Changes to UCR 2008, Change 2, made by UCR 2008, Change 3 for Section 5.3.6, Multifunction Mobile Devices

SECTION	CORRECTION	EFFECTIVE DATE
All	New UCR section created to address Multifunction Mobile Devices	Immediate

TABLE OF CONTENTS

SECTION **PAGE**

LIST OF FIGURES

LIST OF TABLES

5.3.6 Multifunction Mobile Devices

5.3.6.1 Section Overview and Scope

This section addresses the requirements for an array of mobile devices and their associated supporting infrastructure elements. A Multifunction Mobile Device (MMD) is defined as an advanced, yet highly portable, computing platform that supports one or more compact input interfaces (e.g., touch screens, stylus, and 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 MMDs category of the DoD Unified Capabilities Approved Products List (APL) encompasses all of the products and systems discussed in this UCR section. Products listed on the DoD UC APL will have been certified to comply with the subsequently defined UCR requirements and applicable DISA FSO STIGs.

5.3.6.2 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 two primary use cases, as shown in Table 5.3.6-1, Multifunction Mobile Device Use Cases. Additional UNCLASSIFIED use cases can also be defined (such as connectivity of MMDs to assured services UC VVoIP and collaboration systems), but these sub use cases will fall within one of these two primary use cases.

Table 5.3.6-1. 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.	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.

Figure 5.3.6-1, Illustration of Multifunction Mobile Device Use Cases, illustrates the relationship between the two 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 DISN Internet Access Point (IAP) or other DISN gateway to reach DISN services or a homed DoD Component Enclave. Also, the supporting infrastructure in the case of Use Case #2 may in some cases, be located at the entry point to the DISN instead of at the DoD Component Enclave. Both Use Case #1 and Use Case #2 are expected to be Government-furnished devices whereby an authorized administrator issues and administers the device on behalf of the user.

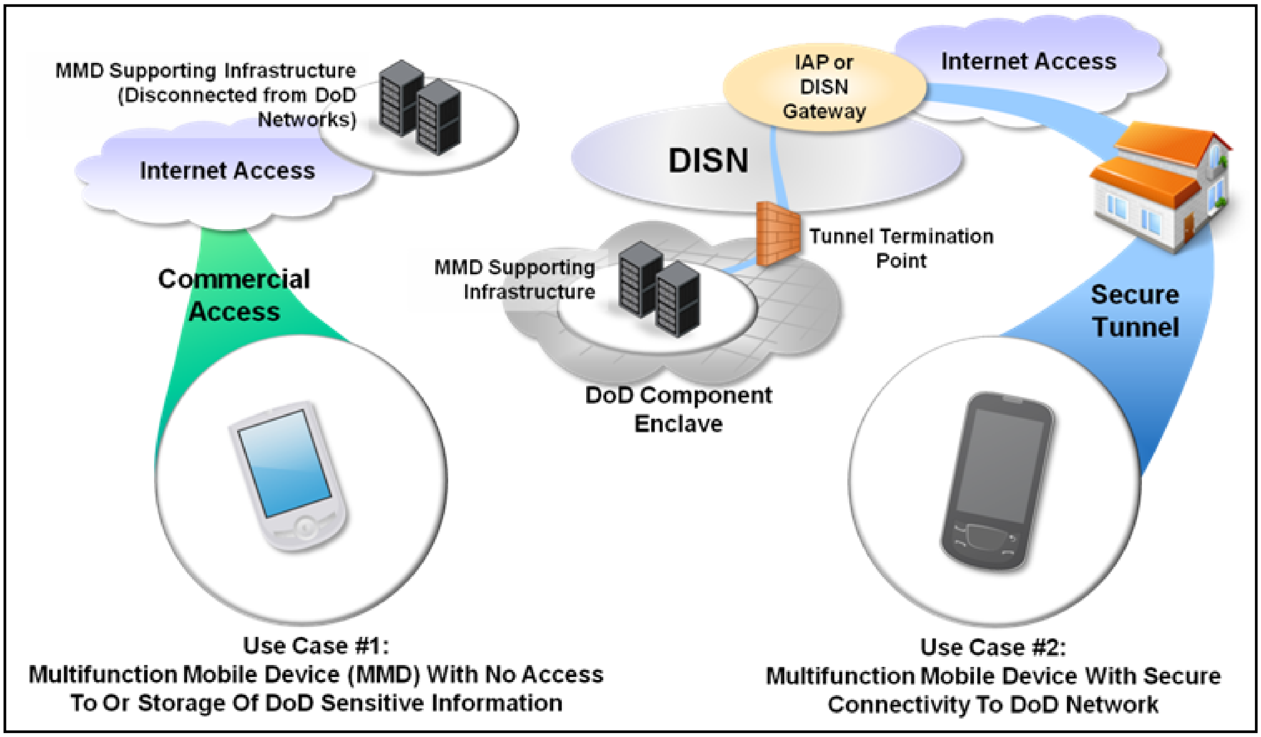
MMD Supporting Infrastructure (Disconnected from DoD Networks)
Internet Access
Commercial Access
IAP or DISN Gateway
Internet Access
DISN
Tunnel Termination Point
MMD Supporting Infrastructure
DoD Component Enclave
Secure Tunnel
Use Case #1:
Multifunction Mobile Device (MMD) With No Access To Or Storage Of DoD Sensitive Information
Use Case #2:
Multifunction Mobile Device With Secure Connectivity To DoD Network

