DoD ANNEX
FOR
PROTECTION PROFILE FOR MOBILE DEVICE MANAGEMENT V3.0

Version 1, Release 1

12 January 2017

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	12 January 2017	Initial Release
V1R0.3	12 December 2016	Draft based on Final PP for MDM v3.0
V1R0.2	07 September 2016	Internal DISA draft based on Draft 2 of the PP for MDM v3.0
V1R0.1	04 August 2016	Internal DISA draft based on Draft 1 of the PP for MDM v3.0

TABLE OF CONTENTS

Page

1. INTRODUCTION....................1

1.1 Background....................1
1.2 Scope....................1
1.3 Relationship to Security Technical Implementation Guides (STIGs)....................1
1.4 Document Revisions....................2

2. CONVENTIONS....................3

3. DOD-MANDATED SECURITY TARGET CONTENT....................4

3.1 DoD-Mandated Assignments and Selections....................4
3.2 DoD-Mandated Optional, Selection-Based, and Objective Functions....................8

4. OTHER DOD MANDATES....................10

4.1 Federal Information Processing Standard (FIPS) 140-2....................10
4.2 MDM Platform and Server Integration....................10
4.3 DoD-Mandated Configuration....................10

LIST OF TABLES

Page

Table 3-1: PP SFR Selections 4
Table 3-2: DoD-Mandated SFRs for MDM Application Management Use Cases 8
Table 3-3: PP Selections and Assignments for Optional SFRs 8
Table 4-1: Configuration Values 10
Table 4-2: Configuration Values for MAS 12

1. INTRODUCTION

1.1 Background

This Annex to the Protection Profile (PP) for Mobile Device Management (Version 3.0, dated 21 November 2016) 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 PP for MDM, 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. MAS features may also be integrated or embedded in the MDM Server rather than deployed as a separate application 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 MAS functions are deployed in a separate server from the MDM and 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)	e. other events: - *MDM agent alerts (generated by FAU_ALT_EXT.2.1 in the MDM Agent EP)* - *MDM Agent audit records (generated by FAU_GEN.1.1(2) in the MDM Agent EP)* - *MD audit records (read by the MDM Agent via FMT_SMF.1.1(1) #19)*
FAU_STG_EXT.1.1(1)	Application note: Audit data includes MDM agent alerts, MDM agent audit records, and MD audit records.
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, 24 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 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 enable/disable these features. 24. assignment: *list of other management functions to be provided by the MD*:

SFR	Selections, Assignments, and Application Notes
	a. *enable/disable automatic transfer of diagnostic data to an external device or service other than an MDM service with which the device is enrolled*[2] b. *enable/disable multi-user modes (if feature supported by MD)* c. *enable/disable automatic updates of system software* d. *wipe non-enterprise data* e. *enable/disable VPN split-tunneling (if the MD provides a configurable control for FDP_IFC_EXT.1.1)* f. *enable/disable use of removable media* *g. configure implementation of the access control policy specified in FDP_ACF_EXT.1.2* h. *configure actions available to users before user is authenticated: enable/disable access to the user's contact, calendar, messaging databases, or camera, (FIA_UAU_EXT.2.1)* 29. a. specifying authorized application repository(s), b. specifying a set of allowed applications and versions (an application whitelist) Application note: 29c may be selected in lieu of 29a and 29b if the use case does not involve user-selection of applications. 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 distributor may install prior to enterprise use. 32. assignment: *cellular, Bluetooth, NFC* 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. a. email notifications, b. calendar appointments, c. contact associated with phone call notification, d. text message notification, e. other application-based notifications, f. none.

[2] Diagnostic data is defined as MD audit logs read by the MDM agent (see function 19) and any other MD status information collected by the MDM Agent.

SFR	Selections, Assignments, and Application Notes
	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. locally connected system, remote system. Application note: Remote systems include cloud based systems. 51. a. Hotspot functionality authenticated by [selection: pre-shared key, ~~no authentication~~]. b. 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 selections: d and e are required. Application note: Function d is not required if *TOE platform* is selected in FTA_TAB.1.1, indicating the host operating system is providing the advisory notice and consent warning message. Assignments and selections within functions: b. *specific device models* b. other features: - *configure server session lock timeout* - *initiate session lock when timeout occurs* - *configure timeout for network connection associated with a communications session at the end of any transaction with an MDM agent or other server* - *terminate network connection when timeout occurs for network connection associated with a communications session with an MDM agent or other server* - *configure Enterprise certificate to be used for signing policies (if function is not automatically implemented during MDM server install) (FMT_POL_EXT.1.1)*

SFR	Selections, Assignments, and Application Notes
	- *configure audit record generation of DoD required auditable events (if function is not automatically implemented during MDM server install) (FAU_GEN.1.1(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(1))* - *configure x509v3 certificates supporting uses detailed in FIA_X509_EXT.2.1(if not configured during server install)* e. 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.* Application note: The numbered commands listed here are a subset of those listed in FMT_SMF.1.1(1).
FMT_SMR.1.1(1)	Assignment: *additional authorized identified roles*[3]: *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.

[3] 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
- FPT_ITT.1.1
- 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 or the MDM system includes a separate MAS server.

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

SFR	MAS functions are embedded in MDM server	MDM system consists of a separate MAS server
FAU_GEN.1.1(2)	√	√
FAU_GEN.1.2(2)		√
FAU_STG_EXT.1.1(2)		√
FMT_MOF.1.1(3)	√	√
FMT_MOF.1.1(4)	√	√
FMT_SMF.1.1(3)	√	√
FMT_SMR.1.1(2)		√
FMT_SMR.1.2(2)		√
FTP_ITC.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
FMT_SMR.1.1(2)	Additional authorized identified roles: *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

SFR/Function	Selections, Assignments, and Application Notes
	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.
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. While information concerning FIPS 140-2 validation should not be included in the ST, failure to obtain validation 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*** *session lock timeout* = 15 minutes ***Configure*** *timeout for network connection with MDM agent or other server* = 10 minutes ***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*** *audit record generation of DoD required auditable events* (if function is not automatically implemented during MDM server install) (FAU_GEN.1.1(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** DoD required device enrollment restrictions allowed for enrollment* [*specific device model*] (if function is not automatically implemented during MDM server install) (FIA_ENR_EXT.1.2) ***Configure** x509v3 certificates used by the MDM for supporting code and policy signing (FIA_X509_EXT.2.1)*
FMT_SMF.1.1(2) d	b. ***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, 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:

SFR/Function	DoD Selections and Values
	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) e	***Configure*** periodicity of [*6 hours or less*] for the following commands to the agent: - *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_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.

Table 4-2 lists configuration values for MAS-related product features implementing the PP Specification of Management Functions (FMT_SMF).

Table 4-2: Configuration Values for MAS

SFR/Function	DoD Selections and Values
FMT_SMF.1.1(3) c.	***Configure*** *approved application access/user groups* (FMT_MOF.1.1(3) ***Enable*** *audit record generation of DoD required auditable events* (if function is not automatically implemented during MDM/MAS server install) (FAU_GEN.1.1(2)): a. *Failure to push a new application on a managed mobile device;* *b. Failure to update an existing application on a managed mobile device.* ***Configure*** *transfer of MAS sever logs to another server for storage, analysis, and reporting* (FAU_STG_EXT.1.1(2)) ***Configure*** *the following Administrator roles and assign at least one Administrator to each role* (FMT_SMR.1.1(2)):

SFR/Function	DoD Selections and Values

	(a) Server Primary Administrator;
	(b) Security Configuration Administrator;
	(c) Device User Group Administrator;
	(d) Auditor.