3.1.5, the Home Agent holds the publically routable address – this means all communication that happens between the Government Infrastructure and the carrier would be funneled through the Home Agent using IPv4 or IPv6 traffic.

4.4 Gap Analysis

The following is the wish-list for carrier services to enable a government controlled infrastructure and secure Voice-over-IP solution. All pertain to the security of the subscriber and the subscriber's data.

4.4.1 Secure Roaming

Global coverage is key for any communication solution, and to that end, the ability to talk globally through secure means is crucial. In the event a government customer connected to a foreign carrier network, the user equipment's control and user traffic should be protected during this transition. As an example, if a connection were established between a Foreign Agent and a Home Agent to accommodate a customer's roaming traffic, a secure data tunnel should be established between these two agents. To that end, the government customer's identity and AAA information should be protected from foreign carrier network traversal, to include the government customer's roaming list.

In the ideal scenario, the government would retain ownership over all the functions concerning roaming between foreign carriers, to include what information is provided to the foreign carriers and how the connections are established.

4.4.2 Network Authentication

Network Authentication is important as it enables the subscriber to have assurance on what carrier they are connecting to. Added benefits of network authentication would be mitigating the rogue base-station threat, as a subscriber's authentication would fail if the rogue base-station did not have access to the

carrier's or subscriber's private key. Commonly used network authentication mechanisms for 3G technologies use a challenge-response mechanism which relies on the secret of the subscriber's private key – usually put through a hashing function [12]. A more robust authentication mechanism would use a Public Key exchange, with the carrier and subscriber having their own public and private key pairs.

Ideally, the government would maintain and enforce all the policies governing carrier authentication of government users, to include government control of the storage of secure credentials and identity information for government users. Only government personnel should have access to the part of the carrier network that interfaces with the government enterprise network.

4.4.3 Audit System

To enable quick reaction capabilities, a functioning and maintained audit system on the core network would enable anomalies and breaches to be detected. One of the most important features a security professional has is the ability to discern the time and cause of a problem.

4.4.4 Secure Identity Module

The 3G specifications for identity module detail authentication, permission and storage directions for the subscriber identity and private keys, but in all cases, no additional protection of the identity module is detailed [1][3]. Measures for improving the security of the identity module would include:

- Encrypting the sensitive data – such as the private key – while not in use
- Providing support for subscriber to identity module authentication; it should not be assumed that just because a subscriber is in possession of the identity module they are the owner
- Physical security mechanisms such as Anti-Tamper switches or passive seals; forensics analysis should be non-trivial
- A hardware randomizer module that supports Operating System and Application use

Ideally, all management and control of a government user's identity module would be under the authority of the government. This control includes all aspects of provisioning the identity module and enforcing the policy dictated by the contents of the identity module.

4.4.5 Secure Over-the-Air Provisioning Server

As mentioned in section 4.3.2.8, the OTA provisioning server enables the carrier to push OS/application layer and identity module updates to the User Equipment, wirelessly. As compromise of the OTA provisioning server could lead to widespread exploitation, the OTA server and the server's connection must be protected. This can be done by keeping the OTA server in the government infrastructure -- or MVNO -- and using a two-way authentication mechanism to guarantee only trusted parties are connecting to the OTA server.

4.4.6 Quality of Service

Quality of Service is important as it provides a layer of assurance for communication during times where the carrier has high network load. To that end, the service priorities for government users are not necessarily the same as for the typical carrier user (online gaming should not hinder SSL connections).For this reason, quality of service policy provisioning and enforcement should be under the authority of the government.

4.5 Risk

The following are risks commonly associated with the carrier services. If any one of these gaps were exploited with malicious intent, compromise of the subscriber, or subscriber information, may yield undesired consequences.

4.5.1 Rogue Base-Station

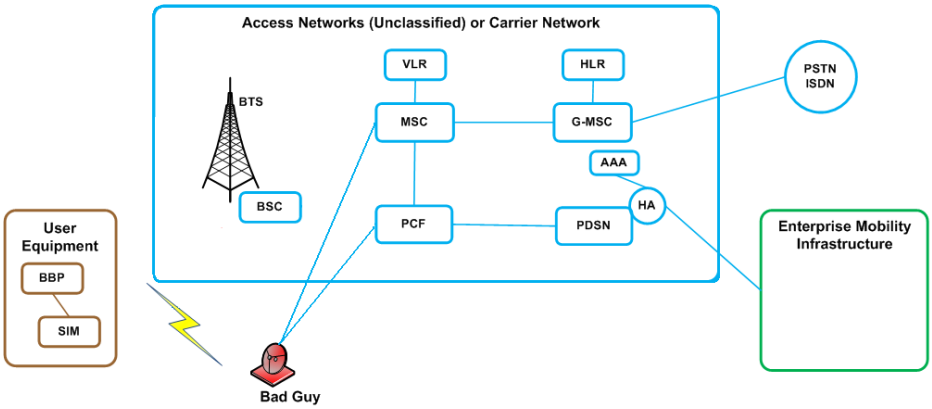

Figure 4-11 A symbolic representation of the Rogue Base-station attack

The idea is a malicious adversary (Figure 4-11) takes a commercially bought base-station and coerces a subscriber's User Equipment into thinking the adversary's base-station is the carrier's base station. If successful, the adversary would become a man-in-the-middle, able to collect and inject data wherever they please. The ability for an adversary to exploit this depends entirely on the 3G technologies used. For instance, it is easier to man-in-the-middle UMTS traffic than CDMA due to CDMA's coding of their signals; this statement should not misconstrue the word "easier" to assume that the man-in-the-middle of CDMA is impossible. It may just cost more.

4.5.2 Rogue Carrier

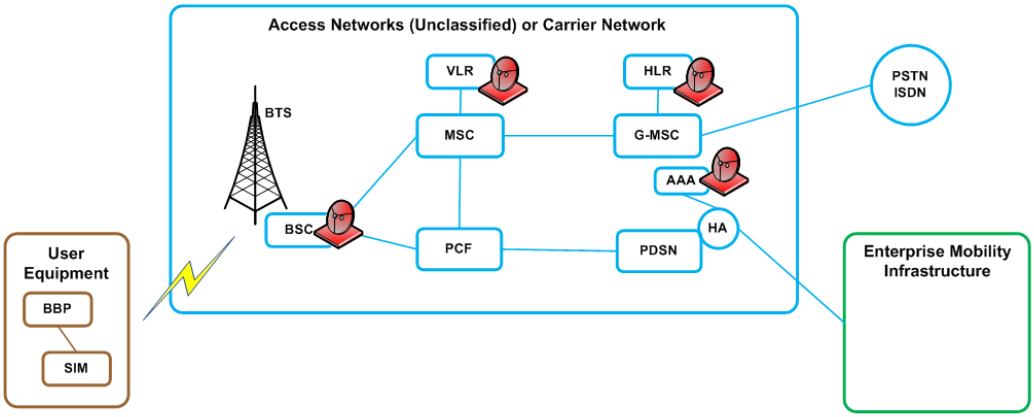

Figure 4-12 A symbolic representation of the Rogue Carrier and the areas of exploit

The idea is the carrier has malicious intent (Figure 4-12) and can no longer be trusted. This could happen due to a transition of company ownership or a disgruntled employee with access to the core network. The risks are several.

The User Equipment can no longer assume that it is connecting to the known carrier as the HLR and AAA servers have been compromised. If the private keys from these databases were provided to malicious agents, authentication of the carrier would fail to provide trust protection and confidentiality on the radio channel would become useless as the traffic could be decrypted or encryption could be disabled.

A malicious actor with access to the VLR/HLR and PCFs will have access to the location of the User Equipment in real-time.

A malicious actor with access to the PDSN or MSC would be able to collect all traffic unencrypted.

A malicious actor with access to the VLR/HLR would be able to distinguish between connections coming from a government's user equipment or a typical carrier customer's user equipment.

A malicious actor with access to the RAN would be able to push AT commands down to the baseband processor, allowing remote control of the User Equipment. AT commands only affect those functions that exist on the baseband processor, though research has shown that if shared memory exists remote exploitation of the application processor may be possible. The complete set of AT commands is comprised of the basic Hayes command set [4], GSM AT command set (3GPP TS 27.005) and manufacturer AT extensions -- which may be proprietary. The following AT commands were sampled from the mentioned former two data sets:

- A0 or ATA: Answer incoming call
- D: Dial a number

- AT+CLCK: Remove PIN code from User Equipment
- AT+CGDCONT: Defines a PDP context, or, forces the User Equipment to connect to a specific APN
- AT+CGSN: Return the IMEI number

Important note: A User Equipment having support for AT commands does not mean all commands are implemented; it is the manufacturer's decision.

4.5.3 Rogue Manufacturer/Supply Chain Compromise

The idea is the manufacturer of the User Equipment has somehow compromised the baseband processor or the firmware prior to the subscriber ever receiving the phone. This would enable a malicious agent to provide modified firmware updates to the carrier for the purpose of being pushed down to the User Equipment in a trusted context; the manufacturer certificate on the User Equipment would not be providing the intended validation mechanism.

In a different context, the User Equipment could have been manufactured with malicious hardware modifications that might enable data exfiltration – such as enabling a radio channel through a non-standard frequency.

4.5.4 Geo-location

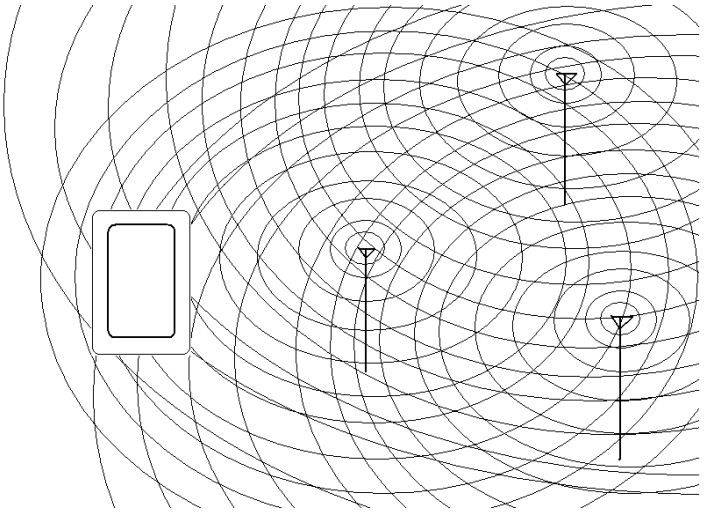

Figure 4-13 A symbolic representation of locating User Equipment via triangulation

A phenomenon relevant to all wireless devices is the propagation of their radio signals through the natural world. If a set of receivers are properly constructed for a particular frequency band, it is possible to determine the location of the origin of a particular signal – in this context, the origin of the signal would be the User Equipment (Figure 4-13).

4.5.5 Frequency Jamming

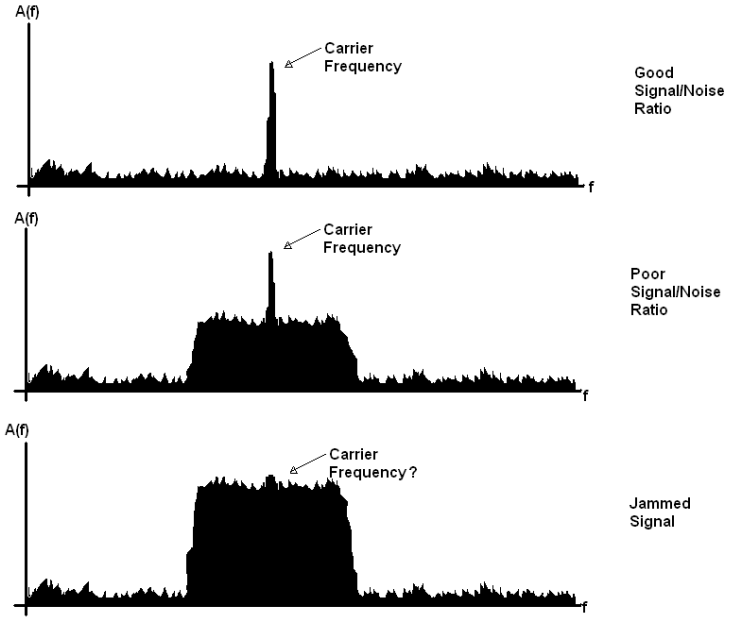

Figure 4-14 The frequency response of the radio channel in good, poor and jammed conditions

Wireless communication is dependent on a radio channel with a reduced noise floor; an increase in the amount of noise on the frequency band being used may result in transmission errors. If the noise floor is high enough for a particular frequency band, transmission through that band becomes impossible; if the noise floor was increased purposefully, this is called frequency jamming (Figure 4-14) and falls under the realm of denial-of-service attacks.

4.5.6 Passive Collection

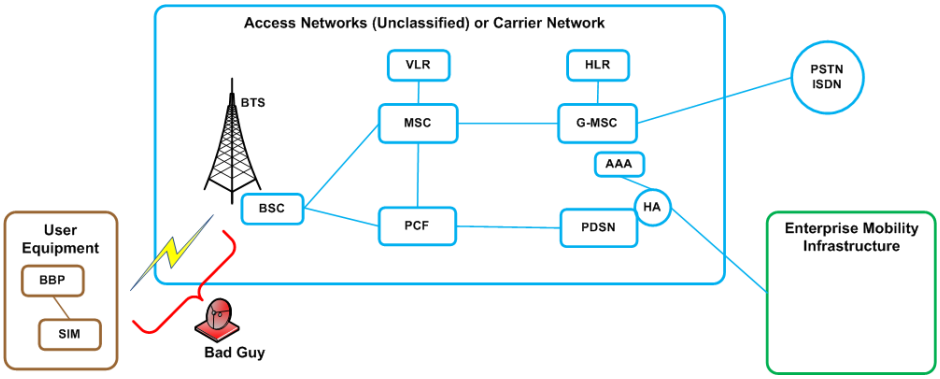

Figure 4-15 A symbolic representation of a passive collector

A person with a suitable receiver technology could sit in between the User Equipment and the base-station and collect all the traffic being exchanged (Figure 4-15). The risk here is that the carrier disabled encryption on the radio channel, enabling the collected traffic to be unencrypted.