Figure 5.3.6-1. Illustration of Multifunction Mobile Device Use Cases

For maximum worldwide interoperability, it is recommended (not required) that these devices support GSM and GPRS, at a minimum; generally, however, these devices will support connectivity to the PSTN and data networks through a wide range of wireless technologies to include 2G, 3G, 4G, WLAN, and personal area networking. The following sections describe these use cases in greater detail.

5.3.6.2.1 Use Case #1: No DoD Network Access or CUI Processing

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, 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 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, 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 which 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 5.3.6.2.2.1, Backend Support Systems Supporting Multifunction Mobile Devices.

5.3.6.2.2 Use Case #2: Full DoD Network Connectivity Use Case

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. The device may connect to the DoD network in a number of ways, including direct access through a wired or wireless LAN 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 NIST FIPS approved cryptographic modules is required. In addition, all of the components that compose this system are required to be fully STIG compliant from an information assurance standpoint.

Requirements for the Use Case #2 MMD platform itself are specified by the DISA FSO STIGs. 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 UCCO Process Guide and DoDI 8100.04. In addition, for more specialized applications, such as connectivity of the MMD to the DISN to directly obtain UC VVoIP and federated XMPP services, requirements to support this use case are specified in Section 5.3.6.2.1.

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 reach back into the DoD Component enclave.

5.3.6.2.2.1 Backend Support Systems Supporting Multifunction Mobile Devices

In the context of the UCR, the MMD Backend Support System (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 Case #2, 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.

5.3.6.2.2.2 Multifunction Mobile Devices Accessing IP-Based UC Services

MMDs supporting Use Case #2 may support a wide range of IP-enabled applications including Voice and Video over IP (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 EI or 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 5.3.6-2, UC Multifunction Mobile Device Application Relationship to the Host Platform, shows the relationship between a UC MMD Application, other non-UC VVoIP-related applications, and the MMD platform.

