DoD ANNEX
FOR
MOBILE DEVICE FUNDAMENTALS (MDF)
PROTECTION PROFILE (PP) V3.0

Version 1, Release 1

20 July 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	20 July 2016	Initial Release

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Background

This Draft Annex to the Protection Profile (PP) for the Final Draft Mobile Device Fundamentals (Version 3.0, dated 10 June 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 that 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 MDF 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 Operating System 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.

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 MDF PP. 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[1]. 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.

[1] For example, if the mobile operating system provides an exception to the data sharing restrictions found in FDP_ACF_EXT.1.2, a configuration setting should be included in the STIG to disable this feature.

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:
    - *Italicized* text indicates a required selection. The presence of the selection indicates this is a DoD-mandated selection.
    - If a selection is not listed, its inclusion or exclusion does not impact DoD compliance.
    - Underlined text indicates additional text provided as a refinement.
    - ***Italicized and bold*** text indicates a required assignment within a selection.
    - ~~*Strikethrough and Italicized*~~ text indicates 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 Selections and Assignments

DoD mandates the following PP SFR selections and assignments for SFRs in Section 5 of the MDF PP:

Table 3-1: PP SFR Selections

SFR	Selections, Assignments, and Application Notes
FAU_GEN.1.1	6. Specifically defined auditable event in Table 1: • FPT_TST_EXT.2, *Detected integrity violation* Application note: Requirement applies only to integrity violation detections that can be logged by the audit logging component. 8. *Specifically defined auditable event in Table 2,* • FIA_AFL_EXT.1 • FIA_UAU.6 • FMT_SMF_EXT.2, *Initiation of unenrollment* • FPT_TUD_EXT.2
FCS_STG_EXT.1.4	~~*the user*~~
FDP_ACF_EXT.1.2	~~*the user*~~ Application note: The TSF is required to support the following two application process groups: Work (or Enterprise) and Personal (or BYOD). In the majority of DoD use cases the MD will be DoD owned and both application process groups will be enabled.
FIA_UAU.5.1	*biometric fingerprint, hybrid* (if supported by the TSF)
FIA_UAU_EXT.2.1	*list of actions =* ~~*any action that enables access to the user's contact, calendar, messaging databases or other DoD sensitive information.*~~ Application note: Examples of actions that enable access to DoD sensitive information include, but are not limited to, voice dialing of stored contacts and voice-enabled personal assistant applications that allow queries for locally stored information.
FIA_X509_EXT.2.1	*code signing for system software updates, code signing for mobile applications, code signing for integrity verification* Application note: If management function is not supported by an operating system, appropriate mitigations should be provided.
FIA_X509_EXT.2.2	*allow the user to choose whether to accept the certificate in these cases,* ~~*accept the certificate*~~
FMT_MOF_EXT.1.2	See Table 3-2
FMT_SMF_EXT.1.1	See Table 3-2
FMT_SMF_EXT.2.1	Include one of the following selections: -*wipe of protected data* -*wipe of sensitive data* (provided that the ST author has identified sensitive data in a manner to include all Enterprise applications and resident Enterprise application data, all data associated with enterprise email, calendar and contact information, and all other local data storage accessible to Enterprise applications and email, calendar,

SFR	Selections, Assignments, and Application Notes
	and contact applications. Include one of the following selections: *-remove Enterprise applications* *-remove all non-core applications* (any non-factory-installed application) Application note: The selection *alerts the administrator* and assignments for the *list of other available remediation actions* may be included as a supplement to, but not in lieu of, one of the required selections above.

