TABLE OF CONTENTS

SECTION **PAGE**

Section 8 Multifunction Mobile Devices 8-1
8.1 Use Cases for Multifunction Mobile Devices 8-2
8.1.1 Use Case #1: No DoD Network Access or CUI Processing (Non Enterprise Activated) 8-4
8.1.2 Use Case #2: Full DoD Network Connectivity Use Case – No Access to DoD UC Services 8-5
8.1.3 Use Case #3: Full DoD Network Connectivity Use Case with Access to DoD UC Services 8-5
8.2 Backend Support Systems Supporting Multifunction Mobile Devices 8-10

LIST OF FIGURES

FIGURE **PAGE**

Figure 8.1-1. Illustration of Multifunction Mobile Device Use Cases 8-3
Figure 8.1-2. UC Multifunction Mobile Device Application Relationship to the Host Platform 8-6
Figure 8.1-3. Options (VPN and B2BUA) for Secure SC Connectivity From a UC Multifunction Mobile Device Application 8-8
Figure 8.1-4. UC Multifunction Mobile Device Application Access via an Untrusted Internet Connection 8-9

LIST OF TABLES

TABLE **PAGE**

Table 8-1. Multifunction Mobile Devices 8-2
Table 8.1-1. Multifunction Mobile Device Use Cases 8-2

SECTION 8
MULTIFUNCTION MOBILE DEVICES

The UCR section associated with UCF Sectoin 8 addresses the requirements for an array of mobile devices and their associated supporting infrastructure elements. A Multifunction Mobile Device (MMD) is an advanced, yet highly portable computing platform that supports one or more compact input interfaces (e.g., touch screens, stylus, miniature keyboard) to facilitate user interaction. These devices provide network access through primarily wireless means, though wired connectivity may also be a feature of these products. An MMD can assume any number of form factors including, but not limited to, a Smartphone, Personal Digital Assistant (PDA), or small form factor wireless tablet. The requirements for unclassified non-Unified Capabilities (UC) Voice and Video over Internet Protocol (IP) (VVoIP)-related functionality (such as e-mail or Web browsing) provided by the MMDs are generally defined by the Defense Information Systems Agency (DISA) Field Security Office (FSO) Security Technical Implementation Guidelines (STIGs) and Security Requirements Guides (SRGs).

MMDs that have access to Department of Defense (DoD) networks also require support from appliances and systems located at protected DoD installations that provide application services, access control, and remote management. The implementation of these supporting services and infrastructures vary greatly from vendor to vendor; however, the Unified Capabilities Requirements (UCR) uses the generic term “Multifunction Mobile Devices Backend Support System,” or “MBSS,” to represent the appliances that allow MMDs connectivity and reachback to the enclave. As with MMDs themselves, non-UC-related functions of the MBSS (e.g., e-mail, Web browsing) are defined by the appropriate DISA FSO STIGs and SRGs. If the MBSS provides UC VVoIP functionality, this is addressed in UCR 2013, Section 8, Multifunction Mobile Devices. During DoD laboratory testing, the MMD and its associated MBSS are treated as a single System Under Test (SUT). Also, the Session Controller (SC) or Softswitch (SS), at a minimum, will also be included in the SUT if the MBSS provides UC VVoIP capabilities.

NOTE: Currently the UCR defines two primary multifunction mobile device-related product categories: the multifunction mobile device itself and the MMD backend supporting services. However, the UC Steering Group is reviewing proposals to add new product categories or refine these categories to include Mobile Device Manager (MDM), MMD Operational Support System (MOSS), Mobile Application Store (MAS), and other components related to MMDs. The outcome of this decision may result in changes to the current MMD section of this UCF.

Table 8-1, Multifunction Mobile Devices, summarizes the MMD category of the DoD UC Approved Products List (APL).

Table 8-1. Multifunction Mobile Devices

PRODUCT	ROLE AND FUNCTION
MMDs	Advanced mobile computing platform that provides wireless connectivity, basic telephony functions, and portable computing capabilities. The device may also provide UC VVoIP-related services
MBSS	An appliance or collection of appliances that allows remotely connected MMDs to access services within a DoD enclave and provides access control and remote management while maintaining or enhancing the network's security posture NOTE: See previous note concerning possible changes to this product category pending decision by the UC Steering Group.