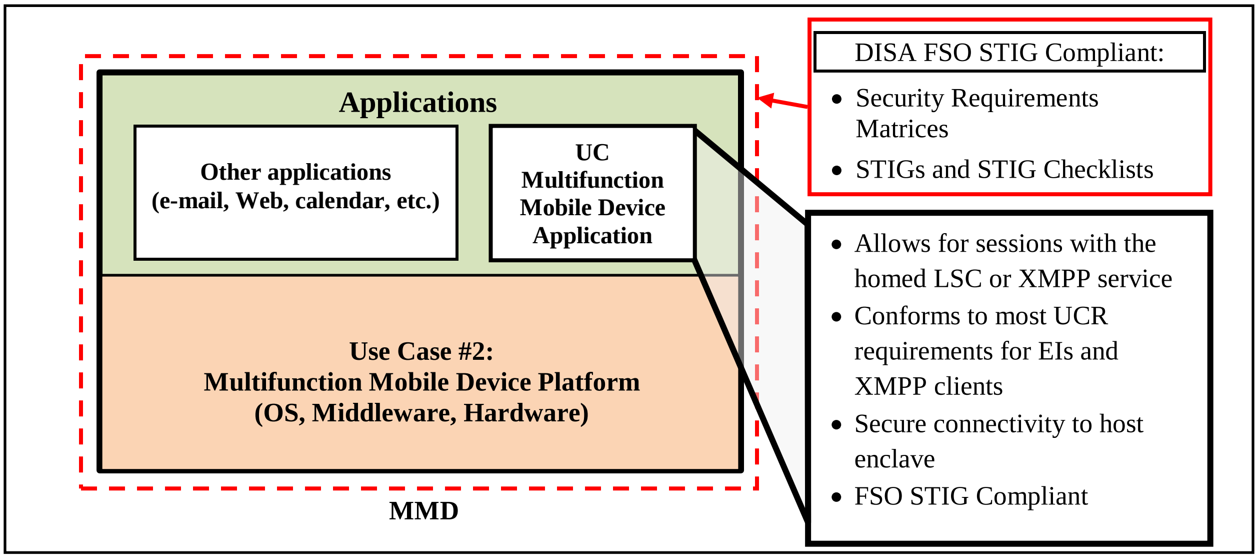
Applications
Other applications
(e-mail, Web, calendar, etc.)
UC
Multifunction
Mobile Device
Application
Use Case #2:
Multifunction Mobile Device Platform
(OS, Middleware, Hardware)
MMD
DISA FSO STIG Compliant:
Security Requirements Matrices
STIGs and STIG Checklists
Allows for sessions with the homed LSC or XMPP service
Conforms to most UCR requirements for EIs and XMPP clients
Secure connectivity to host enclave
FSO STIG Compliant

Figure 5.3.6-2. 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 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 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, 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 LSC, a UC MMD Application is permitted to connect to only its homed LSC 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 an EBC, at the edge of the homed enclave. This B2BUA communicates on behalf of the UC MMD Application to the homed LSC using the LSC's native, vendor-defined, line-side protocol or AS-SIP. Secure connectivity with this B2BUA is generally expected to occur at OSI layer 4 or above.

2. Establish a VPN tunnel to a VPN server located within the home enclave's DMZ. The VPN server extracts the VVoIP signaling from the VPN tunnel and transmits the information to the homed LSC.

   NOTE: The VPN in this context does not necessarily denote 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 LSC's vendor defined line-side protocol or AS-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 5.3.6-3, Options for Secure LSC Connectivity from a UC Multifunction Mobile Device Application, and Figure 5.3.6-4, 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 IDSs are omitted from these figures.

