TABLE OF CONTENTS

SECTION **PAGE**

LIST OF TABLES

SECTION 8
MULTIFUNCTION MOBILE DEVICES

8.1 INTRODUCTION

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. A more detailed discussion on multifunction mobile devices, supporting infrastructure, and DoD approved use cases can be found in Unified Capabilities Framework (UCF) 2013, Section 8, Multifunction Mobile Devices.

The MMD category of the Department of Defense (DoD) Unified Capabilities (UC) Approved Products List (APL) encompasses all of the products and systems discussed in this Unified Capabilities Requirements (UCR) section. Products listed on the DoD UC APL will have been certified to comply with the subsequently defined UCR requirements and applicable Defense Information Systems Agency (DISA) Field Security Office (FSO) Security Technical Implementation Guidelines (STIGs) and Security Requirements Guides (SRGs).

NOTE: Currently, the UCR defines two primary multifunction mobile device-related product categories: the MMD 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 UCR.

8.1.1 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 two primary use cases, as shown in Table 8.1-1, Multifunction Mobile Device Use Cases. Additional discussion regarding these uses cases occurs in UC Framework 2013, Section 8, Multifunction Mobile Devices.

Table 8.1-1. Multifunction Mobile Device Use Cases

USE CASE NUMBER	TITLE	HIGH LEVEL DESCRIPTION
#1	Non Enterprise Activated Use Case: 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 Section 8 of the UCF)
#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
#3	Full Connectivity to DoD Network and Processing of Sensitive UNCLASSIFIED Information Use Case Full Connectivity to oOD 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

8.1.2 Multifunction Mobile Devices and Components

Table 8.1-2, Acronyms and Appliances Specifying Type of Component, shows the acronyms and appliances that represent a specific UC APL product.

Table 8.1-2. Acronyms and Appliances Specifying Type of Component

ACRONYM	APPLIANCES
MMD	MMD [Includes the platform hardware, Operating System (OS), applications, and ancillary devices such as Bluetooth Common Access Card (CAC) readers]
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 Extensible Messaging and Presence Protocol (XMPP) services]
MBSS	MMD Backend Support System (Includes the system hardware, OS, applications, and any required ancillary equipment) (The term MMD Operational Support System may replace this term in subsequent UCR revisions)

8.2 REQUIREMENTS

8.2.1 IO and IA Test Report Considerations

Beginning with UCR 2013, all UCR requirements will be adjudicated as Technical Deficiency Reports (TDRs) and will appear only in Interoperability (IO) test reports. The DISA FSO STIGs and SRGs shall form the basis for any Information Assurance (IA) findings appearing in IA test reports. As a result, some requirements have been removed from this section in order to minimize duplication between IA findings and IO TDRs in test reports.

8.2.2 The [Alarm] Tag: Generation of Alarms

If the [Alarm] tag appears after a requirement's applicability statement (e.g., Required or Conditional), then this tag has the same meaning as defined in Section 4.2.1, The [Alarm] Tag: Generation of Alarms.

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

MMD-010000 [**Conditional: MMD, MBSS, MDM**] If the system conforms to Use Case #1, then the system shall comply with all requirements defined within the appropriate DISA FSO STIG(s) and SRG(s).

NOTE: At the time of this writing, the DISA FSO General Mobile Device (Non-Enterprise Activated) STIG serves as one of the primary baselines for Use Case #1.

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

MMD-020000 [**Conditional: MMD, MBSS, MDM**] If the system conforms to Use Case #2, then the system shall comply with all requirements defined within the appropriate DISA FSO STIGs and SRGs.

NOTE: At the time of this writing, the DISA FSO Wireless STIGs and SRGs contain the most directly applicable Information Assurance (IA) requirements for Use Case #2 mobile devices.

8.2.5 Requirements for Multifuction Mobile Devices Confroming to Use Case #3

MMD-030000 [Conditional: MMD, MBSS, MDM] If the system conforms to Use Case #3, then the system shall comply with all requirements identified in this UCR for Use Case #2 devices.

MMD-040000 [**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 following requirements:

MMD-040010 [**Required: UC_Multifunction_Mobile_App**] The application shall conform to all IO and IA interoperability requirements specified for End Instruments (EIs) or Assured Services Session Initiation Protocol (AS-SIP) EIs (AEIs) if the application implements AS-SIP) in the UCR, with the exception of the following requirements:

NOTE: This includes the capability to support operation on IPv6-enabled MMD platforms and connected networks.