8.1 USE CASES FOR MULTIFUNCTION MOBILE DEVICES

In the context of the UCR, the scenarios in which MMDs may be used for UNCLASSIFIED applications are currently grouped into three primary use cases, as shown in Table 8.1-1, Multifunction Mobile Device Use Cases.

Table 8.1-1. Multifunction Mobile Device Use Cases

USE CASE NUMBER	TITLE	HIGH LEVEL DESCRIPTION
#1	No Connectivity to DoD Network and No Processing of CUI Data Use Case. No connectivity to DoD e-mail.	MMD that has no connectivity to a DoD network and processes only publicly available DoD data information (Data as defined in this context is clarified in the next section).
#2	Full Connectivity to DoD Network and Processing of Sensitive UNCLASSIFIED Information Use Case. No Connectivity to DoD UC Services.	MMD that supports access to DoD Networks either directly or via a secure tunnel established across public networks. Securely processes and stores DoD information at the CUI level. This MMD does not interace with any DoD UC Services.
#3	Full Connectivity to DoD Network and Processing fo Sensitive UNCLASSIFIED Information Use Case. Full Connectivity to DoD UC Services.	MMD that supports access to DoD Networks either directly or via a secure tunnel established across public networks. Securely processes and stores DoD information at the CUI level. This MMD has full connectivity to DoD UC Services.

Figure 8.1-1, Illustration of Multifunction Mobile Device Use Cases, illustrates the relationship between the primary MMD use cases. The illustration for Use Case #1 shows an MMD with access to only a commercial network and publicly available information. For this scenario, external supporting infrastructure, as shown in the figure, may not, in all cases, be needed or used. The illustration for Use Case #2 depicts the connection of an MMD through a Defense Information Systems Network (DISN) Internet Access Point (IAP) or other DISN gateway to reach DISN services or a homed DoD Component Enclave. Also, the supporting infrastructure in Use Case #2 may, in some cases, be located at the entry point to the DISN instead of at the DoD Component Enclave. Use Case #3 resembles Use Case #2, but involves connectivity to DoD UC services in addition to connectivity to DoD enterprise networks. In Use Case #1, Use Case #2,

and Use Case #3, the MMDs are expected to be Government-furnished devices, whereby an authorized administrator issues and administers the devices on behalf of the user.