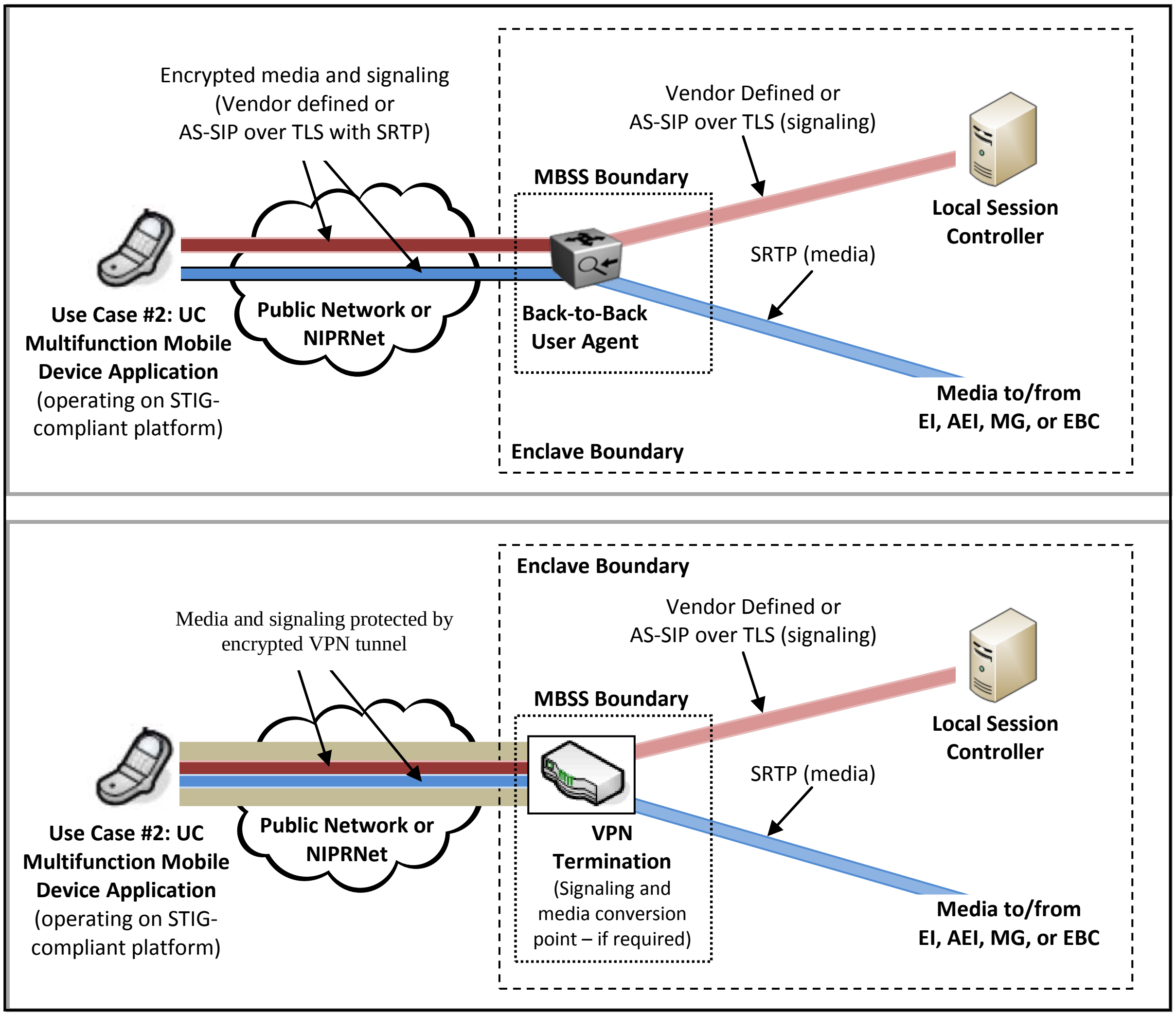
Encrypted media and signaling (Vendor defined or AS-SIP over TLS with SRTP)
Vendor Defined or AS-SIP over TLS (signaling)
MBSS Boundary
Local Session Controller
SRTP (media)
Back-to-Back User Agent
Public Network or NIPRNet
Use Case #2: UC Multifunction Mobile Device Application (operating on STIG-compliant platform)
Media to/from EI, AEI, MG, or EBC
Enclave Boundary
Enclave Boundary
Media and signaling protected by encrypted VPN tunnel
Vendor Defined or AS-SIP over TLS (signaling)
MBSS Boundary
Local Session Controller
SRTP (media)
Public Network or NIPRNet
VPN Termination (Signaling and media conversion point – if required)
Use Case #2: UC Multifunction Mobile Device Application (operating on STIG-compliant platform)
Media to/from EI, AEI, MG, or EBC

Figure 5.3.6-3. Options (VPN and B2BUA) for Secure LSC Connectivity from a UC Multifunction Mobile Device Application

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 LSC for session establishment, the LSC will serve as the basis for interoperability between other AS-SIP devices on the UC network as well as other devices served by the line-side protocol of the LSC. As a result, the UC MMD Application and the MBSS are considered to be a part of the LSC during testing at an approved DoD laboratory. The UC MMD Application, the STIG-compliant platform, the MBSS, and the LSC are tested together as a complete SUT.

