DoD ANNEX
FOR
MOBILE DEVICE MANAGEMENT PROTECTION PROFILE V4.0

Version 1, Release 1

01 May 2019

Developed by DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

REVISION HISTORY

Version	Date	Description
V1R1	1 May 2019	Initial Release
V1R0.1	15 April 2019	Internal DISA draft based on Draft 2 of the MDM PP v4.0

TABLE OF CONTENTS

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Background

This Annex for the Protection Profile (PP) for Mobile Device Management (Version 4.0, dated 25 April 2019) delineates PP content that must be included in the Security Target (ST) for the Target of Evaluation (TOE) to be fully compliant with DoD cybersecurity policies pertaining to information systems. This content includes DoD-mandated PP selections and assignments and PP Security Functional Requirements (SFRs) listed as optional or objective in the PP but mandated in DoD.

Deficiencies of the TOE with respect to the DoD Annex will be reported as appropriate under the Risk Management Framework for DoD Information Technology (DoD Instruction 8510.01). DoD may determine that a TOE that does not conform to this Annex may pose an unacceptable risk to DoD. Accordingly, any vendor seeking authorization for use of its product within DoD should include the additional PP specificity described in this Annex in its ST.

The MDM PP, in conjunction with this Annex, addresses the DoD-required cybersecurity controls in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. Taken together, they supersede the DoD Mobile Device Management Security Requirements Guide.

1.2 Scope

The information in this document is applicable to all DoD-administered systems and all systems connected to DoD networks.

The Mobile Application Store (MAS) Server is an application on a general-purpose platform or on a network device, executing in a trusted network environment. Rather than being deployed as a separate application server, MAS features are usually integrated or embedded in the MDM Server[1]. The MAS server hosts applications for the enterprise, authenticates Agents, and securely transmits applications to enrolled mobile devices.

1.3 Relationship to Security Technical Implementation Guides (STIGs)

A successful Common Criteria evaluation certifies the capabilities of the TOE but does not assure its subsequent secure operation. To address security concerns with the ongoing operation of the TOE in the field, a product-specific STIG is prepared in conjunction with the Common Criteria evaluation. The STIG lists the configuration requirements for DoD implementations of the TOE and is published in Extensible Configuration Checklist Description Format (XCCDF) to facilitate automation where feasible.

[1] Table 3-2 of this document describes which MAS-related DoD-mandated SFRs apply to the use case where the MAS functions are embedded in the MDM server.

This Annex contains the required DoD configuration of features implementing the Security Management (FMT) class of SFRs listed in the PP for MDM. For each applicable FMT SFR, the STIG will discuss the vulnerability associated with non-compliance configuration and provide step-by-step, product-specific procedures for checking for compliant configurations and fixing non-compliant configurations.

In most cases, the ST will not cover all security-relevant configurable parameters available in the TOE. However, the STIG will include these whenever they impact the security posture of DoD information systems and networks. Accordingly, the DoD Annex only addresses a subset of the controls expected to be included in a STIG.

1.4 Document Revisions

Comments or proposed revisions to this document should be sent via email to: disa.stig_spt@mail.mil.

2. CONVENTIONS

The following conventions are used to describe DoD-mandated ST content:

- If a PP SFR is not listed, there is no DoD-mandated selection or assignment for that SFR.
- For SFRs included in this annex:
    - Underlined text indicates a required selection. The presence of the selection indicates this is a DoD-mandated selection.
    - If a selection is not listed, then its inclusion or exclusion does not impact DoD compliance.
    - **Bold** text indicates additional text provided as a refinement to add details to the requirement.
    - *Italicized* text indicates a required assignment.
    - ~~Strikethrough and underlined~~ text indicates that the ST author must exclude the selection.

The Annex provides the minimum text necessary to disambiguate selections and assignments. Readers will need to view both the MDF PP and the DoD Annex simultaneously to place the Annex information in context.