Table 3-2: Management Functions (Table 4 of MDF PP)

Management Function **Status Markers:** M – Mandatory O – Optional/Objective Red highlighted text – deviations from Table 4 in the MDF PP	**FMT_SMF_EXT.1**	**FMT_MOF_EXT.1.1**	**Administrator**	**FMT_MOF_EXT.1.2**
3. enable/disable VPN protection	M	O	M	O
4. list of all radios: Wi-Fi, Bluetooth, NFC (if the radio is supported by the MD, it must be included by the ST author)]	M	O	M	M
8. a. *restricting the sources of applications,* b. *specifying a set of allowed applications based on [assignment:* ***application characteristics****] (an application whitelist),* (See application note below)	M	-	M	M
18. h. *enable/disable all Bluetooth profiles except for HSP (Headset Profile), HFP (HandsFree Profile), and SPP (Serial Port Profile)*	M	O	M	M
19. (See application note below)	M	O	M	M
20. enable data at rest protection	M	O	M	M
21. enable removable media's data at rest protection	M	O	M	M
22. enable/disable location services	M	O	M	M
23. *Biometric Fingerprint, Hybrid Authentication Factor* (if supported by the TSF)	M	O	M	M
24. enable/disable all data signaling over [assignment: ***list of externally accessible hardware ports***]	M	O	M	M
25. (See application note below)	M	O	M	M
26. enable/disable developer modes	M	O	M	M
27. enable/disable bypass of local user authentication	M	O	M	M
28. wipe Enterprise data	M	O	M	-
29. read audit logs kept by the TSF (See application note below)	M	O	M	-
30. configure [selection: certificate, public-key] used to validate digital signature on applications	M	O	M	M
36. configure unlock banner	M	O	M	M
37. configurable the auditable items	M	O	M	M

Management Function **Status Markers:** M – Mandatory O – Optional/Objective Red highlighted text – deviations from Table 4 in the MDF PP	**FMT_SMF_EXT.1**	**FMT_MOF_EXT.1.1**	**Administrator**	**FMT_MOF_EXT.1.2**
39. a. USB mass storage mode	M	O	M	M
40. enable/disable backup of *all applications* to *locally connected system, remote system*	M	O	M	M
41. a. *Hotspot functionality authenticated by [selection: pre-shared key, ~~passcode~~, ~~no authentication~~],* *b. USB tethering authenticated by [selection: pre-shared key, passcode, ~~no authentication~~]*] (See application note below)	M	O	M	M
42. (See application note below)	M	O	M	M
43. place applications into application groups based on [assignment: ***enterprise configuration settings***]	M	O	M	M
44. (See application note below)	M	O	M	O
45. Enable/disable the Always On VPN protection	M	O	M	M
46. Revoke Biometric template (if biometric authentication is supported by the MD)	M	O	M	O
47. [assignment: 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 (see function 15)* *d. wipe non-enterprise data (See application note below)* *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(access control policy that prevents application control processes from accessing data of other application control processes)* *h. configure administrator-configured triggers for FMT_SMF_EXT.2.1 (if administrator-configured triggers are supported by the TSF)* *i. configure actions available to users before user is authenticated: disable access to the user's contact, calendar, messaging databases, or other DoD-sensitive information (FIA_UAU_EXT.2.1)*	M	O	M	M
Application Notes: 8. The application whitelist, in addition to controlling the installation of applications on the MD, 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 application – any application integrated into the operating system (OS) by the OS or mobile device (MD) vendors. Pre-installed application – additional non-core applications included in the OS build by the OS vendor, MD vendor, or wireless carrier. 19. The ST author must select "*f. all notifications*" if there is no other means to administratively restrict applications from issuing notifications in the locked state where those notifications could include DoD sensitive information. If it is possible to administratively restrict notifications on a per-app basis, then it is permissible to allow				