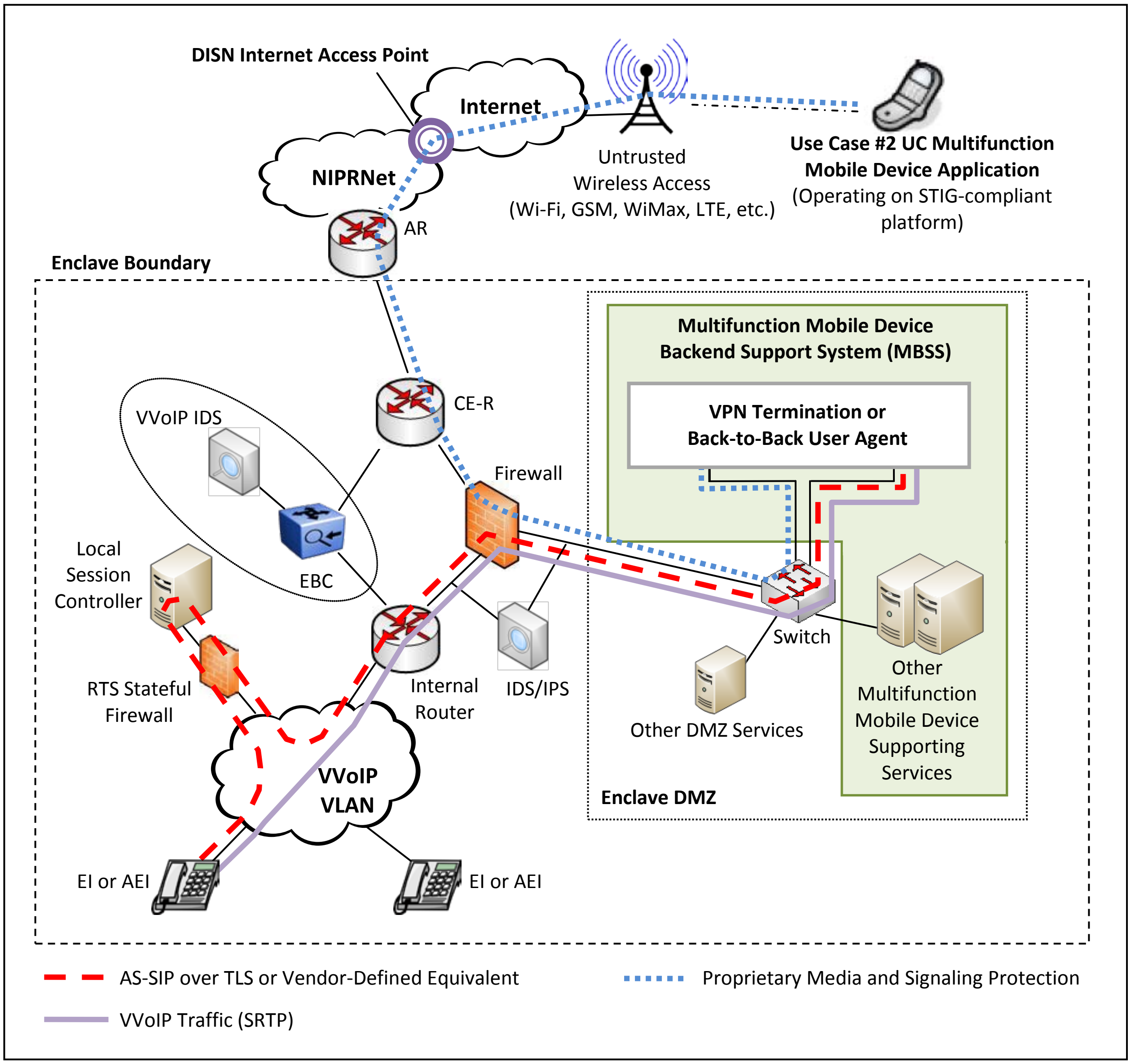

Figure 5.3.6-4. UC Multifunction Mobile Device Application Access via an Untrusted Internet Connection

Figure 5.3.6-4, 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 5.3.6-4 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 5.3.6-4, 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 EBC, sites may prefer to place the B2BUA in-line with the EBC 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 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 EBCs 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 5.3.6-4 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 EBC or the 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 Section 5.4, Information Assurance Requirements, and the packets must have appropriate DSCP markings consistent with the requirements in Section 5.3.3, Network Infrastructure End-to-End Performance Requirements. 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 LSC, some vendors may choose to implement certain functions within the LSC 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).