4.6 References

[1] GSM 11.11, Digital cellular telecommunications system Specification of the Subscriber Identity Module – Mobile Equipment Interface; http://www.ttfn.net/techno/smartcards/gsm11-11.pdf

[2] 3G Release 4, Technical Specifications and Technical Reports for a UTRAN-based 3GPP system; http://www.3gpp.org/ftp/Specs/html-info/21101.htm

[3] CS0023-0, Removable User Identity Module for cdma2000 Spread Spectrum Systems; http://www.3gpp2.org/public_html/specs/CS0023-0.pdf

[4] The AT Command Set Reference – History; http://nemesis.lonestar.org/reference/telecom/modems/at/history.html

[5] Overview of 3G Packet Data; http://adaptive.ucsd.edu/2003_salih_3Gdata.ppt

[6] 3G Tutorial, UMTS Overview; http://www.umtsworld.com/technology/overview.htm

[7] Policy Charging and Rules Function; http://en.wikipedia.org/wiki/PCRF

[8] 9-1-1, http://en.wikipedia.org/wiki/9-1-1#Wireless_telephones

[9] Enhanced 9-1-1, http://en.wikipedia.org/wiki/Enhanced_9-1-1

[10] WAP Provisioning Smart Card Specification; http://www.openmobilealliance.org/tech/affiliates/wap/wap-186-provsc-20010710-a.pdf

[11] ISO/IEC 7816-4 APDU Specification; http://www.ttfn.net/techno/smartcards/iso7816_4.html

[12] UMTS Security Features; http://www.umtsworld.com/technology/security.htm

[13] UICC-Terminal Interface; http://www.etsi.eu/deliver/etsi_ts/102200_102299/102221/08.02.00_60/ts_102221v080200p.pdf

[14] Mobile Virtual Network Operator; http://en.wikipedia.org/wiki/Mobile_virtual_network_operator

5 Enterprise Mobility Infrastructure

5.1 Overview

The basic tenets of enterprise mobility solutions are to provide services to users while protecting data, enterprise resources, users, and their mobile devices. To meet these basic tenets, the role of the enterprise mobility infrastructure is to:

a. **Host and support user applications, in this case VoIP call management using a SIP server**. This is a new service and must be Government controlled and protected since it is on the enterprise side of the VPN used by the mobile device to connect to the infrastructure.

b. **Secure the traffic path**. Each Voice over Internet Protocol (VoIP) session (or phone call) initiated from the mobile device is transported over a commercial carrier infrastructure, through an encrypted IPsec VPN (Virtual Private Network) tunnel. The VPN is the first of two layers of commercial encryption required to protect classified information. Although traditional encryption devices are said to have a "black" (ciphertext) and "red" (plaintext) side, the requirement for two encryption layers introduces a new term. As used in this document, "grey" refers to data protected by a single (inner) layer of encryption while "black" refers to ciphertext protected by both inner and outer layers. The VPN in conjunction with the protected operations environment for grey traffic protects user and management traffic passed across the carrier. The encrypted IPsec VPN session in combination with a Secure Voice over Internet Protocol (SVoIP) application, which establishes the secondary data encrypted tunnel, provides a secure connection between devices, even when using a public commercial infrastructure for the IP packet data transport.

c. **Control which devices get access and what they can do (authentication and authorization).** The device is a commercial mobile device that can introduce vulnerabilities into government networks. Only authorized Government users are allowed into the enterprise. Connecting the enterprise to a carrier and allowing the use of commercial devices potentially exposes the enterprise to huge numbers of threats. Carrier controls on access and routing information plus these infrastructure controls can limit that exposure.

d. **Manage devices to maintain security (Mobile Device Management).** Maintain the secure state of devices. This includes keeping configurations, software, and signature files up to date. If secure state is lost (or suspected lost), a device may be remotely erased to remove any sensitive information and render the device useless.

e. **Perform cyber defense.** Monitor and report on operations and prevent what intrusions we can (IPS) (audit collection/analysis/reporting, other monitoring, reporting to cyber defense/CND) – track activities and status: what devices and other components are doing, what events/intrusions are detected, status of devices, call records

f. **Provide overall security management and supporting services**. Maintain certificate validity and ties to identities. Manage trust anchors to keep user community secure. Revoke certificates for lost devices/end of use.

g. **Support and perform Government side of provisioning for devices and for infrastructure**. Provide certificates and trust anchors, register devices, Government approved software, provide patches, and maintain software baselines.

The enterprise mobility infrastructure will be a new capability, as interconnection with, or shared use of, other systems are not yet allowed. It will need to be housed in a protected facility (SCIF may be appropriate for TS level use; S level may not need a SCIF). As a new system, there are certain functions that are inherent such as internal networking functions (e.g., Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Network Time Protocol (NTP) server, switches).

A device's traffic (IP data) is routed by the carrier to the infrastructure where it establishes a secure connection via VPN. Services and enterprise management functions are provided by the infrastructure to the device over this VPN. This is similar to remote access via VPN from a laptop to the enterprise used during telework or travel. The infrastructure user services required are simply those needed to establish and manage phone calls between authorized cellular devices. The infrastructure is, however, also responsible for managing the device and monitoring usage. Since most of the security functions are built on authenticated identification and on keying, the infrastructure includes security management services to issue and manage device certificates.

5.2 Description

The infrastructure is the collection of mobility-oriented network, security, applications, and related capabilities for the government's enterprise. The infrastructure serves as the access point for all mobile devices into the government infrastructure. The infrastructure encompasses the application services and data provided to mobile device users and the infrastructure to secure, provision, and manage this usage. This includes:

- Mobility-oriented networking and security capabilities to provide access control, secure session routing, data-in-transit protection, and boundary protection (for the networks and infrastructure).
- Mobility-oriented application and security capabilities to provide access control server-side mobility applications and boundary protection (protect the enterprise).
- Management and Provisioning components to provide capabilities for initializing mobile devices then supporting and monitoring their operation including provisioning systems, monitoring usage, and providing situational awareness. Security management functional capabilities are provided for loading and configuring devices, managing privileges and policies, managing keys and certificates, and maintaining accountability.

The use of cellular mobile devices, commercial carriers, layered commercial products, and VoIP entails a number of threats to address. These threats include actions taken by an adversary or by an authorized user, under both malicious and accidental motivations. Some principal areas to address are:

- The potential for unauthorized users and devices to attempt access Government resources via widely available commercial cellular carriers.
- Loss or theft of authorized devices which are then used to attempt access to Government resources and masquerade as authorized users. A subset of this would be a stolen device that had been tampered with to alter the configuration and circumvent controls.
- Authorized users attempting to misuse their privileges, such as by trying to use disallowed services or connect directly to commercial services.
- Insiders, with access to commercial carrier facilities or Government facilities, attempting unauthorized access to services or data possibly by misconfiguring security components.

The goals or consequences of these attempts include the following:

- To circumvent controls intended to apply the appropriate access/authorization privileges to services, data, or resources.
- To circumvent cryptographic controls intended to provide confidentiality of information (e.g., man-in-the-middle).
- To circumvent controls intended to verify the identification attributes of a mobile user, device, or entity (e.g., impersonation).
- To circumvent controls limiting the improper or excessive use or treatment of a mobile device by an authorized user including theft of services) (attempts to establish SVoIP call above authorized classification level, ties up an excessive amount of resources, or causes user errors).
- To circumvent controls by any manner in which information or data is in a state of accessibility of an adversary such as by bypassing encryption (e.g., eavesdropping).
- To circumvent controls associated with the application (e.g., call high-jacking).

5.2.1 Rationale for Security Design

There are millions of users and devices connected to each major cellular carrier's networks and each network allows roaming and interconnection with other carriers so there is a very large attack surface of unauthorized users that could potentially attempt to access the Government resources. Due to the magnitude of this threat vector, multiple layers of defense are employed. In the carrier section, the first lines of defense are described (only authenticated authorized devices and only data traffic are routed to the Government, the IP address is not publicized, the APN controls what is passed).

The Enterprise Mobility Infrastructure provides additional layers of defense that complement what the carrier provides and also protect against stolen phones, insider threats and systems failures within the carrier. Firewalls are used to limit the traffic types to just those needed for the allowed services (e.g., IPSec, SIP, and SRTP). Intrusion detection/prevention systems are employed to check for malware and anomalies in the traffic. These boundary defenses are layered to monitor and control both Black traffic and Grey traffic

The VPN authenticates the Government provisioned identification of the device (PKI credentials) and checks that the device is authorized. This prevents any unauthorized device from accessing the internal Government networks and services. A stolen device with a valid credential could only be used if the thief were able to find the right password in a small number of tries or tampered with the phone (both of which are addressed for the user equipment). Once a device is reported stolen, it is removed from internal authorization systems and would not be allowed to connect to either the VPN or the SIP server.

The SIP server (covered in the applications section), authenticates the Government provisioned identification of the device user (PKI credentials) and checks that the user is authorized. The credentials and associated public key material used for the device authentication in VPN establishment are cryptographically independent of the credentials and key material used for user authentication and secure call establishment. Two different sets of passwords on the device protect these so it would be necessary and difficult to break both in order for a thief to masquerade as an authorized user.

The Government provisioning process is controlled in multiple ways to ensure that authorized devices and users are registered and provided correct credentials and that these credentials can't be stolen or otherwise compromised. When devices are reported stolen, the registration and authorization records within the infrastructure are updated and access is no longer possible from that device.

5.2.2 Security Approach in the Enterprise Mobility Infrastructure

5.2.2.1 Authentication

The strong authentication of a mobile device and its user provides the basis for determining whether a device or a user has authorized access to networks, enterprise services, and data. Authenticated identities also provide the basis for associating actions with users to provide accountability. PKI certificates are used for both device/VPN and user/VoIP authentication.

5.2.2.2 Authorization

Authorization provides decisions about allowing access to resources based on policy rules. Attributes associated with the authenticated identity of the user and the user's platform can be used to make authorization decisions in accordance with digital policies that reflect mission needs. Only authorized users and devices are allowed to access the infrastructure and obtain services.

5.2.2.3 Data in Transit Protection (DIT)

DIT protection maintains the confidentiality and integrity of data as it is exchanged between systems over communications means. DIT protection is particularly important when the communications networks used are outside of Government control, subject to eavesdropping by wide communities, or subject to radio intercept. Two layers of commercial DIT are used to provide protection of classified information. One layer is an IPsec VPN that connects the device to the Grey network. The second layer of DIT is at the application/transport protocol level and has two forms: TLS protection of the call establishment traffic between the device and SIP services and SRTP protection of the user voice traffic from one device to another.

5.2.2.4 Boundary Protection and Cyber Defense (networking and enterprise services)

Boundary protection is placed at key points in the architecture to filter, monitor, and control traffic entering/exiting a domain or enclave. The first layer of boundary protection is where the traffic routed from the carrier is attempting to access the infrastructure's Black network. It is very important to have strong firewalls and IDS/IPS here since there are many users and threats represented by the carrier user population. A second layer of boundary protection after the VPN provides additional assurance and a means to monitor the grey network traffic.

5.2.2.5 Accountability/Audit

Authenticated identities of users and devices are used to correlate audit events, which can be used to provide situational awareness of mobile devices, users, and their associated activities. In addition accountability provides the tracking of data dissemination and handling and supports overall information sharing situational awareness.

5.2.2.6 Personnel and Physical Security

The primary focus of this document is on those security mechanisms designed into the networks and services but it is also important to include aspects of personnel and physical security that contribute to the overall security of operations. For instance, the Grey network needs to be housed in a physically

secure facility appropriate for the classification of the traffic handled. Also, the personnel that provision devices and manage the infrastructure need to be cleared and trusted commensurate with their access and responsibilities.

5.3 Approach

5.3.1 Architecture

Figure 5-1 shows the correspondence of the segments described in the overview to the component types and architectural components defined in the reference architecture. The Enterprise Mobility Infrastructure encompasses all of the component types of Mobility Networking Services and Mobility Enterprise Services and the Government components of Management and Provisioning.

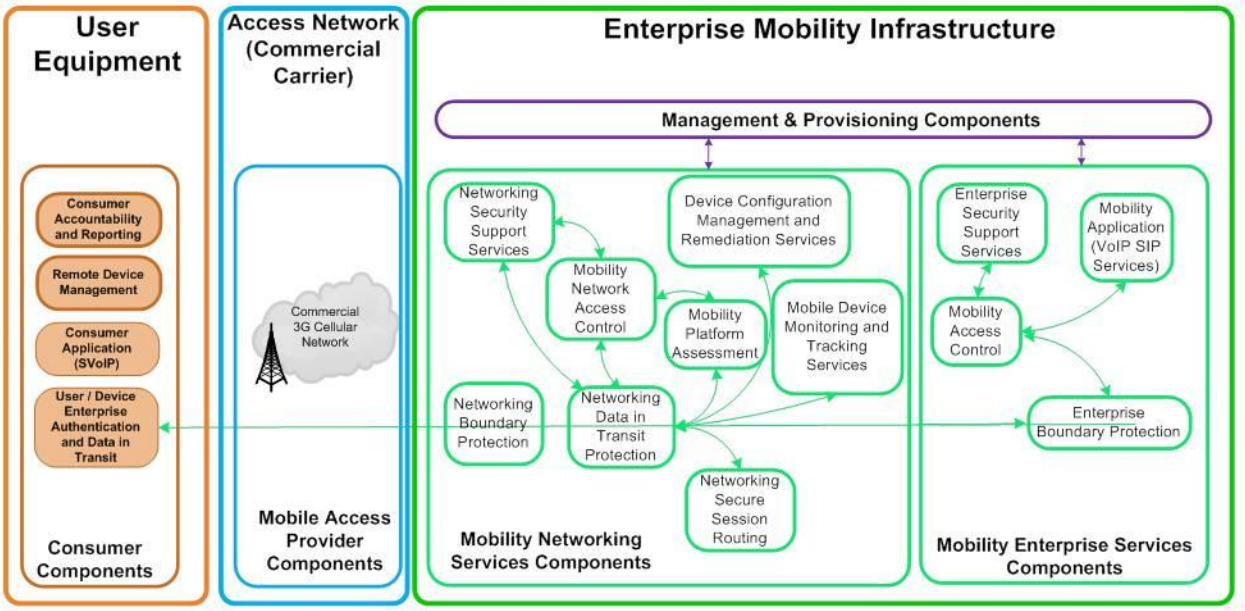

Figure 5-1 Mobile Voice over IP (VoIP) Architecture

Table 5-1 provides a mapping of the Enterprise Mobility Infrastructure architectural components identified in Figure 5-1 to the components identified and described in section 5.3.2.

Table 5-1 Architectural Components to System Components Mapping

Architectural Component	System Component
Networking Boundary Protection	• Carrier Border Router • Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) • Firewall (multiple)
Networking Data in Transit Protection	• Virtual Private Network (VPN) Gateway
Mobility Network Access Control	• Virtual Private Network (VPN) Gateway
Mobility Platform Assessment	• Device Security Assessment

Architectural Component	System Component
Device Configuration Management and Remediation Services	• Device Configuration and Policy Management • Remediation • Secure Disable and Wipe • Collection of audit log records received from the mobile device
Mobile Device Monitoring and Tracking Services	• Location Tracking
Networking Secure Session Routing	• Network Support Services
Networking Security Support Services	• AAA Services • Audit Services
Enterprise Boundary Protection	• Grey Network Border Router • Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) • Firewall
Mobility Access Control	• SIP Services
Mobility Application	• SIP Services
Enterprise Security Support Services	• AAA Services • Certification Revocation List (CRL) and Certificate Verification Services • Audit Services
Management and Provisioning	• Certificate Authorities • Enrollment workstations • Government Provisioning Workstation

General Infrastructure Support (not identified as an architectural component)	• Infrastructure Management Services:
	  • Host Security Manager
	  • Enterprise Security Manager
	  • Network Manager
	  • CM/Patch Manager
	• Network Support Services:
	  • Routers and Switches
	  • DNS Services
	  • Network Time Services
	  • DHCP Services
	• Directory Services

5.3.2 Security Relevant Components

Figure 5-2 shows a more detailed view of the components that provide the functionality previously described. A typical implementation will have networked components in two different security domains (i.e., Black networking that is connected to the carrier and Grey networking that is protected by a VPN established with the device), as well as standalone components and components that may be connected to the Internet but isolated from the other networks. There will generally be no connections to other operational networks and systems for these first implementations. There will be cyber defense Computer Network Defense (CND) information collected by these networks that can be reported to existing monitoring systems, but direct connectivity is not yet defined.