Management Function **Status Markers:** M – Mandatory O – Optional/Objective Red highlighted text – deviations from Table 4 in the MDF PP	FMT_SMF_EXT.1	FMT_MOF_EXT.1.1	Administrator	FMT_MOF_EXT.1.2
notifications from applications that do not handle DoD sensitive information. In this case, the ST author must select: a. email notifications, b. calendar appointments, c. contact associated with phone call notification, d. text message notification. 25. *list of protocols where the device acts as a server* = Protocols supporting wireless remote access. This function is not mandated if there is no native MD support for wireless remote access. Mobile hotspot connections (see function 41) are not considered wireless remote access if the wireless device connected to the MD cannot access the application processor. 32. It is acceptable for the audit logs to be read remotely by the MDM. 40. Remote systems include cloud based systems. 41. If MD supports hotspot feature, selection a. must be included by the ST author. If MD supports USB tethering, selection b. must be included by the ST author. For hotspot functionality, pre-shared keys derived from passcodes are acceptable; simple password authentication is not. If the TOE forces use of a single compliant sub-selection for a or b (i.e., it does not allow configuration of this parameter), then the ST author does not need to specify management functionality for that feature. 42. 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. 44. An acceptable alternative to restricting a user's ability to disenroll an MD in management is for the MD to automatically perform a wipe of protected data upon disenrollment. Application note: The ST author will designate in the ST which functions in Table 4 of the MDF PP are supported for the full device, Work environment/profile/group, and the Personal environment/profile/group. The following functions must be supported for the Personal environment/profile/group: 17, 20, 21, 47d.				

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

The following Security Functional Requirements (and associated selections and assignments) listed as objective in the PP are mandated for the DoD:

- FAU_SAR.1.1
- FIA_BLT_EXT.1.2: For untrusted remote devices, *list of Bluetooth profiles* = <u>all available Bluetooth profiles</u>.
- FIA_BMG_EXT.2.1 - <u>if TSF supports fingerprint biometric authentication</u>

- FIA_BMG_EXT.3.1 - if TSF supports fingerprint biometric authentication
- FIA_BMG_EXT.4.1 - if TSF supports fingerprint biometric authentication
- FIA_BMG_EXT.5.1 - if TSF supports fingerprint biometric authentication
- FIA_BMG_EXT.6.1 - if TSF supports fingerprint biometric authentication
- FPT_AEX_EXT.2.2
- FPT_BBD_EXT.1.1
- FPT_TST_EXT.2.2 (A selection-based requirement driven by the use of certificates for integrity verification in FIA_X509_EXT.2.1)
- FPT_TUD_EXT.2.5 Application note: If the requirement is not supported by an operating system, appropriate mitigations should be provided.
- FPT_TUD_EXT.2.7
- FTA_TAB.1.1
- FTP_BLT_EXT.2.1

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 to include applications could preclude use of the TOE within DoD.

4.2 Federal Information Processing Standard (FIPS) 201-2

The TOE is expected to interface with FIPS 201-2 compliant credentials (to include derived credentials as described in NIST Special Publication 800-157). The TOE may connect to a peripheral device (e.g., a smart card reader) in order to interface with PIV credentials, or natively store derived credentials (whose protections are evaluated in the Protection Profile).

4.3 Core and Carrier-Installed Applications on Mobile Devices

Core and vendor-installed applications are expected to go through an authorized DoD mobile application vetting process to identify the risk of their use and compensating controls. These applications are subject to the application installation policy of Function 8b in FMF_MOF_EXT.1.2 and FMF_SMF_EXT.1.1 regardless of the fact that they were not installed by the user of the device.

4.4 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.

Table 4-1: Configuration Values

FMT_SMF_EXT.1 Function	DoD Selections and Values
Function 1	minimum password length = ***6 characters*** minimum password complexity = ***the password must not contain more than two sequential or repeating characters*** (e.g., the sequences 111, 234, 765, nnn, xyz, cba placed anywhere within the password would violate the complexity rule). No maximum password lifetime is required. Application note: The MDF PP does not provide selections for password complexity. Therefore, the DoD-mandated complexity rule described above is not included in the MDF PP. Vendors must either provide the capability to support this rule or justify why an alternative