3. DOD-MANDATED SECURITY TARGET CONTENT

3.1 DoD-Mandated Assignments and Selections

DoD mandates the following PP SFR selections and assignments for SFRs in Section 4 of the PP for MDM:

Table 3-1: PP SFR Selections

SFR	Selections, Assignments, and Application Notes
FAU_GEN.1.1(1)	c. Commands issued to the MDM Agent
FIA_ENR_EXT.1.2	specific device models
FIA_X509_EXT.2.1	code signing for system software updates, code signing for integrity verification, policy signing
FIA_X509_EXT.2.2	~~accept the certificate~~
FMT_SMF.1.1(1)	The following commands must be supported: 13, 14, 16, 17, 18, 19, 20, 21, 22, 23 The following MD configuration policies must be supported: 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 44, 47, 48, 49, 50, 51, 52, 53, 54, 55, 57, 58, 59 Assignments and selections within functions: Application note: Selections and assignments are only applicable where the managed MD supports the function. 21. Application note: Data or application sharing between different application processes or groups of application processes (including copy/paste of data) are considered an exception to the access control policy and therefore, the Administrator must be able to disable these features. 29. Specifying authorized application repository(s), specifying a set of allowed applications and versions (an application whitelist) Application note: The application whitelist functionality specified in Function 29 extends to core and pre-installed apps where the MD supports such configuration. The application whitelist must control user access/execution of all core and preinstalled applications or the MD must provide an alternate method of restricting user access/ execution to core and pre-installed applications. Core apps are those bundled with the MD operating system. Pre-installed apps are those that a mobile carrier or device manufacturer may install prior to enterprise use. 32. Assignment: *cellular, Wi-Fi, Bluetooth, NFC*

SFR	Selections, Assignments, and Application Notes
	34. List of protocols where the device acts as a server = protocols supporting wireless remote access Application note: This function is not mandated if there is no native MD support for wireless remote access. Mobile hotspot connections (see function 51) are not considered wireless remote access if the wireless device connected to the MD cannot access the application processor. 40. Email notifications, calendar appointments, contact associated with phone call notification, text message notification Application note: Notifications are permitted where the content of the notification does not contain DoD sensitive information (e.g., a notification that alerts the user that there is an appointment but does not reveal the subject or location of the appointment.) 49. a. USB mass storage mode, USB data transfer without user authentication 50. Application note: Must include the capability to disable backup to cloud based systems. 51. Hotspot functionality authenticated by [selection: pre-shared key, ~~no authentication~~]. USB tethering authenticated by [selection: pre-shared key or passcode or both, ~~no authentication~~] Application note: A managed MD will often support MDM management of security-critical parameters not covered by the MDM PP (e.g., MD features not envisioned at the time of the MDM PP's publication). The STIG associated with the mobile operating system running on the MD will identify which of these management functions are expected to be supported by the MDM. The MDM ST author should review the DoD Annex for the MDFPP and the STIG for supported MDs prior to finalizing the MDM product ST.
FMT_SMF.1.1(2)	Function selection d is required if *TOE platform* is not selected in FTA_TAB.1.1. Selecting *TOE Platform* indicates the host operating system is providing the advisory notice and consent warning message. Assignments and selections within functions: b. *specific device models* c.3. list of commands = 5. *query connectivity status*; 6. *query the current version of the MD firmware/software*; 7. *query the current version of the hardware model of the device*; 8. *query the current version of installed mobile applications*; 19. *read audit logs kept by the MD.*

SFR	Selections, Assignments, and Application Notes
	Application note: The numbered commands listed here are a subset of those listed in FMT_SMF.1.1(1). c.8. other management functions: - *configure server administrator login session timeout* - *configure Enterprise certificate to be used for signing policies (if function is not automatically implemented during MDM server install) (FMT_POL_EXT.1.1)* - *configure MDM Agent/platform to perform a network reachability test (if function is not automatically implemented during MDM server install) (FAU_NET_EXT.1.1)* - *configure transfer of MDM sever logs to another server for storage, analysis, and reporting (FAU_STG_EXT.1.1)* - *configure x509v3 certificates supporting uses detailed in FIA_X509_EXT.2.1(if not configured during server install)*
FMT_SMR.1.1(1)	Assignment: *additional authorized identified roles*[2]: *Server Primary Administrator, Security Configuration Administrator, Device User Group Administrator, Auditor* Application note: - Server Primary Administrator: Responsible for server installation, initial configuration, and maintenance functions. Responsible for the setup and maintenance of Security Configuration Administrator and Auditor accounts. - Security Configuration Administrator: Responsible for security configuration of the server, setup, and maintenance of mobile device security policies, defining device user groups, setup and maintenance of Device User Group Administrator accounts, and defining privileges of Device User Group administrators. - Device User Group Administrator: Responsible for maintenance of mobile device accounts, including setup, change of account configurations, and account deletion. Can only perform administrative functions assigned by the Security Configuration Administrator. -Auditor: Responsible for reviewing and maintaining server and mobile device audit logs.

[2] It is acceptable for these roles to be defined by the host operating system server/platform if MDM server account management is provided by the host server.

