DoD ANNEX
FOR
PROTECTION PROFILE FOR MOBILE DEVICE MANAGEMENT V2.0

Version 1, Release 3

28 October 2016

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
1.1	29 Apr 2014	Initial Release
1.2	20 July 2015	Updated table 2-1: - added function 53(d) and associated Application note to FMT_SMF.1.1(1) Refinement Updated table 3-1: - added application note at end of table
1.3	28 October 2016	- Updated notation conventions - Updated content of Table 2-1 (FAU_GEN.1.1(1) Refinement, FMT_SMF.1.1(1) Refinement, and FMT_SMF.1.1(2) Refinement) - Added Tables 2-2, 2-3, and 3-2 to the document - Updated content of Table 3-1 (FMT_SMF.1.1(1) Refinement and FMT_SMF.1.1(2) Refinement)

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Background

This Annex to the Protection Profile (PP) for Mobile Device Management (Version 2.0, dated 31 December 2014) 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 which are 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 additional 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. The MAS Server may be separate to or included in the MDM Server. 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.

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. DOD-MANDATED SECURITY TARGET CONTENT

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.
  - *Italicized* text indicates a required assignment within a selection.
  - ~~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 PP for MDM and the DoD Annex simultaneously to place the Annex information in context.

2.1 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 2-1: PP SFR Selections

SFR	Selections, Assignments, and Application Notes
FAU_GEN.1.1(1) Refinement	f. 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))* *- MD audit records (read by the MDM Agent via FMT_SMF.1.1(1) Refinement #19)*
FMT_SMF.1.1(1) Refinement	Function selections: 14, 19, 22, 33, 34, 35, 36, 37, 39, 46, 48, 49, 50, 51, 53 Application note: Selections are only applicable where the managed MD supports the function. On 53, to the extent that the STIG requires a certain management function, it must list the case here. Assignments and selections within functions: 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

SFR	Selections, Assignments, and Application Notes
	policy and therefore, the Administrator must be able to enable/disable these features. 28. a. specifying authorized application repository(s), b. specifying a set of allowed applications and versions (an application whitelist). Application note: 28c may be selected in lieu of 28a and 28b if the use case does not involve user-selection of applications. Application note: The application whitelist functionality specified in Function 28 extends to core and pre-installed apps where the MD supports such configuration. 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. 33. List of protocols where the device acts as a server = *protocols supporting remote access*. 39. a. email notifications, b. calendar appointments, c. contact associated with phone call notification, d. text message notification, e. other application-based notifications. 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. locally connected system, remote system. 50. a. Hotspot functionality authenticated by [selection: pre-shared key, ~~no authentication~~]. b. USB tethering authenticated by [selection: pre-shared key, passcode, ~~no authentication~~] 53. list of other policies to be provided by the MD = 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* 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 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 other DoD-sensitive information (FIA_UAU_EXT.2.1)*

SFR	Selections, Assignments, and Application Notes
	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. Application note for 53(d): The MDM is expected to support implementation of all functions depending on how the MD implements the function as described in the MD ST: some management functions may apply to the full MD, to one or more application processing groups supported by the MD, or both.
FMT_SMF.1.1(2) Refinement	Function selections: d, e and f. Application note: Function d is not required if *MDM server platform* is selected in FTA_TAB.1.1. Assignments and selections within functions: b. specific devices 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) Refinement. f. additional functions required to support SFRs: *- 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 DoD required Administrator roles defined in FMT_SMR.1.1(1)* *- 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) Refinement)* *- configure MDM Agent/platform to perform a network reachability*

SFR	Selections, Assignments, and Application Notes
	test (if function is not automatically implemented during MDM server install) (FAU_NET_EXT.1.1) *- transfer of MDM sever logs to another server for storage, analysis, and reporting (FAU_STG_EXT.1.1(1))* Application note: The MDM server is not required to transfer MD audit logs to another server if the MDM Platform provides this functionality.
FMT_SMR.1.1(1) Refinement	*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, setting up 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.

2.2 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.1.1Refinement
- FAU_STG_EXT.2.1
- FMT_POL_EXT.1.1
- FPT_ITT.1.1(1) Refinement
- FTA_TAB.1.1

The following table lists optional and objective SFRs that are mandatory if the MDM server supports application management functions or the MDM system includes a separate MDM server.