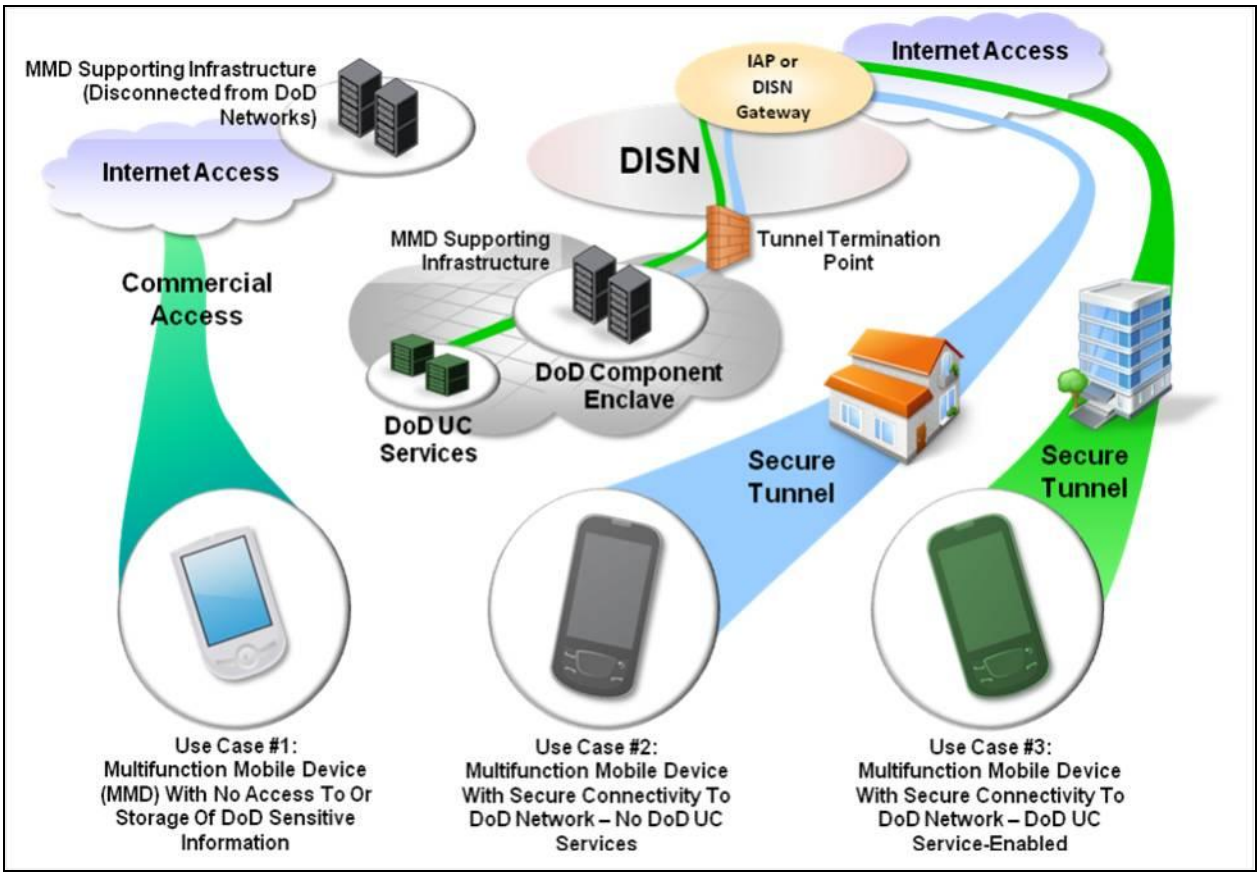

Figure 8.1-1. Illustration of Multifunction Mobile Device Use Cases

At the time of this document's writing, the devices provided for use in all three use cases are expected to be Government furnished. However, even though DoD policy does not currently permit the use of the "Bring Your Own Device" (BYOD) model, various DoD Components are actively examing the use of this approach in conjunction with virtualization, secure boot, and other device hardening techniques. Future developments in mobility dvice security and policy could eventually permit the use of the BYOD approach by DoD Components.

For maximum worldwide interoperability, it is recommended (not required) that these devices support Global System for Mobile Communications (GSM) and General Packet Radio Service (GPRS), at a minimum; generally, however, these devices will support connectivity to the Public Switched Telephone Network (PSTN) and data networks through a wide range of wireless technologies to include 2G, 3G, 4G, Wireless Local Area Network (WLAN), and personal area networking. The following sections describe the use cases in greater detail.

8.1.1 Use Case #1: No DoD Network Access or CUI Processing (Non Enterprise Activated)

While many DoD users of MMDs require the ability to connect to DoD networks and process Controlled Unclassified Information (CUI), pilot efforts within the DoD have determined that a number of scenarios exist in which access to sensitive DoD networks and information is not required. Though completely disconnected from sensitive DoD networks and data information, these MMDs still delivered critical capabilities that facilitated the fulfillment of a DoD component's mission. Examples of the capabilities provided by these types of devices might include the use of MMDs to distribute publicly releasable training materials, flight maps, briefings, or meteorological data.

MMDs supporting this use case can be used to conduct official DoD business; however, devices conforming to this use case are barred from processing, storing, transmitting, or receiving any persistent information (i.e., data or files that are stored or captured on the device) other than that which is publicly releasable and fully UNCLASSIFIED. In this context, persistent information would include, but would not be limited to, e-mail, files, calendar information, Short Message Service (SMS) messages (and similar), and Web-browsing traffic. Sensitive information of a real-time nature that is non-persistent, such as voice and video communications, would not be considered data in this context since such information is stored on the device only in a temporary manner. However, if Use Case #1 devices are used to support sensitive real-time communications, such use must be in accordance with DoD policy including DoD Directive (DoDD) 8100.02. Caution must be exercised when communicating with other DoD entities using devices meeting only the minimum set of requirements specific to Use Case #1 given that such communications would consist of information requiring protection from disclosure.