The network infrastructure and server components should be designed to provide the performance, scalability, availability, and reliability appropriate for each solution implementation. This will be driven by mission requirements, number of users, and environment. The network infrastructure and server components should be designed to provide the required degree of availability through the use of redundant technologies with hot failover capabilities. Requirements specific to performance, scalability, availability, and reliability are not included within the component requirements below but should be addressed as part of a given solution implementation.

The Carrier Management Data line in Figure 5-2 identifies the ability for the cellular carrier to electronically exchange information with the Government. This could include billing information, successful and unsuccessful device activations, device deactivations (e.g., if the device is reported lost), device authentication failures, identification of roaming devices, and geographical location of tracked devices. The ability to exchange information electronically and the types of information that may be exchanged are carrier-dependent. The carrier may connect to a separate network (e.g., the NIPRNet) or connect directly into Enterprise Mobility Services through a VPN association (via the VPN Gateway) to the grey network, the Carrier Border Router to the black network, or through a separate Carrier Management Border Router to the black or grey network. This is dependent on available technologies and the trust relationship between the Government and the carrier.

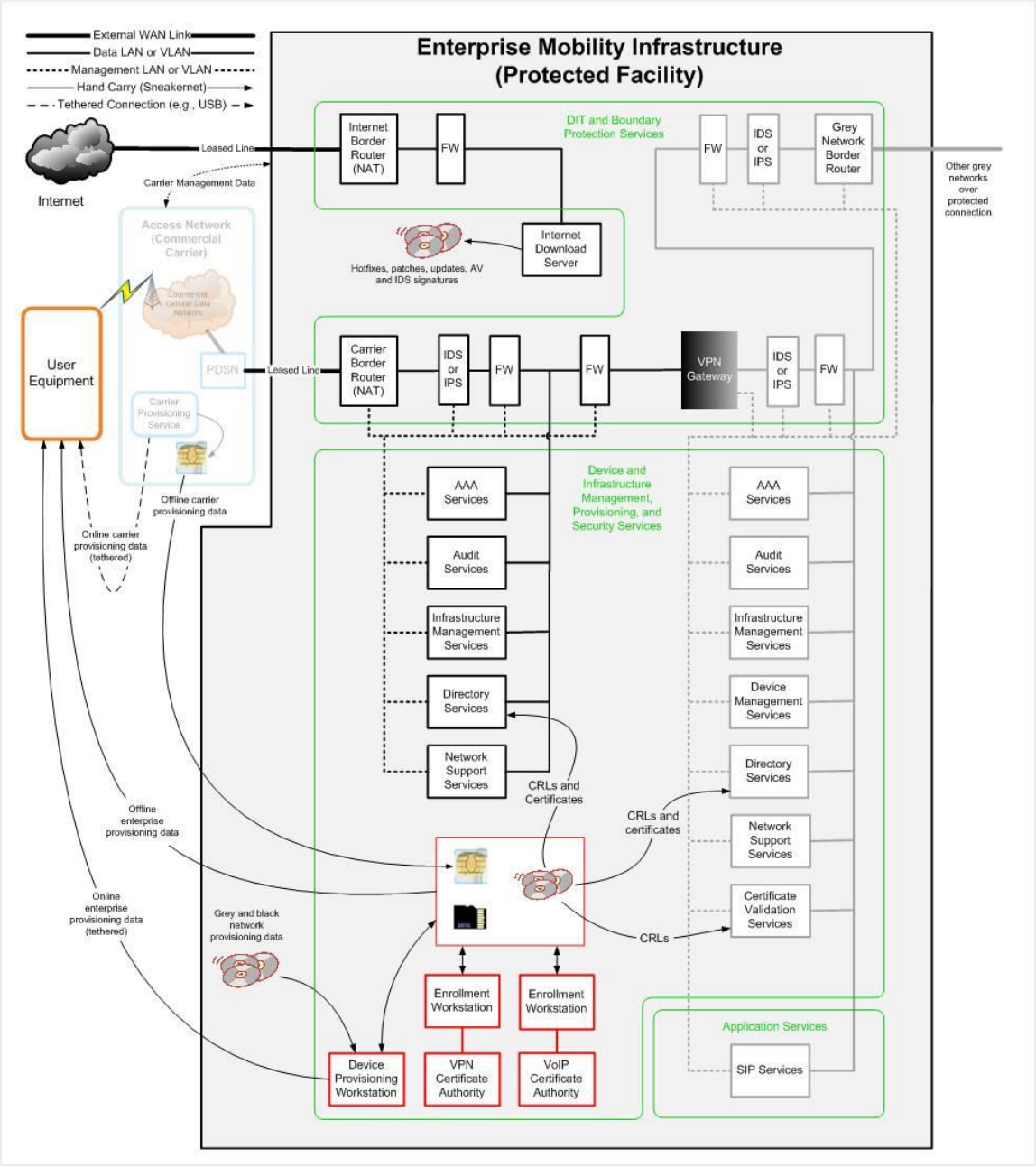

Figure 5-2 Enterprise Mobility Infrastructure Components

5.3.2.1 Data-in-Transit (DIT) and Boundary Protection Services

This section covers the following architectural components identified in Figure 5-1: Networking Boundary Protection, Networking Data in Transit Protection, and Enterprise Boundary Protection.

Data-in-Transit encryption, authentication, and boundary protection services are closely related as encrypted channels must be authenticated and protection keys negotiated at domain boundaries.

The first "outer" layer of encryption consists of a mutually authenticated IPsec tunnel-mode association. The User Equipment (UE) establishes an IPsec association with the VPN Gateway using the Internet Key Exchange version 2 (IKEv2) protocol. Mutual public key authentication is performed using keys and certificates issued by the VPN Certificate Authority (VPN CA). The VPN Gateway queries the Directory Service for a CRL or queries the Certificate Validation Responder using the Online Certification Status Protocol (OCSP) to verify that the UE certificate is valid. Once the VPN Gateway has verified the identity of the mobile device, it must check the identity against a black- or white-list to determine whether the UE is authorized to access the grey network. The list may be stored locally on the VPN Gateway or centrally within the Directory Service or shared database. The VPN Client and Gateway negotiate encryption keys for subsequent confidentiality and integrity protection of the IPsec association.

The following components provide boundary protection capabilities:

5.3.2.1.1 Border Router

A border router that provides Network Address Translation (NAT) services provides additional isolation between a public network and the black network. The Carrier Border Router is required to perform NAT unless the cellular carrier is able to statically or dynamically assign IP black addresses to Government UEs from a private Government address space. Such an address space must be isolated from any other IP address spaces used by the carrier. Border Router requirements are listed in Table 5-2. The Carrier Border Router, VPN client on the UE, and the VPN Gateway must support IPsec and IKE NAT traversal. In this document the term NAT encompasses Port Address Translation (PAT).

UE grey IP addresses are either pre-configured or dynamically assigned by the VPN Gateway. As these IP addresses are private, NAT is not required for a UE to access the grey network. NAT may be required on the Grey Network Border Router depending on the nature of the connection to the remote Government network; however, NAT traversal within the grey network complicates SIP and SVoIP interoperability and is therefore not recommended. See Section 7: Secure Mobility Interoperability for more information on intra-Government connectivity.

Table 5-2 Border Router Requirements

Req #	Requirement Description	Threshold / Objective
BR.1	The Border Router shall be able to operate on IPv4 networks.	T=O
BR.2	The Border Router shall be able to operate on IPv6 networks.	T=O
BR.3	The Internet and Carrier Border Routers shall be configurable to provide Network Address Translation (NAT) and Port Address Translation (PAT) services.	T=O
BR.4	The Carrier Border Router shall be configurable to allow IPsec and IKE NAT traversal.	T=O

Req #	Requirement Description	Threshold / Objective
BR.5	The Border Router shall be configured in accordance with DISA Network Perimeter Router L3 Switch STIG v8r9 and NSA Enterprise Mobility Infrastructure (EMI) Configuration Guidance.	T=O

5.3.2.1.2 Network Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)

An IDS checks for network attack signatures and alerts the security administrator if a possible network attack is detected. In additional, an IPS is able to automatically respond and block suspect traffic or even disconnect the entire network if necessary. An IDS may passively monitor network traffic (e.g., from a promiscuous port on a network switch), but an IPS must be in-line with the network connection unless it is able to cooperate with its associated firewall to perform the blocking. IDS/IPS capabilities are often combined in a single unit with a firewall, but separate units eliminate single points of failure. With the exception of the firewall between the black and grey networks, and the Internet Access firewall, each firewall has an associated IDS or IPS. The Internet Access firewall may have an associated IDS/IPS, but is not necessary as the Internet Patch Server is non-critical, isolated from operational networks, and can be easily replaced if attacked. IDS/IPS requirements are listed in Table 5-3.

Table 5-3 IDS/IPS Requirements

Req #	Requirement Description	Threshold / Objective
IDS.1	The Network IDS/IPS shall be able to operate on IPv4 networks.	T=O
IDS.2	The Network IDS/IPS shall be able to operate on IPv6 networks.	T=O
IDS.3	The Network IDS/IPS shall provide intrusion detection capabilities.	T
IDS.4	The Network IDS/IPS shall provide intrusion detection and prevention capabilities.	O
IDS.6	The Network IDS/IPS shall be configured in accordance with DISA Network IDS/IPS STIG v8r9 and NSA EMI Configuration Guidance.	T=O

5.3.2.1.3 Network Firewall

A firewall validates and blocks unauthorized traffic at the boundary of each major network segment in accordance with a configured policy. As all application layer traffic is encrypted, a deep inspection firewall provides minimal additional value. The baseline architecture identifies five firewalls:

1. The firewall behind the Internet Border Router is placed to prevent attacks from the Internet by restricting allowable ports, protocols, and IP addresses to those necessary to download hot fixes, patches, and other updates for infrastructure components. The firewall is monitored and managed from the black management LAN or VLAN.
2. The firewall behind the Carrier Border Router is placed to prevent attacks from the Commercial Carrier Access Network. Only IPsec and IKEv2 traffic from registered UE black IP addresses is allowed passage. Unless the UE is preconfigured with fixed

remote IP addresses, it may also be necessary to allow passage of DNS traffic for translation between names and IP addresses.

3. The firewall between the firewall listed immediately above and the VPN Gateway prevents unauthorized traffic from the black data network from reaching the VPN Gateway. Only IPsec and IKEv2 traffic to and from registered UE black IP addresses is allowed passage.
4. The firewall between the VPN Gateway and the grey infrastructure data network monitors traffic decrypted by the VPN Gateway and traffic routed to the VPN Gateway for encryption. SIP-over-TLS traffic must be allowed passage, and also OCSP and/or LDAP traffic if the VPN Gateway performs certificate revocation checking. DNS traffic may be required unless the UE is configured to use fixed grey IP addresses. SVoIP traffic is looped back by the VPN Gateway and does not transit this firewall unless connectivity to another VoIP grey network ("mobility domain") is required (see next bullet).
5. If connectivity to a remote grey network in another Government facility is required, the connection may be protected by a firewall depending on the level of trust in the remote network and the connecting link. The firewall, if deployed, allows passage of SIP-over-TLS and SVoIP traffic. Connectivity to other Government networks will be discussed in Section 7 (Secure Interoperability) of this document.

Network Firewall requirements are listed in Table 5-4.

Table 5-4 Network Firewall Requirements

Req #	Requirement Description	Threshold / Objective
F.1	The Network Firewall shall be able to operate on IPv4 networks.	T=O
F.2	The Network Firewall shall be able to operate on IPv6 networks.	T=O
F.4	The Network Firewall shall be validated by NIAP as complying with the Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall.	O
F.5	The Network Firewall shall be configured in accordance with DISA Network Firewall STIG v8r9 and NSA EMI Configuration Guidance.	T=O

5.3.2.1.4 Virtual Private Network (VPN) Gateway

The VPN Gateway serves as the main entry point into the grey network and authenticates requested VPN associations using the Internet Key Exchange protocol. A VPN client that cannot be identified or authenticated is denied access to the grey network. As public key authentication only confirms the identity of the User Equipment (UE), the VPN Gateway must maintain a black- or white-list on which to base authorization decisions. As the Carrier Border Router may implement Network Address Translation (NAT) of black IP addresses, the VPN Gateway must support NAT traversal. VPN Gateway requirements are listed in Table 5-5.

If the cellular carrier is connecting to the Government via a public network such as the Internet (rather than a private leased line), a second VPN gateway may be required to securely establish

a protected tunnel through the public network. The requirements for such a VPN gateway are not specifically addressed in Table 5-5 although most are relevant.

Table 5-5 VPN Gateway Requirements

Req #	Requirement Description	Threshold / Objective
VPN.1	The VPN Gateway shall be validated as complying with FIPS 140-2 Level 2 or better under the Cryptographic Module Validation Program (CMVP).	T
VPN.2	The VPN Gateway shall be validated as complying with FIPS 140-2 Level 3 or better under the Cryptographic Module Validation Program (CMVP).	O
VPN.3	The VPN Gateway shall be validated as complying with NIST-approved cryptographic algorithms and modes of operation under the Cryptographic Algorithm Validation Program (CAVP).	T=O
VPN.4	The VPN Gateway shall be operated in FIPS-compliant mode using NIST-validated algorithms.	T=O
VPN.6	The VPN Gateway shall be validated by NIAP as complying with the IPsec VPN Gateway Protection Profile.	O
VPN.7	The VPN Gateway shall support IPsec in tunneling mode.	T=O
VPN.8	The VPN Gateway shall be configurable to prohibit split-tunneling.	T=O
VPN.9	The VPN Gateway shall be able to operate on IPv4 networks.	T=O
VPN.10	The VPN Gateway shall be able to operate on IPv6 networks.	T=O
VPN.11	The VPN Gateway shall use IKEv1 for authentication and key agreement.	T
VPN.12	The VPN Gateway shall use IKEv2 for authentication and key agreement.	O
VPN.13	The VPN Gateway shall perform mutual authentication with VPN clients using public key cryptography.	T=O
VPN.14	The VPN Gateway shall perform certificate path validation.	T=O
VPN.15	The VPN Gateway shall check for revoked certificates.	T=O
VPN.16	The VPN Gateway shall be configurable to use 2048-bit RSA keys for authentication.	T
VPN.17	The VPN Gateway shall be configurable to use Suite B ECC keys with a 256-bit or 384-bit prime modulus for authentication.	O
VPN.18	The VPN Gateway shall use 128-bit or 256-bit AES keys to protect the confidentially and integrity of data (tunneled IP packets) exchanged over IPsec security associations.	T=O
VPN.19	The VPN Gateway shall be interoperable with commercially available products using IETF-approved protocols for the issuance of X.509v3 public key certificates.	T
VPN.20	The VPN Gateway shall be interoperable with commercially available products using IETF-approved protocols for the installation of X.509v3 root key certificates (trust anchors).	T

Req #	Requirement Description	Threshold / Objective
VPN.21	The VPN Gateway shall be interoperable with commercially available products using IETF-approved protocols for checking certificate validity.	T
VPN.22	The VPN Gateway shall be interoperable with applicable existing Public Key Infrastructures (PKIs) for the issuance of public key certificates.	O
VPN.23	The VPN Gateway shall be interoperable with applicable existing Public Key Infrastructures (PKIs) for the installation of root key certificates (trust anchors)	O
VPN.24	The VPN Gateway shall be interoperable with the applicable existing Public Key Infrastructures (PKIs) for checking certificate validity.	O
VPN.25	The VPN Gateway shall consult a white-list to authorize access to the protected network based on the authenticated UE identity.	T
VPN.26	The VPN Gateway shall consult a white- or black-list to authorize access to the protected network based on the authenticated UE identity.	O
VPN.27	The VPN Gateway shall be configurable to consult an external white- or black-list to authorize access to the protected network based on the authenticated UE identity.	O
VPN.28	The VPN Gateway shall be able to audit and report all attempts to establish a security association.	T=O
VPN.29	The VPN Gateway shall audit and report all unsuccessful attempts to establish a security association.	T=O
VPN.30	The VPN Gateway shall selectively audit and report successful attempts to establish a security association based on configurable criteria.	T=O
VPN.31	The VPN Gateway shall audit and report all integrity check failures.	T=O
VPN.32	The VPN Gateway shall support NAT traversal.	T=O
VPN.33	The VPN Gateway shall be configurable to assign a grey IP address to a VPN client upon successful establishment of a security association.	T=O
VPN.34	The VPN Gateway shall terminate security associations that have been inactive for a configurable period of time.	T=O
VPN.35	The VPN Gateway shall be configured in accordance with DISA Remote Access VPN STIG v8r9 and NSA EMI Configuration Guidance.	T=O

5.3.2.2 Device and Infrastructure Management, Provisioning, and Security Services

The Device and Infrastructure Management, Provisioning, and Security Service shown in Figure 5-2 have been decomposed into the following sub-services. In all cases, a given sub-service may be implemented using a single or multiple servers depending on the design and technologies

selected. Servers may also be implemented as Virtual Machines (VMs) to reduce hardware, space, power, and cooling costs.