Table 2-2: DoD-Mandated SFRs for MDM Application Management

SFR	MDM server supports MD application management functions	MDM system consists of a separate Mobile Application Store (MAS) server
FAU_GEN.1.1(2) Refinement	√	√
FAU_GEN.1.2(2) Refinement		√
FAU_STG_EXT.1.1(2)		√
FMT_MOF.1.1(3) Refinement	√	√
FMT_MOF.1.1(4) Refinement	√	√
FMT_SMF.1.1(3) Refinement	√	√
FMT_SMR.1.1(2)		√
FMT_SMR.1.2(2)		√
FPT_ITT.1.1(2) Refinement		√
FPT_ITT.1.1(3) Refinement		√
FTP_ITC.1.1(3) Refinement		√

Table 2-3 lists DoD-mandated selections and assignments for Appendix B of the MDM PP.

Table 2-3: PP Selections and Assignments for Optional SFRs

SFR	Selections, Assignments, and Application Notes
FMT_SMR.1.1(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. Responsible for the maintenance of applications in the MAS. -Security configuration administrator: responsible for security configuration of the server, 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. Responsible for defining which apps user groups or individual users have access to in the MAS. Can only perform administrative functions assigned by the Security configuration administrator.

SFR	Selections, Assignments, and Application Notes
	-Auditor: responsible for reviewing and maintaining server and mobile device audit logs.

3. OTHER DOD MANDATES

3.1 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.

3.2 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 user identification and logical access control
- Authentication of MDM Platform accounts via an enterprise directory service
- Periodic transfer of audit logs to another server
- DoD remote access requirements where the MDM server also provides a gateway for MD remote access to enterprise network services

3.3 DoD-Mandated Configuration

The table 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. Non-binary configuration values are shown in *italics*.

Table 3-1: Configuration Values

SFR/Function	DoD Selections and Values
FMT_SMF.1.1(1) Refinement #19	***Enable*** read audit logs kept by the MD
FMT_SMF.1.1(2) Refinement b	***Enable*** audit record generation of DoD required auditable events (if function is not automatically implemented during MDM server install) (FAU_GEN.1.1(1) Refinement) ***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)

SFR/Function	DoD Selections and Values
	Configure session lock timeout = *15 minutes* ***Configure*** session to lock when session lock timeout occurs ***Configure*** timeout for network connection with MDM agent or other server = *10 minutes* ***Configure*** network connection to terminate when timeout occurs for network connection associated with a communications session with an MDM agent or other server ***Configure*** the following Administrator roles and assign at least one Administrator with each role (FMT_SMR.1.1(1) Refinement): *(a) MD user;* *(b) Server primary administrator;* *(c) Security configuration administrator;* *(d) Device user group administrator;* *(e) Auditor.* ***Configure*** Enterprise certificate to be used for signing policies (if function is not automatically implemented during MDM server install) (FMT_POL_EXT.1.1)
FMT_SMF.1.1(2) Refinement d	***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.*

SFR/Function	DoD Selections and Values
	-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 *MDM server platform* is selected in FTA_TAB.1.1. Regardless of whether the banner is supported by MDM platform or 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. An image with the required banner text is an acceptable method for implementing this requirement. Application note: When a MD cannot support the display of a banner message (for example, if there is no API for this function), an alternative approach that should be considered would be to configure the MDM server to send the banner message periodically to the MD via an alert message, if this capability is available.
FMT_SMF.1.1(2) Refinement 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

Table 3-2 lists configuration values for MAS-related product features implementing the PP Specification of Management Functions (FMT_SMF).

Table 3-2: Configuration Values for MAS

SFR/Function	DoD Selections and Values
FMT_SMF.1.1(3)	***Configure*** approved application access groups ***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) Refinement):

SFR/Function	DoD Selections and Values
	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 with each role (FMT_SMR.1.1(2) Refinement): *(a) MD user;* *(b) Server primary administrator;* *(c) Security configuration administrator;* *(d) Device user group administrator;* *(e) Auditor.*