Use Case #1 devices cannot connect to DoD networks. Network access, if enabled, would generally occur through a commercial network service provider. Connectivity to DoD networks for this use case, even if indirectly through DoD network-connected PCs, is expressly prohibited. In addition, connectivity to and use of commercial voice networks must occur only in accordance with existing DoD policies.

As a result of these DoD network connectivity and processing restrictions, this type of MMD does not have to meet the same rigorous Information Assurance requirements levied on products that connect to DoD networks and process sensitive data information. However, use of these devices by DoD components will still be subject to approval by the DoD Component Designated Approving Authority (DAA).

The DoD Component DAA may also permit the installation of commercial applications on the device to support voice, video, Web browsing, Global Positioning System (GPS), Wi-Fi, and other services. However, DoD e-mail functionality is not permitted for use by MMDs conforming only to Use Case #1 applicable requirements. Technical controls are required to be enforced that allow DoD administrators to control the applications that are permitted for installation on the MMD. Also, if remote management servers are used for the purpose of remote

administration, these supporting infrastructure servers are not permitted to have connectivity to any operational DoD networks. Management of MMDs for this use case is further discussed in Section 8.2, Backend Support Systems Supporting Multifunction Mobile Devices.

8.1.2 Use Case #2: Full DoD Network Connectivity Use Case – No Access to DoD UC Services

Mobile devices conforming to Use Case #2 are permitted to connect to DoD networks, transmit and receive sensitive information, and securely store the received information. However, these devices do not have connectivity to DoD UC Services. The device may connect to the DoD network in a number of ways, including direct access through a wired or WLAN connection or indirect access by establishing a secure overlay across a carrier connection or via a DoD-connected PC. To secure data in transit and storage of data at rest, use of National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) approved cryptographic modules is required. In addition, all the components that compose this system are required to be fully complient from an Information Assureance standpoint based on the approved STIG(s) resulting from the FSO SRG-to-STIG vendor process using the appropriate Mobile SRG(s) and/or STIG(s) directly developed by the FSO.

Requirements for the Use Case #2 MMD platform itself are specified by the DISA FSO SRGs. Conformance of the MMD platform to DISA FSO requirements is validated during testing by the appropriate DoD laboratory or in the field in accordance with the UC Connection Office (UCCO) Process Guide and DoD Instruction (DoDI) 8100.04.

For this scenario, note that certain requirements are applicable to not only the MMD itself, but also the supporting infrastructure responsible for remote monitoring, remote management, and provisioning of the device from a centralized enforcement point. The next section discusses the role that the Backend Support System plays in supporting the MMD's secure reachback into the DoD Component enclave.

8.1.3 Use Case #3: Full DoD Network Connectivity Use Case with Access to DoD UC Services

Mobile devices conforming to Use Case #3 follow the same connectivity model defined for Use Case #2. These devices connect to DoD networks, transmit and receive sensitive information, and securely store the received information. However, in addition to conforming to all Use Case #2 requirements, these devices connect to DoD UC Services. For example, devices following into this use case may support a wide range of Internet Protocol (IP)-enabled applications including VVoIP or XMPP-enabled collaboration services. This UCR defines a "Unified Capabilities (UC) Multifunction Mobile Device Application" (UC Multifunction Mobile Device App) as an application, or series of applications, operating on an MMD that minimally provides VVoIP or XMPP-based collaboration functionality comparable to an End Instrument (EI) or Assured Services End Instrument (AEI) (or collaboration client). However, unlike a typical EI or

AEI, the UC MMD Application operates within the confines of a DISA FSO STIG-compliant MMD host platform.

This UCR specifies the functionality necessary for UC MMD Applications to connect securely to UC VVoIP and XMPP-based systems within DoD enclaves. Other applications may operate on the platform as well to support e-mail, calendar, Web browsing, SMS, and other services. However, the requirements for these additional services are defined in DISA FSO publications. Figure 8.1-2, UC Multifunction Mobile Device Application Relationship to the Host Platform, shows the relationships among a UC MMD Application, other non-UC VVoIP-related applications, and the MMD platform.