MMD-040020 [**Conditional: UC_Multifunction_Mobile_App**] If the application does not support all codec types specified in Section 2.9, End Instruments, for EIs and AEIs, then this noncompliance is permitted, provided that the application's homed MBSS transcodes appropriately when communicating with the Session Controller (SC) (Softswitch [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.

MMD-040030 [**Conditional: UC_Multifunction_Mobile_App**] When the UC MMD Application connects to its homed SC via the MBSS, it is not required to support the capability to support Multilevel Precedence and Preemption (MLPP) or display the precedence level of calls. However, if it does so, then it must do so in accordance with (IAW) the requirements in Section 2, Session Control Products.

MMD-040040 [Required: UC_Multifunction_Mobile_App] The cryptographic interoperability 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 Transport Layer Security (TLS) and Internet Protocol Security (IPSec) in Section 4, Information Assurance.

MMD-040050 [**Required: UC_Multifunction_Mobile_App**] For VVoIP media traffic, the cryptographic profile shall be equal to or stronger than the profile defined for Secure Real-Time Transport Protocol (SRTP) in Section 4, Information Assurance.

MMD-040060 [**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 SC, then the application and its associated platform shall conform to all requirements applicable to Wireless End Instruments (WEIs) specified in Section 7, Network Edge Infrastructure Requirement.

MMD-040070 [**Conditional: UC_Multifunction_Mobile_App**] Any chat or collaboration capabilities provided by the UC MMD Application shall be IAW UC XMPP 2013.

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

MMD-050000 [**Conditional: MBSS**] If the MBSS provides connectivity to the SC (or SS) on behalf of any served UC MMD Applications, then the product shall conform to the subtended requirements:

MMD-050010 [**Conditional: MBSS**] If the system supports UC MMD applications, unless explicitly stated otherwise by the subtended requirements, on the interface used by the MBSS to communicate with its homed SC or SS, then the MBSS shall act as any other EI or AEI and so comply with all functional and Information Assurance interoperability requirements in this UCR for EIs or AEIs as appropriate.

MMD-050020 [**Conditional: 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 2.9, End Instruments, then the system shall support a transcoding function that securely translates this media traffic into a format compatible with the SC line-side protocol.

MMD-050030 [**Conditional: MBSS**] If the system supports UC MMD applications, then the system shall ensure that VVoIP media, signaling, IM, and any other supported UC traffic originating from the MMD that traverses the MBSS are marked with the appropriate Differentiated Services Code Point (DSCP) value specified in Section 6, Network Infrastructure End-to-End Performance, upon entrance into the enclave UC network.

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

MMD-050040 [**Conditional: MBSS**] If the served UC MMD Applications do not support MLPP, then the MBSS shall interface with its homed SC and use the procedures defined in Section 2, Session Control Products, to handle calls received above the ROUTINE level that cannot be forwarded to the UC MMD Application (e.g., forwarding to an attendant).

MMD-050050 [**Conditional: MBSS**] If the system supports UC MMD applications, then the system shall provide secure connectivity to the served UC MMD applications by, at a minimum, implementing Back-to-Back User Agent (B2BUA) (SBC-like) application layer gateway functionality or alternatively providing Virtual Private Network (VPN) functionality when communicating with served UC MMD Applications.

MMD-050060 [**Conditional: MBSS**] If the system supports UC MMD applications, then 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 Intrusion Detection System (IDS) monitoring requirements in Section 4.2.4, Ancillary Equipment; Section 13, Security Devices; and Section 4.2.9, Confidentiality.

MMD-050070 [**Conditional: MBSS**] If the system supports UC MMD applications, then the product shall support either an onboard VVoIP IDS/Intrusion Prevention System (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.

MMD-050080 [**Conditional: MBSS**] [Alarm] If the system supports UC MMD applications, then the VVoIP IDS/IPS threat detection capabilities shall be IAW the VVoIP IDS/IPS functional requirements specified in Section 13, Security Devices. The product shall support the capability to generate and transmit an alarm to the Network Management System (NMS) when these threats are identified.

MMD-050090 [**Conditional: MBSS**] If the product provides the capability to transmit decrypted media and signaling to an external VVoIP IDS/IPS platform, then 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 4, Information Assurance.

MMD-050100 [**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.