3.2 DoD-Mandated Optional, Selection-Based, and Objective Functions

The following SFRs (and associated selections and assignments) listed as optional or objective in the PP are mandated for the DoD:

- FAU_SAR.1.1
- FAU_SAR.1.2
- FTA_TAB.1.1

The following table lists optional and objective SFRs that are mandatory for DoD use cases if the MDM server includes embedded Mobile Application Store (MAS) features.

Table 3-2: DoD-Mandated SFRs for MDM Application Management Use Cases

SFR
FAU_GEN.1.1(2)
FAU_GEN.1.2(2)
FMT_MOF.1.1(3)
FMT_SMF.1.1(3)

Table 3-3 lists DoD-mandated selections and assignments for optional SFRs listed in Appendix A of the MDM PP.

Table 3-3: PP Selections and Assignments for Optional SFRs

SFR/Function	Selections, Assignments, and Application Notes
FTA_TAB.1.1	Application note: Selection of *TOE platform* indicates the host operating system is providing the advisory notice and consent warning message.

4. OTHER DOD MANDATES

4.1 Federal Information Processing Standard (FIPS) 140-2

Cryptographic modules supporting any SFR in the Cryptographic Support (FCS) class must be FIPS140-2 validated. Information concerning FIPS 140-2 validation should be included in the ST. Failure to obtain validation to include applications could preclude use of the TOE within DoD.

4.2 MDM Platform and Server Integration

The MDM Platform and Server are expected to support:

- Use of MDM Platform user accounts and groups for MDM server administrator identification and logical access control
- Authentication of MDM Platform accounts via an enterprise directory service
- Periodic transfer of audit logs to another server

In addition, the MDM Platform and Server may support:

- DoD remote access requirements where the MDM server provides a trusted channel/gateway for MD remote access to enterprise network services

4.3 DoD-Mandated Configuration

Table 4-1 below lists configuration values for product features implementing the PP Specification of Management Functions (FMT_SMF). The ST is not expected to include this configuration information, but it will be included in the product-specific STIG associated with the evaluated IT product.

Table 4-1: Configuration Values

SFR/Function	DoD Selections and Values
FMT_SMF.1.1(1) #19	***Enable*** read audit logs kept by the MD
FMT_SMF.1.1(2) b	***Configure*** specific approved device models
FMT_SMF.1.1(2) c.2	***Configure*** warning banner with required DoD text For devices accommodating advisory warning messages of 1300 characters: *You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.* *By using this IS (which includes any device attached to this IS), you consent to the following conditions:* *- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense,*

SFR/Function	DoD Selections and Values
	personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. *- At any time, the USG may inspect and seize data stored on this IS.* *-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.* *- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.* *- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.* *- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.* For MDM platforms or servers with severe character limitations: *I've read & consent to terms in IS user agreem't.* Application note: As noted above, Function d is not required if *TOE platform* is selected in FTA_TAB.1.1. Regardless of whether the banner is supported by the TOE platform (host server) or the MDM server, the system should be configured to prevent further activity on the information system unless and until the user executes a positive action to manifest agreement to the advisory message.
FMT_SMF.1.1(2) c.3	***Configure*** <u>periodicity of [*6 hours or less*] for the following commands to the agent</u>: *- query connectivity status* *- query the current version of the MD firmware/software* *- query the current version of the hardware model of the device* *- query the current version of installed mobile applications* *- read audit logs kept by the MD*
FMT_SMF.1.1(2) c.8	***Configure*** <u>administrator login session timeout = 15 minutes</u> ***Configure*** <u>Enterprise certificate to be used for signing policies</u> (if function is not automatically implemented during MDM server install) (FMT_POL_EXT.1.1)

SFR/Function	DoD Selections and Values
	Configure MDM Agent/platform to perform a network reachability test (if function is not automatically implemented during MDM server install) (FAU_NET_EXT.1.1) ***Configure*** transfer of MDM sever logs to another server for storage, analysis, and reporting (FAU_STG_EXT.1.1(1)) ***Configure*** x509v3 certificates used by the MDM for supporting code and policy signing *(FIA_X509_EXT.2.1)*
FMT_SMR.1.1(1)	***Configure*** *the following Administrator roles and assign at least one Administrator to each role*: *(a) MD user;* *(b) Server Primary Administrator;* *(c) Security Configuration Administrator;* *(d) Device User Group Administrator;* *(e) Auditor.*
FMT_SMF.1.1(3) c	***Configure*** *the following audit events (if function is not automatically implemented during MDM server install):* *(a) Failure to push a new application on a managed mobile device;* *(b) Failure to update an existing application on a managed mobile device.*