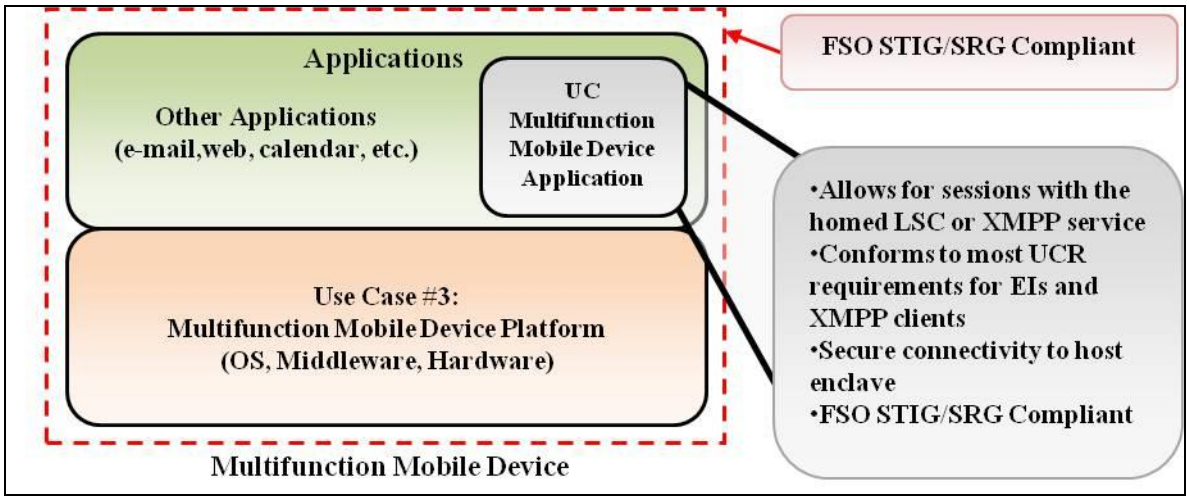

Figure 8.1-2. UC Multifunction Mobile Device Application Relationship to the Host Platform

Even though a UC MMD Application provides functionality similar to a standard EI or AEI, there are some important differences. Primarily, a UC MMD Application will typically leverage untrusted networks to reach its homed DoD enclave. For example, the MMD platform may connect to an untrusted commercial network at Open System Interconnect (OSI) Layers 2 and 3 but then use a secure mechanism at OSI Layer 3, Layer 4, or higher to reach its homed enclave in a secure manner. Also, because public networks in many cases do not provide Quality of Service (QoS) and availability guarantees, calls made using a UC MMD Application may not have availability comparable to calls originating and terminating within the Assured Service UC VVoIP network. Finally, other applications operating on the same platform as the UC MMD Application could provide any number of e-mail, GPS, Bluetooth, Web browsing, Instant Messaging (IM), SMS, and other applications and services. These additional services must not weaken the security posture of the UC MMD Application when it connects to UC services.

The addition of UC MMD Applications to the operating environment not only provides the opportunity for enhanced mobility and connectivity for UC VVoIP network services, but also requires the implementation of additional safeguards to maintain the network's security posture.

Unlike an EI or AEI, which has nearly direct network layer connectivity to its homed SC, a UC MMD Application is permitted to connect to only its homed SC in one of two ways:

1. Establish an encrypted VVoIP signaling and media traffic session with a Back-to-Back User Agent (B2BUA), providing functionality similar to a Session Border Controller (SBC), at the edge of the homed enclave. This B2BUA communicates on behalf of the UC MMD Application to the homed SC using the SC's native, vendor-defined, line-side protocol or UC Session Initiation Protocol (SIP). Secure connectivity with this B2BUA is generally expected to occur at OSI Layer 4 or above.
2. Establish a Virtual Private Network (VPN) tunnel to a VPN server located within the home enclave's Demilitarized Zone (DMZ). The VPN server extracts the VVoIP signaling from the VPN tunnel and transmits the information to the homed SC.

   NOTE: The VPN in this context does not necessarily denote IP Security (IPSec) since a wide range of tunneling mechanisms could be used at various OSI layers to support secure connectivity while maintaining optimal performance. If necessary, a translation step can occur at the VPN server if the information received or transmitted via the VPN tunnel is not already compatible with the SC's vendor-defined line-side protocol or UC SIP.