5.3.2.2.1 Security Services

This section covers the following architectural components identified in Figure 5-1: Networking Security Support Services and Enterprise Security Support Services.

5.3.2.2.1.1 Authentication and Authorization Services

AAA services provide authentication (verification of a user's identity), authorization (determination of whether the authenticated user is authorized to access a network or other resource), and accountability (a record of authentication and authorization decisions made). The authentication and authorization decisions may be made by the same component, or they may be made by different components depending on the mechanisms, protocols, and products selected. In the case of public key authentication, the relying party (authenticator) must make a separate authorization decision. This may be based on a black- or white-list stored locally or retrieved from a centralized directory service or database.

The UE-to-VPN Gateway IPsec association is established using mutual public key authentication. The VPN Gateway uses a black- or white-list containing User Equipment names to determine authorization to access the protected network based on the authenticated identity of the UE.

The User Equipment and the SIP Service perform mutual authentication using certificates in TLS. Within SIP, the User Equipment also uses a userid and password to authenticate itself to the SIP Service. If a userid and password is used, the SIP Server may delegate the authentication and authorization decision to a separate AAA Service (e.g., using the RADIUS protocol). Security parameters for SRTP are negotiated through the exchange of SDP Security Descriptions (SDES).

The following components make authentication and authorization decisions:

- **AAA Service**. The Authentication, Authorization, and Accountability (AAA) service is used to provide AAA services where public key cryptography is not used. This includes local login to Enterprise Mobility Infrastructure components. There may be more than one type of AAA service depending on the design of the system; for example, a RADIUS server, a Windows Domain Controller, and a Kerberos Authentication/Ticket Granting Server (for Linux realms).

Table 5-6 Authentication, Authorization, and Accountability Requirements

Req #	Requirement Description	Threshold / Objective
AAA.1	The AAA Service shall authenticate users based on userid and password.	T=O
AAA.2	The AAA Service shall authorize access by an authenticated user based on a black- or white-list.	T=O
AAA.3	The AAA Service shall audit all authentication and authorization failures.	T=O
AAA.4	The AAA Service shall be configurable to audit selected authentication and authorization successes.	T=O

Req #	Requirement Description	Threshold / Objective
AAA.5	The AAA Service shall support Windows Domain authentication if the infrastructure includes components running Microsoft Windows.	T=O
AAA.6	The AAA Service shall support Kerberos authentication if the infrastructure includes components running Linux.	T=O
AAA.7	The AAA Service shall support RADIUS authentication if required by the system design (e.g., to support the SIP Service).	T=O
AAA.9	The AAA Service shall be evaluated by NIAP as complying with the Authentication Server Protection Profile.	O
AAA.10	The AAA Service shall be configured in accordance with DISA Remote Access Policy STIG v8r9 and NSA EMI Configuration Guidance.	T=O

- **Certification Revocation List (CRL) and Certificate Verification Service**. This service provides infrastructure components with the ability to check for revoked public key certificates. A CRL may be posted to a directory service, or it may be used by a Certificate Validation Service that acts on behalf of the relying party (normally using the Online Certificate Status Protocol). Figure 5-2 shows both a Certificate Validation Service and a Directory Service in the grey network for use by the VPN Gateway and SIP Service (if it supports public key authentication of SIP clients). A Directory Service is shown on the black network for use by black network components including the VPN client on the UE. A Certification Validation Service might also be provided on the black network.

Table 5-7 Certificate Validation Requirements

Req #	Requirement Description	Threshold / Objective
CVR.1	The Security Services shall enable posting of full CRLs to the Directory Service.	T
CVR.2	The Security Services shall enable posting of delta CRLs to the Directory Service.	O
CVR.3	The Security Services shall include a Certificate Validation Service. (The requirements for the Certificate Validation Service, when deployed, are listed in Table 5-8.)	O

Table 5-8 Certificate Validation Service Requirements

Req #	Requirement Description	Threshold / Objective
CVS.1	The Certificate Validation Service shall validate X.509v3 certificates.	T=O

Req #	Requirement Description	Threshold / Objective
CVS.2	The Certificate Validation Service shall support the Online Certificate Status Protocol (OCSP).	T=O
CVS.3	The Certificate Validation Service shall be configured in accordance with NSA EMI Configuration Guidance.	T=O

5.3.2.2.1.2 Audit Service

An auditing and logging service is required to monitor and report events generated by infrastructure components (see Infrastructure Management Service) and the mobile device itself is responsible for auditing and logging events. The Device Management Service is responsible for monitoring and reporting events received from the mobile device. An audit collection and analysis capability gathers information from the Infrastructure Management Service and Device Management Service to create an integrated audit repository. This audit information can then be correlated with other information such as device location and call activity to create a view of the operational and security status of mobile operations. Initially, the degree of integration and correlation will be limited and manual but the objective is to automate this and provide situational awareness. Audit requirements are listed in Table 5-9.

Table 5-9 Audit Requirements

Req #	Requirement Description	Threshold / Objective
AR.1	The Audit Service shall record audit events reported by infrastructure components.	T=O
AR.2	The Audit Service shall provide integrity protection of audit records in transit from infrastructure components.	T=O
AR.3	The Audit Service shall provide integrity protection of audit records at rest.	T=O
AR.4	The Audit Service shall allow configuration of an audit policy that encompasses deletion and/or overwriting of audit records.	T=O
AR.5	The Audit Service shall provide the ability to backup audit records to tape of other long-term storage media.	T=O
AR.6	The Audit Service shall require authentication and authorization for users to view, modify, delete, or backup audit records.	T=O
AR.7	The Audit Service shall be configured in accordance with NSA EMI Configuration Guidance.	T=O

5.3.2.2.2 Infrastructure Management Services

These are additional capabilities not identified in the Enterprise Mobility Architecture. They do not directly relate to management of the UE, but instead manage infrastructure components that interact with the UE.

The Infrastructure Management Service consists of the components required to manage the infrastructure components. Management of UEs is covered by the Device Management Service.

This service has been decomposed into the several discrete managers identified below; however, these may be combined depending on available technologies and products.

Host Security Manager:

- The Host Security Manager is responsible for managing security capabilities on Enterprise Mobility Infrastructure components including anti-virus, host-based IDS/IPS, host-based firewall, and spam filter capabilities.
- The Host Security Manager automatically pushes out updates (e.g., virus signatures) at regular intervals, or immediately if an update is critical.

Enterprise Security Manager:

- The Enterprise Security Manager manages network IDS/IPS and network firewall policies.

Network Manager:

- The Network Manager is responsible for monitoring and management of networking components including routers, switches, and the VPN Gateway.

CM/Patch Manager:

- The CM/Patch Manager monitors Enterprise Mobility Infrastructure components for compliance with configuration management policy. It is responsible for pushing out hot fixes, patches, and updates as needed. Files to be pushed out may be obtained from the Internet indirectly via the Internet Download Server (on CD or DVD) or received directly on CD or DVD from hardware and software vendors.
- All files must be evaluated for authenticity and integrity (including malicious code scanning), and tested before being provided to the CM/Patch Manager for distribution to infrastructure components.

Host System Security Services:

- Systems that host management services must provide authentication, authorization, and audit. They also require host-based security services (e.g., anti-malware).

Infrastructure Management requirements are listed in Table 5-10.

Table 5-10 Infrastructure Management Requirements

Req #	Requirement Description	Threshold / Objective
IM.1	The Infrastructure Management Services shall provide virus signature updates to infrastructure components running anti-virus software.	T=O
IM.2	The Infrastructure Management Services shall provide intrusion detection signature updates to infrastructure components running host-based IDS/IPS software.	T=O
IM.3	The Infrastructure Management Services shall provide the ability to create and distribute firewall policies to infrastructure components running host-based firewall software.	T=O

Req #	Requirement Description	Threshold / Objective
IM.4	The Infrastructure Management Services shall provide intrusion detection signature updates to network-based IDS/IPS components.	T=O
IM.5	The Infrastructure Management Services shall provide the ability to create and distribute firewall policies to network-based firewall components.	T=O
IM.6	The Infrastructure Management Services shall be able to automatically update virus and IDS/IPS signatures at a configurable frequency.	T=O
IM.7	The Infrastructure Management Services provide the ability to receive, authenticate, and validate virus and IDS/IPS signatures received indirectly via the Internet (e.g., via the Internet Download Server) or directly from applicable vendors.	T=O
IM.8	The Infrastructure Management Services shall provide the ability to securely configure, manage, and monitor all networking components (e.g., switches, routers, firewalls).	T=O
IM.9	The Infrastructure Management Services shall provide the ability to remotely install software updates on infrastructure components.	T=O
IM.10	The Infrastructure Management Services shall provide the ability to receive, authenticate, and validate software updates received indirectly via the Internet (e.g., via the Internet Download Server) or directly from applicable vendors.	T=O
IM.11	The Infrastructure Management Services shall track the Configuration Management status of infrastructure components.	T=O
IM.12	The Infrastructure Management Services shall be configured in accordance with NSA EMI Configuration Guidance.	T=O

Table 5-11 lists requirements for host systems (desktop, server, and laptop computers) managed by Infrastructure Management Services. These host systems may themselves be providing infrastructure management services. A subset of these requirements may be satisfied by using the Host-Based Security System (HBSS) available from DISA.

Table 5-11 Host System Security Requirements

Req #	Requirement Description	Threshold / Objective
HSS.1	The host system be configured in accordance with DISA DoD Host Based Security System (HBSS) STIG v3r5 and NSA EMI Configuration Guidance.	T=O
HSS.2	The host system shall be able to authenticate users.	T=O
HSS.3	The host system shall prohibit unauthorized users from accessing resources.	T=O
HSS.4	The host system shall maintain separation of user roles.	T=O

Req #	Requirement Description	Threshold / Objective
HSS.5	The host system shall audit actions taken by users (types of actions and content of audit record are configurable).	T=O
HSS.6	The host system shall perform anti-malware detection.	T=O
HSS.7	The host system shall include a host-based firewall.	T=O
HSS.8	The host system shall include a host-based IDS/IPS capability.	T=O
HSS.9	The host system shall verify the integrity of its software environment.	T
HSS.10	The host system shall implement hardware roots of trust for performing integrity verification and reporting (attestation).	O
HSS.11	The host system shall be capable of reporting platform status.	T=O

5.3.2.2.3 Device Management Services

This section covers the following architectural components identified in Figure 5-1: Mobility Platform Assessment, Device Configuration Management and Remediation Services, and Mobile Device Monitoring and Tracking Services.

The Device Management Services perform Mobile Device Management (MDM) and is responsible for managing the configuration and security of UEs, tracking and monitoring them, providing remote wipe capability, and collecting audit records from the device. Overall, MDM is a broad ranging term that encompasses many different sets of functions. These can be grouped in to Software Distribution, Policy Management, Inventory Management, and Security Management categories (other groupings have also been used in industry surveys). Provisioning is sometimes included as part of MDM but is addressed separately in this document although some components may support both initial provisioning and ongoing management activities.

Application stores are also included as part of MDM by some definitions – the initial deployment of secure mobile services will not include an enterprise application store or any capability for a user to browse and select applications. Initially, there will be very few applications allowed to be installed on secure mobile devices so these can be easily managed by an application repository associated with the provisioning workstation. This will contain approved and signed applications and all necessary applications will be installed during initial provisioning. Patches to these applications and any new applications will initially be provided by physically returning to the provisioning workstation but the goal is to manage this remotely via MDM capability. This will still entail a small number of applications and all changes will be pushed out from MDM using an internal store of approved and signed applications.

The Device Management Service is deployed on the grey network to manage and monitor UEs.

A corresponding MDM client may be required to be installed on the mobile device. The most critical initial capabilities for device management services are:

- **Device Security Assessment**. It is essential for continued security of the overall system that the user equipment is maintained in a secure state after initial configuration and provisioning. Assessing the security status of the device verifies that it is operating as expected with an approved configuration and policy settings. This provides the

foundation for trusting its identity and applications. Initially, this assessment may just be done locally on the device and only checked periodically during inspections by system administrators. The objective goal is to provide remote assessment that will check every device and provide timely status information for each connection attempt to the infrastructure.

- **Device Configuration and Policy Management (especially patch management)**. Another part of maintaining the user equipment in a secure state is the ability to address discovered vulnerabilities by expeditiously applying patches, updating policy settings, and making other changes. Until remote management capability is deployed, this may entail physical return of the device to the Government provisioning workstation for updating. Obviously this is not a practical solution for future larger deployments and is inconvenient for many users. The objective is to provide secure remote management capability that can push patches, policy changes, white/black list changes, trust anchor changes, and new applications to devices.

Table 5-12 lists top-level requirements for specific device policy settings.

Table 5-12 Specific Device Policy Setting Requirements

Req #	Requirement Description	Threshold / Objective
DP.1	The Device Policy shall be configurable to allow or preclude the use of Bluetooth.	T
DP.2	The Device Policy shall be configurable to allow or preclude the use of WiFi.	T
DP.3	The Device Policy shall be configurable to allow or preclude the use of the camera.	T
DP.4	The Device Policy shall be configurable to allow or preclude the use of Near Field Communications (NFC).	T
DP.5	The Device Policy shall be configurable to allow or preclude the use of USB as mass storage.	T

- **Remediation**. The device security assessment will include determination of whether the device is compliant with current configurations. The determination will typically fall in to one of three categories: completely compliant and current, not completely current but acceptably compliant, or non-compliant (and not suitable for operation). If other than completely compliant and current, remediation can be used to update the device. This can be done remotely and online if the device is acceptably compliant. If the device is non-compliant, it probably will need to be returned to the provisioning workstation for reconfiguration. Initially, as noted above, all updating may require physical return to the provisioning workstation but the objective is to provide some level of remediation online. This capability is closely related to Device Configuration and Policy Management.
- **Location Tracking.** It is an important and valuable capability to track the geo-location of mobile devices (although this also entails operational security concerns and risks for some uses). Such tracking can help locate lost or stolen devices and can be used as part

of the authorization decision process (there may be different access rules depending on whether user is inside or outside a given facility or country). The device and the carrier may both capture some of this information and may be able to provide it to the Government infrastructure but not necessarily in real time. The objective goal is to remotely track device location in real time and an ongoing basis.