5.3.6.2.2 Multifunction Mobile Device Approval Process

Conformance to the requirements specified in this UCR as well as to DISA FSO STIGs is validated during testing at the appropriate DoD Component laboratory in accordance with DoDI 8100.04, with additional details for the process being specified in the UCCO Process Guide posted at www.disa.mil/ucco.

5.3.6.3 Requirements

5.3.6.3.1 Introduction

The following sections contain the specific requirements applicable to MMDs and any supporting infrastructure conforming to the previously described use cases. IA and interoperability testing of these requirements will occur in accordance with DoDI 8100.04 and the UCCO Process Guide currently located at http://www.disa.mil/ucco.

The requirement key words (i.e., Required, Conditional) are defined elsewhere in this UCR. Failure to satisfy an IA requirement will result in a UCR Category I, II, or III finding. Failure to satisfy any interoperability requirements will result in a Test Discrepancy Report, which will be adjudicated following DoD laboratory testing as part of the UCCO process.

Table 5.3.6-2, Acronyms and Appliances Specifying Type of Component, shows the acronyms and appliances that represent a specific UC APL product.

Table 5.3.6-2. Acronyms and Appliances Specifying Type of Component

ACRONYM	APPLIANCES
MMD	MMD (Includes the platform hardware, OS, applications, and ancillary devices such as Bluetooth CAC readers)
MMD_OS	MMD Operating System (Denotes requirements that are specific to only the operating system portion of the MMD)
UC_MMD_App	Unified Capabilities MMD Application (Applications residing on a Use Case #2 MMD providing IP-based connectivity to DoD UC services including VVoIP and XMPP services)
MBSS	MMD Backend Support System (Includes the system hardware, OS, applications, and any required ancillary equipment)

5.3.6.3.1.1 The [Alarm] Tag: Generation of Alarms

If the **[Alarm]** tag appears after a requirement’s applicability statement (e.g., Required and Conditional), this tag has the same meaning as defined in Section 5.4.6.1.1, The Alarm Tag, Generation of Alarms.

5.3.6.3.2 Requirements for Multifunction Mobile Devices Conforming to Use Case #1

1. **[Conditional: MMD, MBSS]** If the system conforms to Use Case #1, the system shall comply with all requirements defined within the appropriate DISA FSO STIG(s).

5.3.6.3.3 Requirements for Multifunction Mobile Devices Conforming to Use Case #2

1. **[Conditional: MMD, MBSS]** If the system conforms to Use Case #2, the system shall comply with all requirements defined within the appropriate DISA FSO STIGs.

   NOTE: At the time of this writing, the DISA FSO Wireless STIGs contain the most directly applicable IA requirements for Use Case #2 mobile devices. However, other STIGs such as the Application Security and Development STIG and the Access Control STIG, also contain critical requirements for Use Case #2.

5.3.6.3.3.1 Requirements for Use Case #2 Multifunction Mobile Devices and Backend Support Systems Supporting UC Applications

1. **[Conditional: UC_Multifunction_Mobile_App]** If the MMD supports a UC MMD Application to allow direct connectivity to DoD-provided UC services, then the application shall comply with the subtended requirements:

   a. **[Required: UC_Multifunction_Mobile_App]** The UC MMD Application shall support the capability to operate on a platform that complies with all requirements contained in applicable STIGs.

   b. **[Required: UC_Multifunction_Mobile_App]** The application shall conform to all functional and IA requirements specified for EIs or AEIs (if the application implements AS-SIP) in the UCR, with the exception of the following requirements:

      NOTE: This includes, but is not limited to, the capability to support operation on IPv6-enabled MMD platforms and connected networks.

      (1) **[Conditional: UC_Multifunction_Mobile_App]** If the application does not support all codec types specified in Section 5.3, IP-Based Capabilities and Features, for EIs and AEIs, this noncompliance is permitted, provided that the application's homed MBSS transcodes appropriately when communicating with the LSC (or MFSS or SS), thereby maintaining interoperability with normal EIs and AEIs that do support these codecs.