Regardless of whether a VPN or B2BUA (or both) is used to securely terminate connections from UC MMD Applications at the edge of the enclave, the MBSS is responsible for terminating the secure connection from the UC MMD Application and providing remote management functions.

Figure 8.1-3, Options for Secure SC Connectivity From a UC Multifunction Mobile Device Application, and Figure 8.1-4, UC Multifunction Mobile Device Application Access via an Untrusted Internet Connection, illustrate the possible connectivity options. For simplicity, required additional security elements such as firewalls and Intrusion Detection Systems (IDSs) are omitted from these figures.

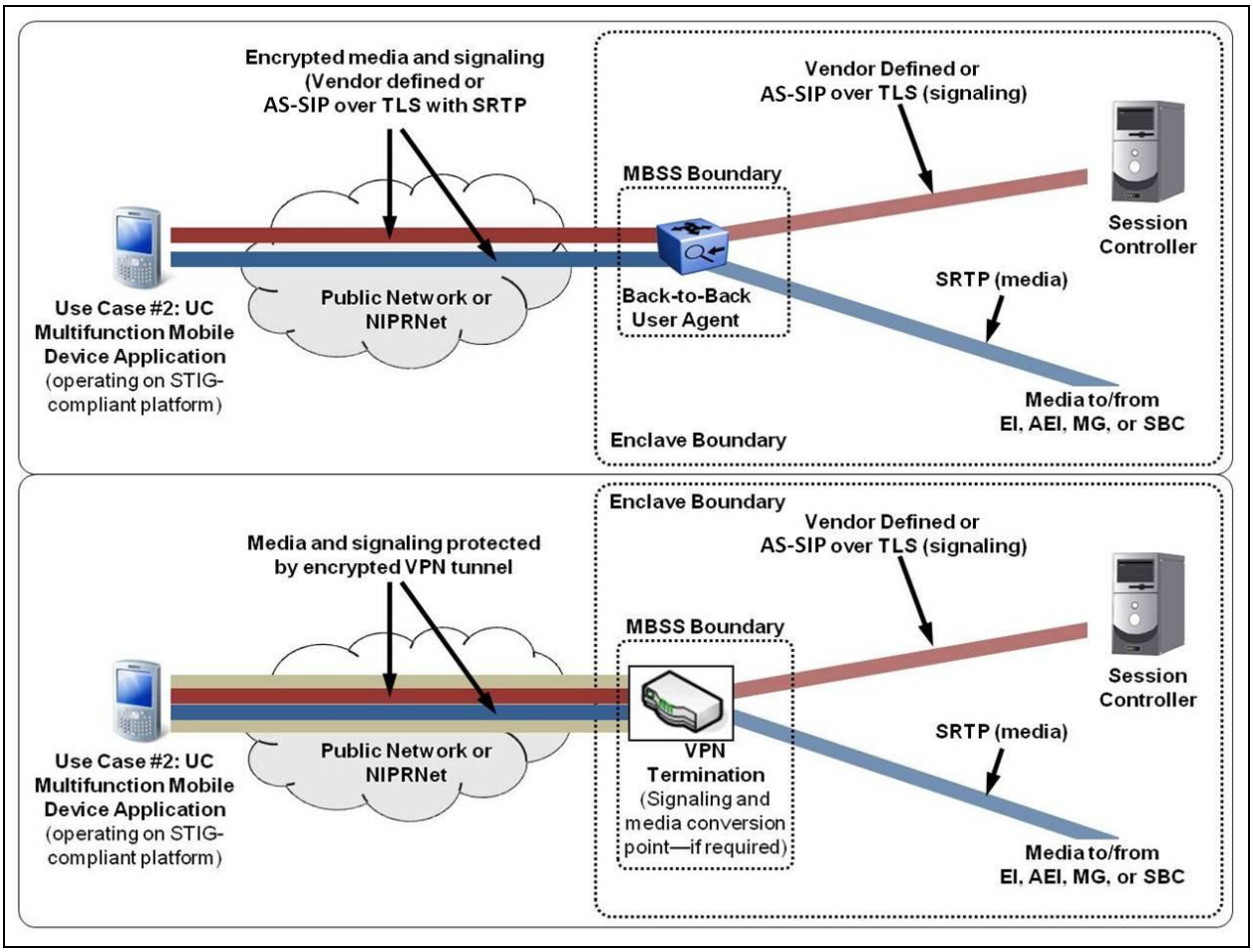

Figure 8.1-3. Options (VPN and B2BUA) for Secure SC Connectivity From a UC Multifunction Mobile Device Application