- **Secure Disable and Wipe.** Responding to theft of secure mobile devices entails multiple actions to ensure that the thief is not able to masquerade as an authorized user and access sensitive resources. Besides updating infrastructure data stores to deny authorization, it is also desirable to erase information from the device. Secure remote wipe capability provides a way to remotely erase data from the device (assuming it is accessible via cellular service). Both the commercial carriers and MDM services can potentially provide remote wipe – but use of the carrier capability will not be allowed. The objective is to provide Government controlled MDM secure wipe. There may be degrees of wipe available (entire device or select areas) – various options would be acceptable with the most important placed on erasing key and certificate material. Secure disable could also be used and would result in the phone being deactivated from the carrier.
- **Collection of audit log records received from the mobile device**. Another important aspect of security is maintaining awareness of what users have tried to do to or with their devices. Audit records will be logged on the device for various actions especially those related to sensitive or potentially suspicious activities. The specific events to log and the information recorded for each will be a function of policy. These audit logs must be protected on the device and reported to the infrastructure to provide awareness, accountability, and oversight. Initially, the collection of audit records from the device may require physical contact either by returning to the provisioning workstation or during an inspection visit by a system administrator equipped with some device capable of extracting the records (perhaps a portable version of the provisioning workstation). The objective goal is to remotely collect audit records from the device each time it connects to the infrastructure so that up to date records are always available.

There are many more MDM functions that can be deployed (although not all are currently available) and will become more useful as device capabilities expand to include data services, stored data on devices, and use of application stores. These include backup and recovery, tracking current inventory of applications, managing more dynamic white/black lists, and supporting online troubleshooting. These are not considered essential for initial deployments but are not precluded.

Table 5-13 lists top-level requirements for Device Management Services. Subsequent tables list the requirements for each sub-service when deployed. For example, it is an Objective requirement to deploy an Audit Collection service (DM.6), but where such a service is deployed it must meet the Threshold requirements of Table 5-19.

Table 5-13 Device Management Requirements

Req #	Requirement Description	Threshold / Objective

Req #	Requirement Description	Threshold / Objective
DM.1	The Device Management Services shall include a Device Security Assessment Service.	O
DM.2	The Device Management Services shall include a Device Configuration and Policy Management Service.	O
DM.3	The Device Management Service shall include a Remediation Service	O
DM.4	The Device Management Services shall include a Location Tracking Service.	O
DM.5	The Device Management Services shall include a Secure Disable and Wipe Service.	O
DM.6	The Device Management Services shall include a Device Audit Collection Service.	O

Table 5-14 Device Security Assessment Requirements

Req #	Requirement Description	Threshold / Objective
DSA.1	The Device Security Assessment service shall be able to assess the device types and operating systems identified for use, e.g., <Vendor X, OS Version Y>.	T=O
DSA.2	The Device Security Assessment service shall be able to interact with client software on the device being assessed to receive requested assessment information.	T=O
DSA.3	The Device Security Assessment service shall be able to authenticate itself to a device.	T=O
DSA.4	The Device Security Assessment service shall be able to request the device to perform integrity measurements and return the results.	T=O
DSA.5	The Device Security Assessment service shall be Security Content Automation Protocol (SCAP) compliant.	O
DSA.6	The Device Security Assessment service shall be able to interact with Mobile Trusted Module (MTM) equipped devices to receive requested attestation and reference integrity measurement information.	O
DSA.7	The Device Security Assessment service shall maintain a data store of assessment results.	T=O
DSA.8	The Device Security Assessment service data store of assessment results shall support multiple assessment records for each device.	T=O
DSA.9	The Device Security Assessment service data store of assessment results shall support requests for assessment results of a device including time of assessment.	T=O
DSA.10	The Device Security Assessment service data store of assessment results shall timestamp each assessment result stored with the time of the assessment.	T=O

Table 5-15 Device Configuration and Policy Management Requirements

Req #	Requirement Description	Threshold / Objective
DC.1	The Device Configuration and Policy Management service shall be able to determine the configuration of the device types and operating systems identified for use, e.g., <Vendor X, OS Version Y>.	T=O
DC.2	The Device Configuration and Policy Management service shall be able to authenticate itself to a device.	T=O
DC.3	The Device Configuration and Policy Management service shall be able to configure the device types and operating systems identified for use, e.g., <Vendor X, OS Version Y>.	T=O
DC.4	The Device Configuration and Policy Management service shall be able to configure policy settings for the device types and operating systems identified for use, e.g., <Vendor X, OS Version Y>.	T=O
DC.5	The Device Configuration and Policy Management service shall accept inputs of approved, signed applications via CD-ROM.	T=O
DC.6	The Device Configuration and Policy Management service shall accept inputs of approved, signed policy settings via CD-ROM.	T=O
DC.7	The Device Configuration and Policy Management service shall verify the integrity of data received on CD-ROM prior to use.	T=O

Table 5-16 Remediation Requirements

Req #	Requirement Description	Threshold / Objective
RR.1	The Remediation service shall be able to remediate the configurations of the device types and operating systems identified for use, e.g., <Vendor X, OS Version Y>.	T=O
RR.2	The Remediation service shall be able to be configured to set the threshold for remediable configurations such as the datedness of the current application versions.	T=O
RR.3	The Remediation service shall be able to authenticate itself to a device.	T=O
RR.4	The Remediation service shall accept inputs of approved, signed applications via CD-ROM.	T=O
RR.5	The Remediation service shall accept inputs of approved, signed policy settings via CD-ROM.	T=O
RR.6	The Remediation service shall verify the integrity of data received on CD-ROM prior to use.	T=O
RR.7	The Remediation service shall maintain a log of each remediation including the device identifier, time of remediation, and outcome.	T=O

Table 5-17 Location Tracking Requirements

Req #	Requirement Description	Threshold / Objective
LT.1	The Location Tracking service shall be able to track the device types and operating systems identified for use, e.g., <Vendor X, OS Version Y>.	T=O
LT.2	The Location Tracking service shall be able to receive location information from the device based on GPS or other geolocation means.	T=O
LT.3	The Location Tracking service shall be able to authenticate itself to a device.	T=O
LT.4	The Location Tracking service shall maintain a data store of collected location information.	T=O
LT.5	The Location Tracking service shall timestamp each location entry in the data store with the time of collection.	T=O
LT.6	The Location Tracking service shall support requests for last known location of a device including time of assessment.	T=O
LT.7	The Location Tracking service shall support requests for location records of a device over a specified period of time.	T=O

Table 5-18 Secure Disable and Wipe Requirements

Req #	Requirement Description	Threshold / Objective
W.1	The Secure Disable and Wipe service shall be able to request audit reporting from the device types and operating systems identified for use, e.g., <Vendor X, OS Version Y>.	T=O
W.2	The Secure Disable and Wipe service shall be able to authenticate itself to a device.	T=O
W.3	The Secure Disable and Wipe service shall be able to command a device to erase all stored data.	T=O
W.4	The Secure Disable and Wipe service shall be able to command a device to erase selected stored data by specifying memory location (internal, microSD, UICC).	T=O
W.5	The Secure Disable and Wipe service shall be able to command a device to erase stored data within a domain (e.g., Government versus personal).	T=O
W.6	The Secure Disable and Wipe service shall be able to command a device to shut down.	T=O
W.7	The Secure Disable and Wipe service shall maintain logs of wipe and disable commands sent including date, command, and device identifier.	T=O

Table 5-19 Device Audit Collection Requirements

Req #	Requirement Description	Threshold / Objective
DAC.1	The Device Audit Collection service shall be able to request audit reporting from the device types and operating systems identified for use, e.g., <Vendor X, OS Version Y>.	T=O
DAC.2	The Device Audit Collection service shall be able to request a device to report stored audit records.	T=O
DAC.3	The Device Audit Collection service shall be able to authenticate itself to a device.	T=O
DAC.4	The Device Audit Collection service shall be able to delete entries from the device audit log.	T=O

5.3.2.2.4 Provisioning Services

This section covers the following architectural components identified in Figure 5-1: Security Management Services, Trust Management, Government Provisioning Service, Audit and Accountability Collection and Analysis, Mobile Application Management, and Mobile Configuration and Access Management.

Provisioning is defined more as a phase of operations rather than a separate set of components and capabilities but there are components that primarily provide provisioning functions so are addressed here. These include core certificate management components and workstations used to configure and initialize the user equipment for secure operations. Provisioning also addresses the infrastructure so that the result is that user equipment and infrastructure components are configured, keyed, registered, and privileged to securely connect, authenticate, and access authorized services.

Provisioning information, for both the mobile device and infrastructure components themselves, originate from different sources. As shown in Figure 5-2, provisioning information may be generated by and obtained from the cellular carrier, infrastructure components (black and grey), and Certificate Authorities (CAs).

The user equipment generally consists of a device (smartphone or tablet) and one or more removable media cards such as Universal Integrated Circuit Card (UICC) and microSD cards.

Information to be provisioned on the mobile device may be delivered on a microSD card. It may remain on the microSD card or it may be copied to the UE itself. In the former case, the microSD card may have to be securely passed from provisioner to provisioner. Commonly used microSD cards are simple memory chips with no data protection. There are some microSD cards that provide both storage and cryptographic protection of the stored data that could be used to relieve distribution security concerns and provided protected storage of data within the device.

Security-critical information such as cryptographic key material is ideally provisioned on either a secure microSD card or a Universal Integrated Circuit Card (UICC). Often referred to as a SIM card, a UICC is actually capable of supporting multiple SIM applications, including the original GSM SIM (SIM) application, UMTS SIM (USIM) application, and ISM SIM (ISIM) application. UICCs provide cryptographic protection of contents. A new Government SIM (GSIM) application

may be developed for securely holding VPN and SVoIP cryptographic keys if existing SIM applications cannot be used or adapted.

Note that only 3G devices based on 3GPP standards generally support UICCs; those based on 3GPP2/CDMA2000 standards do not. 4G-capable devices support UICCs.

Figure 5-2 shows a Device Provisioning Workstation that collects provisioning information and loads it onto the UE. Loading of information onto the UE, including the approved software image, may be performed by a combination of direct connection (e.g., USB), microSD card, and UICC. The Device Provisioning Workstation may be handling highly sensitive information (such as private keys), so it should be a standalone device that is not connected to any networks.

5.3.2.2.4.1 Certificate, Key, and Trust Management

At the heart of provisioning is the certificate, key, and trust management services that provide the foundation for authentication and data in transit protection. The main components of this are the Certificate Authorities (CAs) that process requests for and generate public key certificate material tied to the identities of devices and users.

The eventual goal is to integrate Certificate and Trust Management Services with existing Public Key Infrastructures, but initial CAs may be stand-alone commercial products. As the CAs generate and certify keys for protecting classified information, outsourcing of this function to a commercial certificate issuing service is not recommended. For the same reason, the CAs are not connected to the operational black or grey networks.

Certificate Authorities generate X.509v3 public key identity certificates for distribution to User Equipments, users, and infrastructure components. Maintaining the confidentiality and integrity of the CA's private signing keys is paramount; therefore, they are located in an isolated physically secure location and are not connected to either of the black or grey operational or management networks. In addition to generating certificates, CAs also generate Certification Revocation Lists (CRLs) that contain the identities of public key certificates where the corresponding private key has been lost or compromised. The CA root public keys or certificates (trust anchors) are installed on each component that performs public key verification. While they are not confidential, they must be protected from tampering, both at-rest and in-transit.

Different CAs are used to issue VPN and SVoIP certificates. Under the "Commercial Solutions for Classified" process, the VPN and SVoIP certificates must be issued by different CA products with different roots of trust to eliminate single points of failure.

Certificate Authorities serve two distinct roles as part of the provisioning process (in addition to their ongoing role of issuing CRLs):

1. Certification of private keys. Private keys should ideally be generated on the requesting device and only the public key presented to the CA for certification; however, the CA or Enrollment Workstation may be required in the short term to generate the private keys on behalf of UEs. Mechanisms must be provided to securely replace (supersede) private/public key pairs on a regularly basis with minimal or no interruption in service. The certificate validity period for different types of key will be defined by policy.
2. Provision of trust anchors. Each CA's root key certificate must be loaded onto each device performing public key authentication. The root key certificate is not confidential

but must be protected from tampering or substitution. As root key certificates are generally long-lived, they may be embedded in the mobile device software image rather than having to be loaded separately. When the root key does eventually expire, a new software load will be required. The new load may contain both old and new root key certificates to allow a smooth transition to the new certificate hierarchy.

5.3.2.2.4.2 Provisioning and Enrollment Workstations

Enrollment Workstation. The Enrollment Workstations act as CA clients that provide the user interface for the certificate and CRL issuance process. The Enrollment Workstations may also support on-chip key generation by UICCs such that the private key is never exported from the UICC. If the private key must be loaded on a non-secure microSD card for transport to a UE, it is generated by the Enrollment Workstation and must be immediately erased after being certified and copied to the microSD card. Private keys stored on microSD cards should be encrypted (e.g., using password-based encryption). MicroSD cards with built-in NIST-validated encryption capabilities are preferred where available. MicroSD cards containing private key material must be strictly controlled and securely erased (or destroyed) at the earliest opportunity. The enrollment workstations tied to the CAs interact with microSD cards (threshold) and either microSD cards or UICCs with cryptographic data protection capability (objective) and load certificates and trust anchors on them.

The Enrollment Workstation is responsible for the creation of secret values (PINs, passphrases, or passwords) used to prevent unauthorized disclosure or access to sensitive key material on the target device. If the target device is a UICC, this is likely to be a Personal Identification Number (PIN) that grants access to the SIM application and its associated data. If the target device is a UE (i.e., keys are stored in a logical identity module), this is likely to be a passphrase or password used to derive an AES key (e.g., using the PKCS #5 PBKDFv2 scheme) that wraps the generated key material. While UICCs offer standardized interfaces, protection of key material on the UE must be compatible with the SVoIP and VPN client software. For more information on protecting keys within the UE and where they must be stored, see Section 3: Operating System and Applications Mobile Device Security of this document.

Carrier provisioning functionality. The SIMs or UICCs are provisioned by the carriers with their portion of the provisioning information, the USIM, which provides the identification and authentication material needed to securely connect to the carrier and be authorized for cellular service. This data can either be directly loaded on the UICC by the carrier or the carrier can pass that info to Government provisioning which can load the UICC itself. The threshold capability may be to use a SIM card with direct carrier provisioning. The objective goal would be for the USIM to be logical area on a UICC with the Government controlling its provisioning through coordination with the carrier.