NOTE: This requirement is intended to accommodate bandwidth-constrained wireless networks where codecs such as G.711 may consume too much bandwidth.

(2) **[Conditional: UC_Multifunction_Mobile_App]** When the UC MMD Application connects to its homed LSC via the MBSS, it is not required to support the capability to support MLPP or display the precedence level of calls. However if it does so, it must do so IAW the requirements in Section 5.3.2, Assured Services Requirements.

c. **[Required: UC_Multifunction_Mobile_App]** All media (e.g., voice and video) exchanged between the UC MMD Application and the MBSS shall be protected using encryption, authentication, and integrity mechanisms that are validated as conforming to FIPS 140-2 level 1 requirements (i.e., must use a FIPS 140-2 validated module).

(1) **[Required: UC_Multifunction_Mobile_App]** The cryptographic profile (algorithms used for confidentiality, integrity, etc.) used to establish secure connectivity from the UC MMD Application to the MBSS to transmit signaling information shall be equal to or stronger than the profiles specified for the TLS and IPSec in Section 5.4, Information Assurance Requirements.

(2) **[Required: UC_Multifunction_Mobile_App]** For VVoIP media traffic, the cryptographic profile shall be equal to or stronger than the profile defined for SRTP in Section 5.4, Information Assurance Requirements.

d. **[Required: UC_Multifunction_Mobile_App]** The application shall support the capability to authenticate, perform integrity checks, and encrypt or decrypt data exchanged with the MBSS using, at a minimum, strong shared secrets.

NOTE: Strong shared secrets would include using a passphrase meeting the complexity requirements specified in this section or pre-shared symmetric keys that support the minimum randomization and length requirements defined Section 5.4, Information Assurance Requirements.

e. **[Conditional: UC_Multifunction_Mobile_App]** If the application connects directly to a DoD-controlled WLAN enclave and bypasses its homed MBSS to connect to its LSC, the application and its associated platform shall conform to all requirements applicable to WEIs specified in Section 5.3, IP-Based Capabilities and Features.

f. **[Conditional: UC_Multifunction_Mobile_App]** Any chat or collaboration capabilities provided by the UC MMD Application shall be IAW Section 5.7, Instant

Messaging, Chat, and Presence/Awareness.

NOTE: This conditional requirement is in addition to any applicable STIGs and STIG checklists such as the Instant Messaging STIG.

g. **[Objective: UC_Multifunction_Mobile_App]** If the device is locked, possibly in a lower power state, but not powered off, the UC MMD Application shall provide users with the capability to continue to receive calls from its homed LSC or SS, via the MBSS, while in this state.

NOTE: The goal of this requirement is to ensure that the device does not require the user to have the device unlocked and fully active (i.e., display on at full power, all components fully active) to receive calls and to facilitate better battery life for the mobile device.

2. **[Conditional: MBSS]** If the MBSS provides connectivity to the LSC (or SS or MFSS) on behalf of any served UC MMD Applications, the product shall conform to the subtended requirements:

a. Reserved:

(1) Reserved.

b. **[Required: MBSS]** The system shall support, at a minimum, the capability to remotely administer (e.g., remote wipe, remote kill, disable) UC MMD Applications.

NOTE: The specific commands for remote administration that must be supported are defined in DISA FSO STIGs and security requirements matrices.

c. **[Required: MBSS]** The system shall ensure that separation is maintained between concurrent sessions transiting the system established from UC Multifunction Mobile Applications.

NOTE: Since the MBSS may have a large number of sessions (signaling and media) traversing its system boundaries, this requirement is intended to prevent a user from accessing other sessions traversing the MBSS that are not assigned to that user.

d. **[Required: MBSS]** Unless explicitly stated otherwise by the subtended requirements, on the interface used by the MBSS to communicate with its homed LSC or SS, the MBSS shall act as any other EI or AEI and so comply with all functional and IA requirements in this UCR for EIs or AEIs as appropriate.