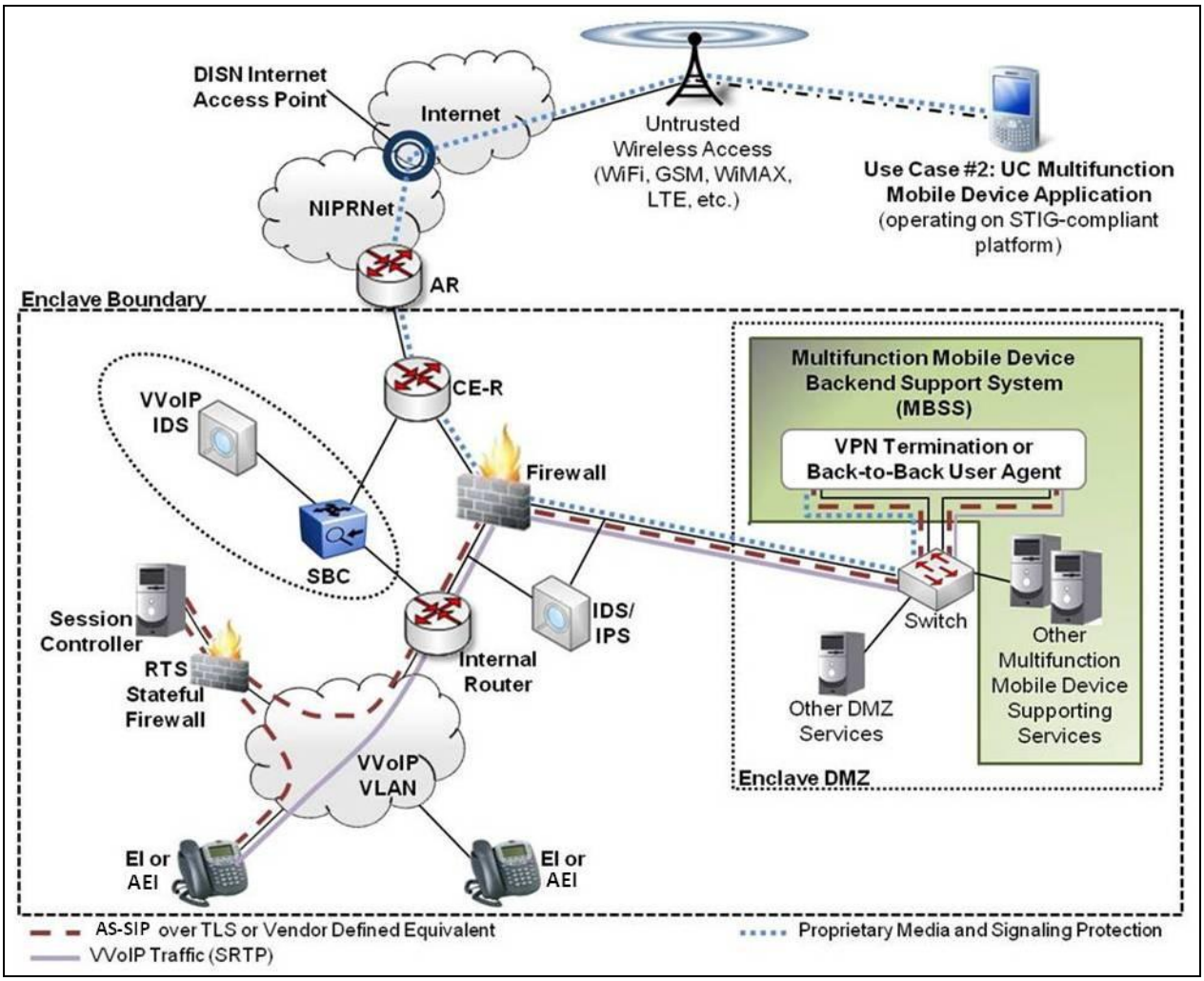

Figure 8.1-4. UC Multifunction Mobile Device Application Access via an Untrusted Internet Connection