Device Provisioning Workstation. A separate standalone provisioning workstation interacts directly with the mobile device, microSD card, and/or UICC to configure it, load software (e.g., VPN and VoIP clients plus security monitoring/device management client), and sets up any user id/passwords needed. This workstation is the central point for registration so would receive out of band (e.g., CD-ROM) information on device and user certificates and carrier provisioned identities. This workstation is also the store for signed approved applications and manages white lists, mandatory application lists, and any black lists and provides those lists to the device during provisioning.

After initial provisioning, the threshold approach to device management in terms of patch management, configuration management, audit collection, periodic security assessment, new software loads, and policy updates would not be performed over the network remote from the device. The threshold approach is to return the mobile device periodically (or as required) to the Government provisioning workstation for overall configuration updates as well as downloading of collected audit logs and assessment info from the device. Threshold remote device management capabilities may only consist of remote wipe/disable via the carrier and carrier updates to the black cellular radio software (if allowed). The objective goals would be to remotely collect audit and assessment data from device, to push out mandatory patches/security related updates to SW and policy, and to provide Government controlled monitoring and remote wipe/disable (see the MDM section for more discussion of these capabilities).

Table 5-20 lists the requirements for a Certificate Authority, Table 5-21 lists the requirements for an Enrollment Workstations, and Table 5-22 lists requirements for a Device Provisioning Workstation.

Table 5-20 Certificate Authority Requirements

Req #	Requirement Description	Threshold / Objective
CAR.1	The Certificate Authority service shall be able to generate X.509v3 format certificates.	T=O
CAR.2	The Certificate Authority service shall be able to process PKCS #7 and #10 messages.	T=O
CAR.3	The VPN Certificate Authority service shall be able to generate device certificates.	T=O
CAR.4	The VPN Certificate Authority service shall be able to accept a common specified field (e.g., International Mobile Equipment Identity, IMEI) as part of the Distinguished Name for device certificates.	T=O
CAR.5	The VoIP Certificate Authority service shall be able to generate user certificates.	T=O
CAR.6	The VoIP Certificate Authority service shall be able to accept a common specified field (e.g., DoD Electronic Data Interchange Personnel Identifier, EDIPI) as part of the Distinguished Name for user certificates.	T=O
CAR.7	The Certificate Authority service shall maintain a data store of all certificates it has issued including date of issuance and current status.	T=O
CAR.8	The Certificate Authority service shall maintain a Certificate Revocation List (CRL).	T=O
CAR.9	The Certificate Authority service shall process certificate revocation requests.	T=O
CAR.10	The Certificate Authority service shall be FIPS 140-2 level 3 compliant or better.	T=O
CAR.12	The Certificate Authority shall provide certification of 2048-bit RSA keys by signing certificates.	T

Req #	Requirement Description	Threshold / Objective
CAR.13	The Certificate Authority shall provide certification of Suite B ECC keys with a prime modulus of 256 or 384 bits by signing certificates.	O

Table 5-21 Enrollment Workstation Requirements

Req #	Requirement Description	Threshold / Objective
EW.1	The VPN Enrollment Workstation shall be able accept entry of requests for device certificates.	T=O
EW.2	The VoIP Enrollment Workstation shall be able accept entry of requests for user certificates.	T=O
EW.4	The Enrollment Workstation shall be able to interface to a microSD card.	T
EW.5	The Enrollment Workstation shall be able to interface to a UICC.	O
EW.6	The Enrollment Workstation shall be able to load a certificate on to a microSD or UICC.	T=O
EW.7	The Enrollment Workstation shall be able to write CRL data to a CD-ROM.	T=O
EW.8	The Enrollment Workstation shall provide generation of 2048-bit RSA keys, and request/receive corresponding certificates from the applicable PKI.	T
EW.9	The Enrollment Workstation shall provide generation of Suite B ECC keys with a prime modulus of 256 or 384 bits, and request/receive corresponding certificates from the applicable PKI.	O
EW.10	The Enrollment Workstation shall provide the ability for the user to select a secret value (PIN, passphrase, or password) that is used to protect generated sensitive key material (whether generated on the Enrollment Workstation, UE, or UICC).	T=O
EW.11	The Enrollment Workstation shall be configurable to define and enforce complexity policies for the secret value (PIN, passphrase, or password) used to protect sensitive key material.	T=O
EW.12	The Enrollment Workstation shall use the PKCS #5 PBKDFv2 algorithm to derive a Key Encryption Key (KEK) from a passphrase or password.	T=O
EW.13	The Enrollment Workstation shall use the AES-CTR algorithm to wrap sensitive key material using the derived KEK.	T
EW.14	The Enrollment Workstation shall store wrapped key material in a configurable location on the UE.	T
EW.15	The Enrollment Workstation shall generate and store an integrity check value on the UE that allows the UE to subsequently verify that key material has been properly unwrapped.	T

Req #	Requirement Description	Threshold / Objective
EW.16	The Enrollment Workstation shall allow creation of a GSIM application on the UICC that contains VPN and SVoIP client key material.	O
EW.17	The Enrollment Workstation shall allow internal generation of non-exportable private keys by the UICC GSIM application.	O
EW.18	The Enrollment Workstation shall configure the GSIM application to require entry of a PIN that is used to grant access to private key material.	O

Table 5-22 Device Provisioning Workstation Requirements

Req #	Requirement Description	Threshold / Objective
DPW.1	The Device Provisioning Workstation shall be able to accept signed applications provided on CD-ROM.	T=O
DPW.2	The Device Provisioning Workstation shall be able to verify the integrity of signed applications provided on CD-ROM.	T=O
DPW.3	The Device Provisioning Workstation shall maintain a data store of accepted signed applications.	T=O
DPW.4	The Device Provisioning Workstation shall be able to output signed applications provided to a CD-ROM.	O
DPW.5	The Device Provisioning Workstation shall be able to digitally sign material output on CD-ROM.	T=O
DPW.6	The Device Provisioning Workstation shall be able to define device policy settings.	T=O
DPW.7	The Device Provisioning Workstation shall maintain white lists, black lists, and mandatory lists of application applicable to each device type.	T=O
DPW.8	The Device Provisioning Workstation shall be able to interface to a microSD card.	T=O
DPW.9	The Device Provisioning Workstation shall be able to interface to a UICC.	T=O
DPW.10	The Device Provisioning Workstation shall be able to interface to the device via its USB port.	T=O
DPW.11	The Device Provisioning Workstation shall maintain a registration data stores including each device it manages.	T=O
DPW.12	The Device Provisioning Workstation shall accept inputs from CD-ROM, microSD, UICC, and devices to input to the registration data store.	T=O
DPW.13	The Device Provisioning Workstation shall accept requests for device registration information.	T=O

Req #	Requirement Description	Threshold / Objective
DPW.14	The Device Provisioning Workstation shall have the ability to load approved software and scripts, including the monitoring and trusted provisioning applications, onto the device via a microSD card.	T
DPW.15	The Device Provisioning Workstation shall have the ability to load device configuration and policy information, with the exception of confidential key material, onto the device via a microSD card.	T
DPW.16	The Device Provisioning Workstation shall have the ability to load approved software and scripts, including the monitoring and trusted provisioning applications, onto the device over USB.	O
DPW.17	The Device Provisioning Workstation shall have the ability to load device configuration and policy information, with the exception of confidential key material, onto the device via USB.	O

5.3.2.2.4.3 Directory Services

Directory Services were not identified in the Enterprise Mobility Architecture, but may be used as a distribution mechanism for trust management information, specifically X.509v3 certificates and X.509 CRLs. If a Directory Service is not deployed, an alternate method of distributing certificate revocation must be provided.

A Directory Service provides structured storage of attributes associated with named entities. These entities may include human users, UEs, and infrastructure components. Directory Services are often used as a central repository for storing certificates and CRLs. Other users of the Directory Service depend on the infrastructure component products and their ability to make use of Directory Services.

The Directory Service may be integrated with an AAA Service (e.g., a Windows Domain Controller provides both Windows AAA and Active Directory Services).

The Directory Service must implement the Lightweight Directory Access Protocol (LDAP).

Table 5-23 Directory Service Requirements

Req #	Requirement Description	Threshold / Objective
DS.1	The Enterprise Management Infrastructure shall implement Directory Services.	O
DS.2	The Directory Service shall support the Lightweight Directory Access Protocol (LDAP).	T=O
DS.3	The Directory Service shall require user authentication and authorization to perform creation, deletion, or modification of directory entries or attributes.	T=O
DS.4	The Directory Service shall be configurable to require user authentication and authorization to read directory entries or attributes.	T=O
DS.5	The Directory Service shall allow storage of X.509v3 certificates.	T=O

Req #	Requirement Description	Threshold / Objective
DS.6	The Directory Service shall allow storage of X.509 CRLs.	T=O
DS.7	The Directory Service shall be configured in accordance with applicable DISA STIGs and any additional guidance provided by NSA.	T=O

5.3.2.2.4.4 Network Support Services

This section covers the following architectural components identified in Figure 5-1: Secure Session Routing.

Network Support Services do not play a direct role in maintaining network security, but are essential for the operation of the network. As such, they must be properly configured and protected from unauthorized access.

Routers and Switches:

- Routers. Border routers provide the entry points for connections to the carrier network and Internet. These routers are configured with the appropriate external interface (e.g., for a T3 leased line to the cellular carrier). Security-related requirements for border routers are addressed in Table 5-2. Other routers may be deployed internally within the black and grey networks as specified in the detailed network design and addressing plan.
- Switches. Switches act as Ethernet hubs for network segments connected to other segments by routers. Using Virtual LAN (VLAN) technology, a single switch or group of switches may provide logical separation between the User Data and Management LANs to save on hardware costs.

DNS Services. The Domain Name Service (DNS) is a support function that maps names to IP addresses. This allows infrastructure IP addresses to be changed without reconfiguring all devices.

Network Time Services. The Network Time Service support component maintains time synchronization using the Network Time Protocol (NTP). Smartphones generally use the time provided by the cellular carrier, so this is primarily applicable to infrastructure components. The NTP server may obtain accurate time from a GPS receiver.

DHCP Services. The Dynamic Host Configuration Protocol (DHCP) may be used to dynamically assign IP addresses to systems attached to the network; however, DHCP is generally not used with server systems. UEs may be assigned a black IP address by the cellular carrier and a grey IP address by the VPN Gateway. If the carrier assigns the black IP address, the Carrier Access Router may need to perform a Network Address Translation (NAT) function to allow use of a private IP address space in the black network.

Table 5-24 Network Support Services Requirements

Req #	Requirement Description	Threshold / Objective
NSS.1	The Network Support Services shall be able to operate on IPv4 networks.	T=O

Req #	Requirement Description	Threshold / Objective
NSS.2	The Network Support Services shall be able to operate on IPv6 networks.	T=O
NSS.3	The Network Support Services shall provide Network Time Servers that provide time synchronization within the infrastructure networks.	T=O
NSS.4	The Network Support Services shall provide DNS Servers within the infrastructure networks.	T=O
NSS.5	The Network Support Services shall require authentication and authorization of users to stop, start, or change configuration.	T=O
NSS.6	The Network Support Services shall be configured in accordance with applicable DISA STIGs and any additional guidance provided by NSA.	T=O

5.3.2.3 Application Services

This section covers the following architectural components identified in Figure 5-1: Mobility Access Control and Mobility Application.

SIP Services that reside on the grey network are discussed in Section 6: Secure Voice over IP Application.

5.3.2.3.1 Inter-Relationship to Other Elements of the Secure VoIP System

5.3.2.3.2 Access Network Relationship

The cellular carrier's packet core may be connected to the Enterprise Mobility Infrastructure via a leased line (e.g., a T3 line), or a VPN may be established to tunnel through a public network such as the Internet. In both cases, implementing Network Address Translation (NAT) on the Carrier Border Router allows the Enterprise Mobility Infrastructure black IP address space to be hidden from the carrier and any intermediate public networks. The NAT capability should also be configured to only perform inbound NAT for authorized protocols: IPsec, IKE, and optionally LDAP for access to CRL data. In the future, allowed protocols may include those necessary to perform device assessment, such as the Trusted Network Connect (TNC) protocol. The Carrier Border Router should be configured to ignore Internet Control Message Protocol (ICMP) messages ("pings") and not respond to external port scanners in general—the objective is to remain as silent as possible in response to probing attempts and so limit the probability and subsequent success of Denial of Service (DoS) attacks. While the Carrier Border Router can provide a significant degree of protection, is it still supplemental to that provided by its associated Network Firewall. The Carrier Border Router, Network IDS/IPS, and Network Firewall could be combined in a single physical unit, but leaving them as separate units avoids a single point of failure due to product defects or misconfiguration.

Establishment of a VPN association between the UE and the VPN Gateway in the Enterprise Mobility Infrastructure means that the Government is not dependent on the carrier to preserve confidentiality or detect loss of integrity of data-in-transit; however, the carrier's protection

mechanisms provide an important additional layer of protection under the concept of defense-in-depth.

The VPN Gateway in the Enterprise Mobility Infrastructure should be configured to prohibit split-tunneling, thereby ensuring that no unencrypted traffic to or from the grey network can bypass the VPN Gateway and mix with black traffic.

Most, if not all carriers, have the ability to create private networks for enterprises. The enterprise is assigned its own IP address space, and all enterprise data traffic is separated from public (and other enterprise) data traffic such that only enterprise traffic is routed to the enterprise network entry point (carrier border router). This separation provides an additional layer of defense-in-depth, but may result in higher costs to the Government.

The carrier is responsible for ensuring availability of the access network. This includes uptime, coverage, Quality of Service (QoS), and support of over-the-air Authentication and Key Agreement (AKA) protocols for detection of rogue base stations. All 3G and 4G AKA protocols allow rogue base stations to be detected by the UE, but some 2G AKA protocols do not. The AKA protocols also provide protection from man-in-the-middle (MITM) attacks that could allow an adversary to intercept, decrypt, read and/or modify, re-encrypt, and re-transmit over-the-air without detection. The VPN association between the UE and the VPN Gateway ensures that a rogue base station or carrier is unable to view or tamper with user data without detection but UEs should be configured to prohibit connection to 2G networks if more protection is required.

In summary, because Government user data is double-encrypted using proven commercial protocols independently of the carrier and any intermediate networks, the greatest risk posed by these networks is loss of availability.

As discussed in section 5.3.2, it may be necessary to create a channel for exchange of management and monitoring information with the carrier. This channel could be used to securely exchange provisioning, activation, location, billing, and other information electronically with the carrier. If such a channel is created, carrier access should be controlled and preferably limited to Government black network resources only.

Other risks posed by the carrier are related to provisioning and ongoing maintenance of the UE. Many of these risks are mitigated by the design and configuration of the UE, but some must be addressed by the Enterprise Mobility Infrastructure as part of the initial provisioning process. A UE must be provisioned by both the carrier and the Government. Provisioning by the carrier first is preferable, as this gives the Government final control over the state of fully provisioned device. The ideal method of provisioning is for the carrier to provision its access information on a UICC as a USIM application and then deliver the UICC to the Government. The Government may provision the UICC with a separate “Government SIM” (GSIM) application or, if possible, update the USIM application without overwriting or corrupting carrier information. UICCs are specifically designed to allow the secure installation and operation of multiple applications. UICCs are available that have been evaluated under the Common Criteria at up to EAL5. If a UICC is used, the UE itself may be delivered directly to the Government with no carrier involvement.