FMT_SMF_EXT.1 Function	DoD Selections and Values
	supported complexity scheme offers equivalent or stronger protection against the vulnerability of easily guessed or simple passwords.
Function 2	screen lock ***enabled*** screen lock timeout = ***15 minutes or less*** number of authentication failures = ***10 or fewer***
Function 3	***Enable***
Function 4	***Disable*** NFC
Function 8	Sources of applications = *list of* ***DoD-approved commercial app repository, MDM server, or mobile application store*** Application whitelist *application characteristics* = ***list of digital signatures, cryptographic hash values, or names and versions*** Applications with the following characteristics may not be placed on the application whitelist: ***-backup MD data to non-DoD cloud servers (including user and application access to cloud backup services),*** ***-transmit MD diagnostic data to non-DoD servers,*** ***-voice assistant application if available when MD is locked,*** ***-voice dialing application if available when MD is locked,*** ***-allows synchronization of data or applications between devices associated with user,*** ***-payment processing,*** ***-allows unencrypted (or encrypted but not FIPS 140-2 validated) data sharing with other MDs or printers.***
Function 18	***Disable*** all Bluetooth profiles except for HSP (Headset Profile), HFP (HandsFree Profile), and SPP (Serial Port Profile)
Function 19	***Disable*** all notifications (unless implementation follows per app approach discussed in Application note for Function 19 in Table 3-2)
Function 20	***Enable***
Function 21	***Enable (or disable removable media use if encryption is not available)***
Function 23	***Disable*** (if biometric fingerprint or hybrid authentication factor are supported by the TSF but FIA_BMG SFRs are not included in the ST)
Function 25	***Disable protocols supporting wireless remote access***. Application note: A mobile device providing personal hotspot functionality is not considered supporting wireless remote access if the functionality only provides access to a distribution network (such as a mobile carrier's cellular data network) and does not provide access to the application processor.
Function 26	***Disable***
Function 27	***Disable***
Function 33	certificate = ***DoD approved certificate(s),*** public key = ***DoD approved public key(s)*** Application note: To the extent this parameter is configurable, it must be populated with DoD-approved certificates or public keys. There is

FMT_SMF_EXT.1 Function	DoD Selections and Values
	no requirement that it be configurable; such certificates or public-keys may be pre-populated with the operating system software.
Function 36	***Configure***: 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 mobile devices with severe character limitations: *I've read & consent to terms in IS user agreem't.* Application note: To the extent permitted by the operating system, 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.
Function 37	***Configure***: Auditable event in Table 1: • FPT_TST_EXT.2, Detected integrity violation

FMT_SMF_EXT.1 Function	DoD Selections and Values
	Application note: Requirement applies only to integrity violation detections that can be logged by the audit logging component. Auditable events in Table 2, • FIA_AFL_EXT.1 • FIA_UAU.6 • FMT_SMF_EXT.2, Initiation of unenrollment • FPT_TUD_EXT.2
Function 39	***Disable*** USB mass storage mode
Function 40	***Disable*** backup to locally connected system ***Disable*** backup to remote system
Function 41	***Enable*** Hotspot functionality authenticated by *preshared key* ***Enable*** USB tethering authentication Application note: if hotspot functionality permitted, it must be authenticated via preshared key. If USB tethering is permitted, the connection must be authenticated. There is no requirement to enable hotspot functionality or USB tethering.
Function 42	***Disable***
Function 47	***Disable*** automatic transfer of diagnostic data to an external device other than an MDM service with which the device is enrolled ***Disable*** multi-user modes (if feature supported by MD) ***Disable*** automatic updates of system software ***Disable*** VPN split-tunneling (if the MD provides a configurable control for FDP_IFC_EXT.1.1). ***Configure*** implementation of FDP_ACF_EXT.1.2 ***Configure*** administrator-configured triggers for FMT_SMF_EXT.2.1 (if supported by the TSF) ***Configure*** actions available to users before user is authenticated: disable access to the user's contact, calendar, messaging databases, or other DoD-sensitive information (FIA_UAU_EXT.2.1)