(1) **[Required: MBSS]** If the VVoIP media traffic transmitted between the UC MMD Application and the MBSS does not use one of the codecs required in Section 5.3, IP-Based Capabilities and Features, then the system shall support a transcoding function that securely translates this media traffic into a format compatible with the LSC line-side protocol.

(2) **[Required: MBSS]** The system shall ensure that VVoIP media, signaling, IM, e-mail, Web browsing, and any other supported traffic originating from the MMD that traverses the MBSS is marked with the appropriate DSCP value specified in Section 5.3, IP-Based Capabilities and Features, upon entrance into the enclave UC network.

NOTE: Ideally, the MBSS should place UC VVoIP traffic onto a VLAN that is separate from the VLAN used for other non-UC VVoIP related services (e.g., e-mail).

(3) **[Conditional: MBSS]** If the served UC MMD Applications do not support MLPP, the MBSS shall interface with its homed LSC and use the procedures defined in Section 5.3.2, Assured Services Requirements, to handle calls received above the ROUTINE level that cannot be forwarded to the UC MMD Application (e.g., forwarding to an attendant).

e. **[Required: MBSS]** The system shall provide secure connectivity, at a minimum, by implementing B2BUA (EBC-like) application layer gateway functionality or VPN termination functionality when communicating with served UC MMD Applications.

(1) **[Required: MBSS]** The UC VVoIP network-related traffic (VVoIP media, signaling) that appears on the network as it transits the system shall remain encrypted at all points with cryptographic strength consistent with the TLS and IPSec profiles (signaling) and SRTP profile (for media) specified in this section of the UCR. The system must not rely on physical safeguards alone to provide confidentiality for data in transit.

NOTE: The MBSSs that provide UC VVoIP capabilities also must conform to the VVoIP IDS monitoring requirements in Section 5.4.6.2.1.5, Authentication Processes, and Section 5.4.6.2.3, Confidentiality.

(2) **[Required: MBSS]** The portions of the MBSS that establish secure connectivity to the UC MMD Application and other security critical components of the MBSS (specifically any portions of the MBSS that provide functionality equivalent to devices specified in existing protection profiles

including FWs, IDSs, and VPNs) shall be validated against the NIAP-validated process for that technology.

NOTE: The system can use and incorporate already NIAP-validated components in a secure manner to comply with this requirement.

NOTE: The NIAP Program Office determines whether CC mutual recognition can be used to satisfy this requirement. Protection profiles or an NIAP-approved security target, if no protection profile exists, will be used during the product's evaluation.

f. **[Objective: MBSS]** The system shall provide number portability and call forwarding features. This capability shall allow users who travel outside of the enclave to use the same profile and phone number associated with their assigned EI or AEI within the enclave but on their UC MMD Application.

g. **[Objective: MBSS]** The product shall support the capability to allow UC MMD Applications to participate in audio and video conferences in a voice-only mode when bandwidth or resources do not permit transmission of the full audio/video media stream to the UC MMD Application.

3. **[Required: MBSS]** The product shall support either an onboard VVoIP IDS/IPS capability that can monitor all VVoIP signaling and media traffic in decrypted form or the capability to present all signaling and bearer traffic to an external VVoIP IDS/IPS in a secure manner.

a. **[Required: MBSS] [Alarm]** The VVoIP IDS/IPS threat detection capabilities shall be IAW the VVoIP IDS/IPS functional requirements specified in Section 5.8, Security Devices Requirements. The product shall support the capability to generate and transmit an alarm to the NMS when these threats are identified.

b. **[Conditional: MBSS]** If the product provides the capability to transmit decrypted media and signaling to an external VVoIP IDS/IPS platform, the product shall at a minimum provide FIPS-compliant confidentiality and integrity for this information in a manner that conforms to the cryptographic profiles specified for TLS and IPSec in Section 5.4, Information Assurance Requirements.

c. **[Conditional: MBSS]** If the product provides the capability to transmit decrypted VVoIP media and signaling to an external IDS/IPS platform, then this interface shall use publicly accessible specifications and standards.

NOTE: The intent of this requirement is to ensure that third-party IDS/IPS vendors have the information necessary to create an interface that can accept and process the received VVoIP information.