For UEs that do not support a UICC the carrier provisioning information must be installed in a logical identity module on the UE itself, as must the Government provisioning information. The UE must allow for carrier and Government provisioning information to be securely separated,

ideally to the same degree of robustness as provided by a UICC. If a provisioned device is received from the carrier, the UE and/or Device Provisioning Workstation must ensure that any mandatory Government software loads do not overwrite of corrupt the carrier-provisioned information, whether they are delivered over a tethered connection or via a microSD card.

For ongoing management, the UE must ensure that any over-the-air carrier software or configuration updates are authenticated by the UE and cannot interfere with Government-provisioned information. Similarly, Government over-the-air updates (provided by Device Management Services using MDM capabilities) must not interfere with carrier-provisioned information.

5.3.2.3.3 User Equipment Relationship

The sole purpose of the black network in the Enterprise Mobility Infrastructure is to securely establish and maintain a VPN tunnel between the UE and grey network. All subsequent interactions with the UE occur over the grey network, including application and device management functions.

As part of establishing the VPN tunnel, the VPN Gateway, or associated component, should perform an assessment of the UE. This may include attestation of the UE's integrity status using something like the Trusted Network Connect (TNC) protocol, and an exchange SCAP messages to verify that the UE configuration is correct. The UE should contain roots of trust such as a trusted Boot ROM and Mobile TPM (MTM) to prevent tampering of attestation and configuration information by malicious software in an attempt to hide its presence.

UEs may be pre-configured with grey IP addresses, or grey IP addresses may be dynamically assigned by the VPN Gateway when an IPsec security association has been established (i.e., the UE has been authenticated and authorized to access the grey network).

An important role of Device Management Services is the ability to push mandatory software updates to UEs, and to provide a trusted app store where all apps are digitally signed and can be verified by the UE as being legitimate Government-approved apps.

5.3.2.4 External Interoperability

The current architecture assumes that the Mobility Enterprise Infrastructure is standalone, but allows the possibility of allowing grey-to-grey connectivity between different "mobility domains" via the Grey Network Border Router. The eventual goal is full integration with Government Enterprise Networks running at different classification levels. This integration is discussed in depth in Section 7: Secure Mobile Interoperability, but several aspects relevant to the mobility infrastructure are highlighted below:

- The current focus is secure VoIP interoperability between UEs. In future it will be necessary to provide interoperability with "red" VoIP phones connected to the NIPRNet, SIPRNet, and other Government fixed networks. This will require deployment of Voice and SIP gateways (proxies) between the mobility infrastructure and Government enterprise networks. It may also be necessary to provide connectivity to the Public Switched Telephone Network (PSTN).
- Future data services such web, email, and conferencing cannot be limited to a mobility domain, but must provide interoperability with users attached to various Government

and non-Government wired networks. As with VoIP, secure gateways will be required to route traffic to other networks and provide boundary protection services.

- The current architecture assumes the deployment of standalone CAs. The eventual goal is to integrate with DoD, Federal, and other PKIs to provide scalability as the system expands.
- CND capabilities are initially standalone, but must eventually be integrated with Enterprise CND capabilities.
- Mobility management and monitoring capabilities are initially standalone, but must eventually be integrated with enterprise capabilities to allow, for example, easier monitoring for FISMA compliance. This includes secure configuration management.

5.4 Gap Analysis

Most of the capabilities required for the infrastructure exist and can be implemented today. This includes VPN, call management, firewalls, IDSs, and PKI. What is currently lacking is primarily comprehensive, automated device management capabilities. However, core capabilities are available and manual procedures can accommodate the smaller communities expected for initial use.

The following gaps have been identified:

- Platform assessment: Use of hardware roots of trust and TPM (or equivalent) technology allows UEs and infrastructure components to attest to their integrity status prior to being granted access to the network.
- Support for the Security Content Automation Protocol (SCAP) to monitor compliance with Government secure configuration guidance (e.g., DISA STIGs) is not yet universal.
- Current Mobile Device Management (MDM) solutions are fragmented and generally proprietary. A unified device management solution based on a set of agreed upon open standards is needed.
- The current architecture supports interoperability with other "mobility domains" but is essentially standalone. Management, CND, and other services need to be integrated with existing enterprise services. This includes integration with DoD and Federal PKIs.
- Authorization capabilities are ad-hoc. Authorization decisions are performed independently across the platforms using widely varied techniques. Approaches to streamline the management of authorization information are needed (e.g., centralized authorization attributes).
- Early implementations may rely on a mixture of public key and userid/password authentication. A goal is to migrate to only public key-based authentication of cryptographic sessions, particularly for mobile devices where passwords are more vulnerable. Use of public key cryptography provides two-factor authentication: something you have (a device that holds the private key) and something you know (a PIN or password that unlocks the private key). This prevents a stolen password from being used to gain access to Government resources from a different device.

5.5 Risks

If the Enterprise Mobility Infrastructure is compromised, there is the potential of far reaching ramifications that may affect each deployed user equipment and the missions dependent on these mobile devices. Worst case, compromise of the infrastructure could result in the recall of all UEs so that they can be sanitized and reprovisioned.

5.5.1 Threats and Risks to the System

External Threats and Risks:

- User device or carrier system uses communications paths to introduce malware to Enterprise Mobility Infrastructure.
- User device or carrier system uses communications paths to attempt to access unauthorized resources.

Internal Threats and Risks:

- An operator within the Enterprise Mobility Infrastructure attempts to make unauthorized changes to approved device configurations, policy settings, software, or status, resulting in the loss of confidentiality, integrity, and availability of the system.
- An operator within the Enterprise Mobility Infrastructure attempts to issue unauthorized certificates or modify registration, identification, and authentication data stores to provide access to unauthorized user devices or users.
- An operator within the Enterprise Mobility Infrastructure makes unauthorized attempts to capture red or grey user traffic for eavesdropping or modification.
- An operator within the Enterprise Mobility Infrastructure attempts to misconfigure or disable systems to deny services to users including unauthorized revocation of certificates.

5.5.2 Risk Mitigations to the System

Mitigations to external threats:

- All communications paths into or out of the Enterprise Mobility Infrastructure are monitored and protected. Interfaces with public or commercial systems use multiple layers of boundary protection and cyber defense.
- All entities interacting with Enterprise Mobility Infrastructure systems are authenticated and authorized prior to accessing any services.
- The certificate authority systems and provisioning workstations are not networked so that the possibility of external attack via network is eliminated.

Mitigations to internal threats:

- All operators are authenticated and authorized prior to performing privileged or security relevant services. All such actions are audited. Separation of duties is enforced so that the individual performing privileged functions is audited by a different individual.

- All approved software for devices is signed to provide integrity and source authentication. Operators within the Enterprise Mobility Infrastructure cannot modify or sign software.
- Denial of service due to malicious insider actions, unintentional actions, and system failures will be detected by monitoring systems resulting in notifications to multiple operators.

5.6 References

- U.S. Government Protection Profiles:
  - IPsec VPN Gateway Protection Profile
  - Network Device Protection Profile (NDPP)
  - Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall
  - Virtualization Protection Profile
  - Authentication Server Protection Profile
  - Network Device V2 Protection Profile
  - Enterprise Security Management Protection Profile
  - Hardware Security Module (HSM) Protection Profile
- DISA Secure Configuration Guidance:
  - Network Infrastructure Router L3 Switch STIG v8r9
  - Network Perimeter Router L3 Switch STIG v8r9
  - Network L2 Switch STIG v8r9
  - Network Firewall STIG v8r9
  - Network IDS/IPS STIG v8r9
  - Other Network Devices STIG v8r9
  - Network Policy STIG v8r9
  - Remote Access Policy STIG v2r6
  - Remote Access Server STIG v2r6
  - Remote Access VPN STIG v2r6
  - Enclave STIG v4r3
  - Access Control STIG v2r3
  - Domain Name System Security Checklist v4r12
  - McAfee Antivirus Security Guidance v4r4
  - Symantec Antivirus Security Guidance v4r1
  - DoD Host Based Security System (HBSS) STIG v3r5

- Desktop Application Antispyware General v4r1
- General Desktop Application STIG v4r1
- Directory Services Guidance v1r1
- Microsoft Active Directory STIG v2r1
- Application Services STIG v1r1
- ESX Server STIG v1r1
- Windows 7 STIG v1r7
- Windows 2008 R2 STIG v1r3
- Unix STIG v5r1

- NIST Publications:
  - FIPS 140-2 Security Requirements for Cryptographic Modules
  - FIPS 180-3 Secure Hash Standard (SHS)
  - FIPS 186-3 Digital Signature Standard (DSS)
  - FIPS 196 Entity Authentication Using Public Key Cryptography
  - FIPS 197 Advanced Encryption Standard (AES)
  - FIPS 198-1 The Keyed-Hash Message Authentication Code (HMAC)
- Public Key Cryptography Standards (PKCS):
  - PKCS #5: Password-Based Cryptography Standard
  - PKCS #7: Cryptographic Message Syntax Standard
  - PKCS #10: Certification Request Syntax Standard
- The Committee on National Security Systems (CNSS):
  - NSTISSP-11 Fact Sheet for National Information Assurance Acquisition Policy
  - CNSSP-15 National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information

6 Secure Voice over IP (SVoIP) Application

6.1 Overview

The SVoIP Application provides the inner layer of protection for mobility services and enterprise services required to enable calling to/from “unanticipated users” and mobile-to-mobile secure calls. The SVoIP application also enables interaction with enterprise unified communications services (e.g., enterprise email, contacts, calendaring). TLS is used to protect Session Initiation Protocol (SIP) signaling messages against loss of integrity, confidentiality and against replay. It provides integrated key management with mutual authentication and secure key distribution. TLS is applicable between mobile devices and SIP proxies, or between SIP proxies. The outer layer of protection is provided by using a Virtual Private Network (VPN) client that is integrated at the mobile device operating system level. The inner layer of protection between the SIP Server and VoIP clients is achieved through the use of a TLS protected channel for SIP signaling. The inner layer of protection between VoIP clients is achieved through the use of SRTP.The Secure VoIP section describes the consumer components, mobility enterprise services components, management and provisioning components, and interactions required to enable a secure voice over secure IP call to/from 3G mobile users. In addition to providing protection to disclosure of modification of communication, the TLS protocol described in this section offers mutual authentication between mobile devices and the SIP server in a cryptographically secure manner.

6.2 Description

The basics of the system operation are as follows:

1. Once the end device is fully booted and in a secure state the user can access the device by entering the required pin or passphrase to unlock the screen lock.

2. When the screen is unlocked, and before any other activities, a second passphrase or password is entered to decrypt the device’s memory, which also stores any required keys.

3. The user first starts the VPN, which establishes a tunnel from the device to the infrastructure.

4. Upon establishment of the VPN the user registers to the SIP server via a TLS connection using the username and password unlocked with the second passphrase. This will establish a SVoIP connection that runs over the VPN connection from the user to the SIP server.

Once the user is registered with the SIP server they will be able to send or receive calls. Once registered with the SIP server the system maintains the secure connection until the phone is powered off. Upon a set amount of idle time the screen will lock, and a user has to re-enter the first password to send and receive calls.

6.3 Approach

To establish a secure 3G/4G Mobile to Mobile call a service request is sent by the mobile device, which includes subscriber information, a data service request, and authentication information. The mobile device is the primary component, which authenticates the data transfer. Establishing a cellular Secure Mobile to Secure Mobile call also includes registration with the VoIP infrastructure enabling the infrastructure to forward calls to the distant mobile device.

The dial plan establishes how the call is handled/routed and defines caller capabilities (e.g., ability to make secure call and to place outside/long distance calls). The mobile device will first register with the VoIP infrastructure. Once the mobile device is registered with the VoIP infrastructure, the mobile device will interact with the IP Private Branch Exchange (PBX)/SIP Proxy Server. The IP PBX/SIP Proxy Server is used to locate the distant mobile device and provides signaling. Once the distance end mobile device is found and accepts the proxied SIP-TLS connection, a Secure Real Time Transport (SRTP) connection is established using SDES for key exchange.

6.3.1 Architecture

Figure 6-1 depicts the mobility components interactions in support of secure 3G/4G Mobile to Mobile (SVoIP) voice calling. Section 7 (Secure Mobile Interoperability will discuss calling between mobile SVoIP devices and other systems such as the Public Switched Telephone Network (PSTN).

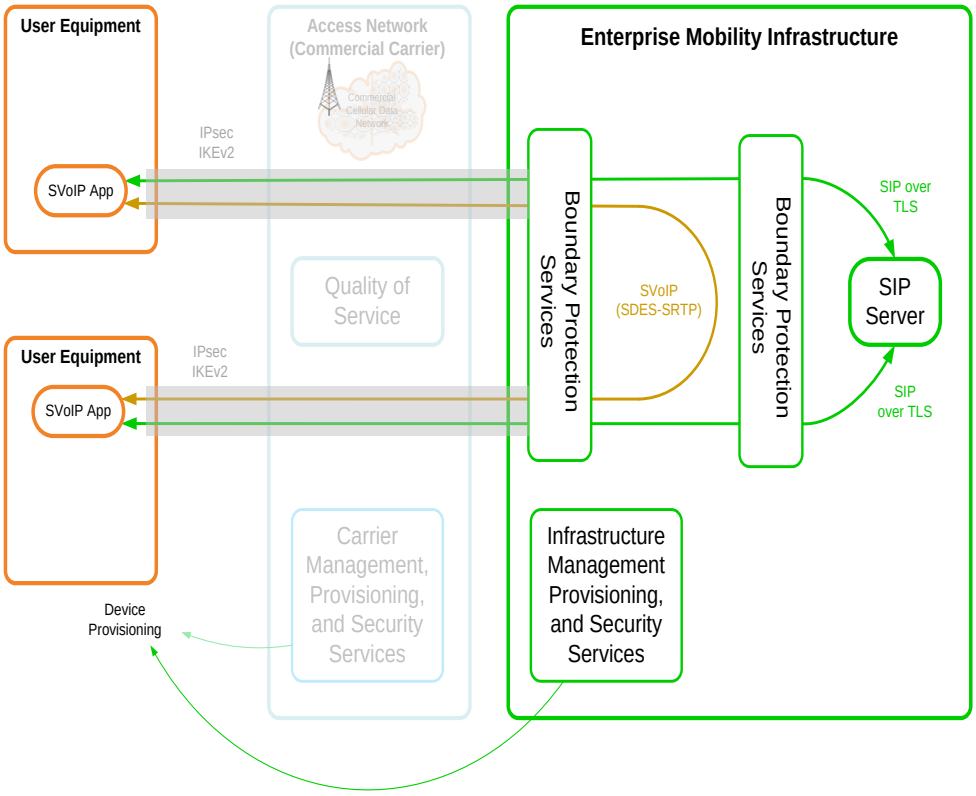

Figure 6-1 Basic Secure VoIP Architecture

6.3.2 Security Relevant Components

Three component types are integral to providing SVoIP capabilities: the consumer's user equipment, the enterprise mobility infrastructure, and the overall management and provisioning of the user's equipment. Two capabilities of the user's equipment are of special interest - the VoIP Application and the necessary security protocols, and the authentication between the user and the device that is also required to authenticate the user and establish secure call session.

6.3.2.1 User Equipment

The User to Device Authentication component:

- Authenticates the call setup session (SIP) and negotiates a session key.
- Authenticates the voice session and negotiates a session key.