From an interoperability standpoint, it is anticipated that UC MMD Application vendors will not field directly compatible solutions. However, because the UC MMD Application relies on its homed SC for session establishment, the SC will serve as the basis for interoperability between other UC SIP devices on the UC network as well as other devices served by the line-side protocol of the SC. As a result, the UC MMD Application and the MBSS are considered to be a part of the SC during testing at an approved DoD laboratory. The UC MMD Application, the STIG/SRG-compliant platform, the MBSS, and the SC are tested together as a complete SUT.

Figure 8.1-4, UC Multifunction Mobile Device Application Access via an Untrusted Internet Connection, provides a more detailed view of how session establishment would occur between a UC MMD Application and a wired EI located within the enclave. Figure 8.1-4 shows a sample DMZ created using a triple-homed firewall; however, other DMZ designs exist using multiple firewalls and could just as easily be implemented to provide secure connectivity for the UC

MMD Application users. (Refer to the latest revision of the Network Infrastructure STIG for information on acceptable DMZ designs.)

Figure 8.1-4, UC Multifunction Mobile Device Application Access via an Untrusted Internet Connection, illustrates the placement of the MBSS within the enclave's DMZ. However, if the system provides B2BUA with dynamic port pinhole functionality similar to that of an SBC, sites may prefer to place the B2BUA in-line with the SBC and data firewall rather than behind the data firewall. For simplicity, this option is not shown in the figure and can be implemented only if done in accordance with (IAW) DISA FSO STIGs and accredited by the site DAA. In addition, the MBSS must provide a VVoIP IDS capability similar to that required of SBCs for VVoIP signaling and for media that traverses the enclave boundary. Existing IDSs can be reused, provided that VVoIP inspection functionality is supported and a dedicated MBSS IDS is not required.

Figure 8.1-4 also shows a call between a UC MMD Application and an EI or AEI. However, the call could just as easily have been routed between the UC MMD Application and an SBC or the Media Gateway (MG), depending on the call source and/or destination. Regardless, the traffic must be in a UC VVoIP-compliant format upon entry into the network. In other words, the VVoIP signaling and media must be protected IAW the requirements in UCR 2013, Section 4, Information Assurance as well as STIGs/SRGs, and the packets must have appropriate Differentiated Services Code Point (DSCP) markings consistent with the requirements in UCR 2013, Section 6, Network Infrastructure End-to-End Performance. Since the platform on which the UC MMD Application resides will likely support other applications besides voice, appropriate marking of the UC MMD Application packets becomes even more important.

The Other Multifunction Mobile Device Supporting Services symbol in the figure represents the services, including authentication of remote devices and checks related to the security posture of the device that must accompany these solutions. These services also may support other non-VVoIP related applications such as e-mail, Web browsing, and IM, as appropriate. In addition, even though the figures show the MBSS VVoIP functionality as being logically separate from the SC, some vendors may choose to implement certain functions within the SC rather than as a service provided by an external device (e.g., providing management for served UC MMD Applications and AEIs and EIs from a central location).

8.2 BACKEND SUPPORT SYSTEMS SUPPORTING MULTIFUNCTION MOBILE DEVICES

In the context of the UCR, the MBSS is a system that supports remote administration, monitoring, and secure enclave access for MMDs. For Use Case #1, the MBSS (if used) supports centralized management of MMDs via commercial networks and is not connected to DoD networks. For Use Cases #2 and #3, the MBSS is located on the DoD network and plays a key role in ensuring DoD policy enforcement and in providing secure DoD enclave access for users of MMDs. The MBSS also facilitates the use of only approved applications and services through the use of granular technical controls and centralized management consoles. The MBSS can take

many forms and is highly vendor dependent; however, some of the common functions and features provided by the MBSS include remote data wipe functionality and remote patch remediation.