The VoIP Application component:

- Performs the call establishment request.
- Negotiates call parameters.
- Establishes a secure call with the called party.
- Terminates the secure call.

Consumer Data and System Protection component:

- Provides host-based firewall and intrusion detection capabilities for SIP and SVoIP.
- Provides software integrity protection for SVoIP application.

The Device external interface component:

- Provides and manages the interface to external and/or removable functional elements (e.g., CAC for user authentication) and protection (e.g., encryption) for the interface to the external and/or removable functional element.

6.3.2.2 Enterprise Mobility Infrastructure

The Enterprise Mobility Infrastructure incorporates robust border protection between mobility and enterprise services along with data flow management across this border, including data scanning/filtering/limiting, protocol termination/bridging, and attribution to sources as required. It offers interworking/mediation services for mobile devices that enhance system and device security. The SIP Server Authentication component:

- Performs access control for user enabling VoIP/SVoIP call.
- Receives user's VoIP/SVoIP call authorization information.
- Sends user/device credentials and call information.

The SIP Services component:

- Provides VoIP call establishment and termination.
- Receives user/device credentials and call information.
- Sends VoIP call establishment and termination event data.

The Mobility Security Services components:

- Provides VoIP and SVoIP call authorization information (PDP), Call Plan, and Call Priority information.
- Sends user's VoIP/SVoIP call authorization information.
- Collects VoIP call records [Call Detail Record (CDR)] regarding establishment and termination event data.
- Receives network monitoring and cyber defense event data related to VoIP/SVoIP call.

The Network Border Routers, Intrusion Detection Systems, and Intrusion Protection Systems components:

- Collects and sends network monitoring and cyber defense event data related to VoIP/SVoIP call.

6.3.2.3 SVoIP Requirements

Req #	Requirement Description	Threshold / Objective
SV.1	The mobility solution shall implement the Session Initiation Protocol (SIP) that complies with RFCs 3261, 4566, and 4568.	T=O
SV.2	The mobility solution shall provide a password for client authentication for SIP REGISTER function requests.	T=O
SV.3	The mobility solution shall protect the SIP communication channel using TLS	T=O
SV.4	The mobility solution shall implement the TLS 1.2 protocol (RFC 5246) supporting Suite B (RFC 6460) ciphersuites, using mutual authentication with certificates.	T=O

6.3.2.4 Encryption Key Requirements

The following requirement is a repeat of the requirements within Section 3, and is repeated here for completeness in dealing with the Secure VoIP application.

Req #	Requirement Description	Threshold / Objective
OEK.3	The ephemeral session encryption key for the SRTP VoIP encryption shall be generated on a per-session basis by the mobile device, and sent through the SIP server to the other mobile device within a SIP message (using SDES)	T=O
OEK.4	The TLS encryption shall meet the requirement as defined in RFC 6460 "Suite B for TLS", Annex A "A Transitional Suite B Profile for TLS 1.1 and 1.0"	T
OEK.5	All SIP messages between the phones and the SIP server shall use TLS.	T=O
OEK.7	The TLS encryption shall meet the requirement as defined in RFC 6460 "Suite B for TLS".	O

6.3.2.5 *Authentication Certificates and Keys Requirements*

The following requirements are a repeat of the requirements within Section 3, and are repeated here for completeness in dealing with the Secure VoIP application.

Req #	Requirement Description	Threshold / Objective
OCK.1	The user authentication private key and the server certificates shall be stored on the end user device and encrypted using an auxiliary password.	T=O
OCK.2	The certificate protection password shall support a minimum of 8 characters long, and be allowed to consist of any combination of upper case letters, lower case letters, digits, and symbols	T=O
OCK.3	The VPN authentication certificates and the SIP/TLS authentication certificates shall be issued by two different CAs.	T=O
OCK.4	Every device/component shall be issued different certificates and corresponding private keys.	T=O
OCK.5	The VPN component of each mobile device shall support the ability to securely contain a unique public key certificate and corresponding private key, used to provide authentication of the mobile device to the network infrastructure, in order to establish a secure communications channel (VPN) with the network infrastructure.	T=O
OCK.6	The SVoIP component of each mobile device shall support the ability to securely contain a unique public key certificate and corresponding private key, used to provide authentication of the mobile device to the SIP server, in order to establish a secure communications channel for sending and receiving SIP messages using TLS.	T=O
OCK.7	The client application shall support the storage of encrypted keys and certificates on the SD cards.	T=O
OCK.9	The SIP server shall support the ability to securely contain a unique public key certificate and corresponding private key, used to provide authentication of the SIP server to the mobile device, in order to establish the TLS channel for SIP messages.	T=O

6.3.3 Inter-relationship to Other Elements of the Secure VoIP System

The SVoIP application provides the secure voice capability to the end-user, and is dependent on all other components of the secure VoIP system being in place. The SVoIP connection runs over the VPN from the user to the SIP server. The outer VPN tunnel is established by routing through the commercial cellular carrier network to the back end government infrastructure. The

certificates used for authentication to both the outer VPN tunnel and inner VoIP tunnel are stored on the mobile device.

Operational considerations include both parties have to be registered within a VoIP/IP telephony infrastructure to receive a call. Architectural considerations include authorization to establish a SVoIP call at a given classification level. Presence is also a consideration in order to initiate a call, to notify a 3G user about missed calls, and messages at potential various classification levels (voicemail boxes).

6.4 Gap Analysis

If a predefined port is not available for SRTP the protocol may run over arbitrary ports. If run arbitrarily the port used for voice can range from any even–number between 16384 and 32766. Deciding which port to use for the SRTP protocol depends on the application, network, and environment.

6.5 Risk

6.5.1 Threats

Several threats specific to the Secure VoIP Application have been identified. With **Unauthorized Access** a user may gain unauthorized access to the mobility solution data and executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or resources. A malicious user, process, or external IT entity may misrepresent itself as the mobility solution to obtain identification and authentication data. An **Unauthorized Update** could occur when a malicious party attempts to supply the end user with an update to the product that may compromise the security features of the mobility solution. An adversary could insert malicious code in the VoIP application to compromise the confidentiality of the VoIP traffic.

There is also a threat against user data that all mobility SIP servers should mitigate. Data traversing the solution could inadvertently be sent to a different user; since these data may be sensitive, this may cause a compromise that is unacceptable. The specific threat that must be addressed concerns user data that is retained by the solution in the course of processing VoIP traffic that could be inadvertently re-used in sending VoIP traffic to a user other than that intended by the sender of the original VoIP traffic.

6.6 References

- Enterprise Mobility Reference Architecture, Description Document, Version 1.0 Draft 3, October 2011.
- Security Requirements for Voice over IP Application, Protection Profile, Version 0.2, *9 December 2011.*
- Security Requirements for Mobility SIP Server, Protection Profile, Version 0.3, 9 December 2011.

- Security Considerations for Voice Over IP Systems, National Institute of Standards and Technology, by D. Richard Kuhn, Thomas J. Walsh, Steffen Fries, January 2005.
- Information Assurance Directorate (IAD), TIPSPIRAL Residual Risk Assessment, 15 December 2011.
- RFC 2119 “Key words for use in RFCs to Indicate Requirement Levels”
- RFC 2543 “SIP: Session Initiation Protocol”
- RFC 4346 “The Transport Layer Security (TLS) Protocol Version 1.1”
- RFC 4492 “Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)”
- RFC 6379 “Suite B Cryptographic Suites for IPsec”
- RFC 6380 “Suite B Profile for Internet Protocol Security (IPsec)”
- RFC 5246 “The Transport Layer Security (TLS) Protocol Version 1.2”
- RFC 6460 “Suite B Profile for Transport Layer Security (TLS)”
- RFC 3261 “SIP: Session Initiation Protocol”
- RFC 4566 “SDP: Session Description Protocol”
- RFC 4568 “Session Description Protocol (SDP) Security Descriptions for Media Streams”

7 Secure Mobility Interoperability

7.1 Overview

This section is a work in progress and will define the architecture for enterprise level interoperability. This section is scheduled for release in the 3rd QTR FY2012. More to come – we promise! The following is the initial discussion based upon being able to connect to existing enterprise services.

7.2 Description

The approach to interoperability within the Mobility solution space can be derived in a straightforward manner from basic Mobility architectural concepts. Mobility at its heart is allowing access to enterprise services from user equipment (commercial mobile devices) via commercial or enterprise wireless access networks.

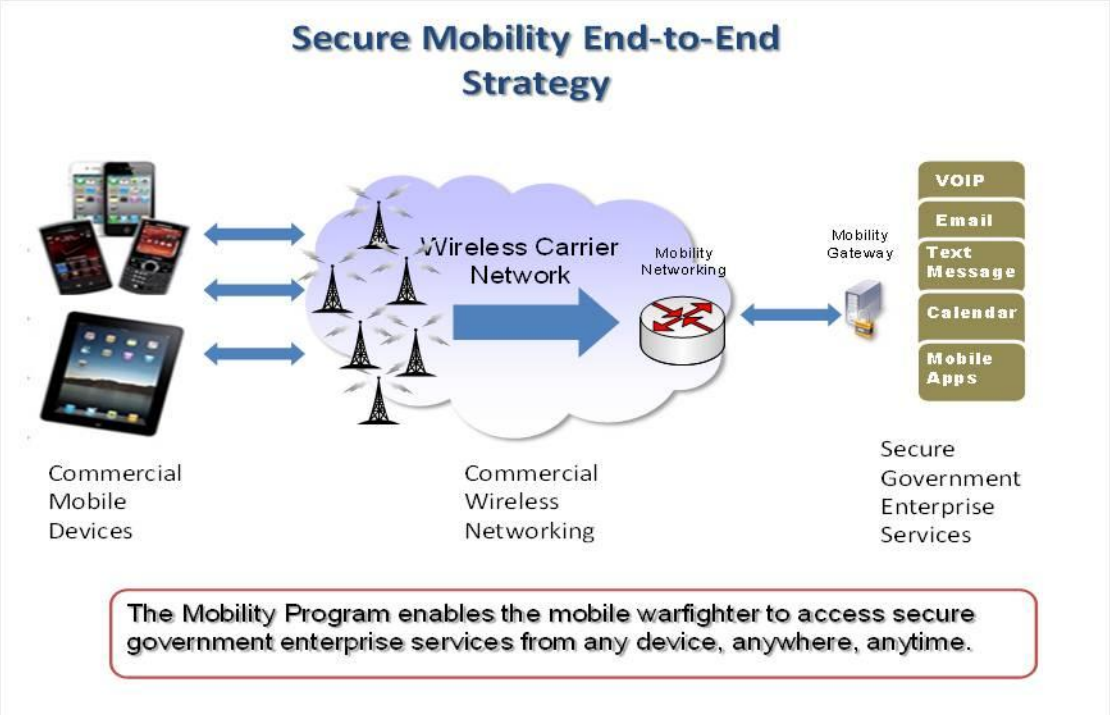

Figure 7-1

There are several ramifications to this architectural strategy in the areas of user commercial user equipment (mobile devices), networking, and enterprise services.

7.2.1 Commercial User Equipment

Commercial, consumer-oriented, devices minimize the device cost, and reduce technical obsolescence by eliminating the development time for government-specific features. On the other hand, commercial mobile devices are complex. They are essentially computer

workstations running a Unix operating system in a small package. They are not a trusted platform, and require mitigation of vulnerabilities in the form of data at rest and data in processing protection. They require a secure computing element for key storage.

7.2.2 Access Networks

Mobility networking also minimizes the cost of the provided service, at the expense of trust. The ramification of the untrusted network is the need for data in transit protection, which will be accomplished by a minimum of two layers of commercial encryption to secure the provided services and applications. The ramification of this is that the only network service used by the mobile device is the data connection that carries the doubly-tunneled sessions. Carrier-provided voice, Short Message Service (SMS), and other value added services are not commercially available to the mobile client. The mobile client can only connect to services in the government enterprise at the other end of the tunnel.

7.2.3 Enterprise Services

Most importantly is the concept of enterprise services, and that mobile devices are one of several category of client. The enterprise service interface becomes the natural point for interoperability, and the natural place for authentication and authorization to occur. Adoption of the widespread best practice of encapsulation of business logic behind the service interface encourages clients to be thin and lightweight. This enables the use of commercial mobile devices by pushing functionality, including security services, into the enterprise. Furthermore, features implemented in the service instead of the client need only be implemented once for all clients. Enterprise services can be broadly categorized into four groups.

1. Unified Capabilities are communications capabilities whose signaling has evolved from the SIP protocol. They include voice, chat, presence, and teleconferencing. Internet protocol Multimedia Services (IMS) is a 3GPP standard for a Mobility Enterprise Services façade to Unified Capabilities.
2. E-mail, which includes delivery and viewing of attachments. E-mail services are typically delivered over a Microsoft Exchange based infrastructure, and may be available in as part of Unified Capabilities and via a web interface.
3. Web applications. The interface to web applications derives from W3C standards. Web applications are typically viewed from a web browser app, although one could readily build a native app to access the same service interface.
4. Virtual desktops. These are typically implemented on a virtual machine provided by a vendor such as VMWare or Citrix, and viewed as a remote display on the client using a dedicated app.

8 ACRONYMS & TERMS

3G	Third Generation standard for mobile telecommunications, includes CDMA
4G	Fourth Generation standard for mobile telecommunications
AT	ATtention (used for sending commands to cellular phones)
CA	Certificate Authority
CDMA	Code Division Multiple Access, a 3G mobile communications standard
CONUS	Continental United States
COTS	Commercial Off the Shelf
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation Lists
CSfC	Commercial Solutions for Classified
CSP	Carrier Service Provider
DTLS	Datagram Transport Layer Security
E911	Enhanced 9-1-1
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
GECC	Global Enterprise Command Center
GSM	Global System for Mobile Communications
IAD	Information Assurance Directorate
IDS	Intrusion Detection System
IP	Internet Protocol
IPSec	Internet Protocol Security
LoE	Level of Effort
Malware	Malicious Software
NIAP	National Information Assurance Partnership
NOT RECOMMENDED	This phrase means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
NSS	National Security Systems
Objective	An objective (O) requirement specifies a feature or function that the Government desires and expects.
OCONUS	Outside the Continental United States
OEM	Original Equipment Manufacturer
OPTIONAL	This word means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the

	same item.
OS	Operating System
OTA	Over The Air
PKI	Public Key Infrastructure
RECOMMENDED	This word means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course
REQUIRED	This word or "SHALL" mean that the definition is a requirement of the specification.
SBC	Session Border Controller
SCIF	Sensitive Compartmented Information Facilities
SDES	Session Description Protocol (SDP) Security Descriptions for Media Streams
SDP	Session Description Protocol
SHALL	This word is a requirement of the specification.
SHALL NOT	This phrase means that the definition is a prohibition of the specification
SIP	Session Initiation Protocol
SRTCP	Secure Real Time Control Protocol
SRTP	Secure Real Time Protocol
SVoIP	Secure Voice Over Internet Protocol
T=O	The threshold requirement also serves as the objective requirement (T=O).
Threshold	A threshold (T) requirement specifies a minimum acceptable feature or function that, in the Government's judgment, still provides the needed capabilities if the corresponding objective requirement cannot reasonably be met (e.g., due to lack of technology maturity, cost or time constraints).
TLS	Transport Layer Security
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity