DoD ANNEX
FOR
MOBILE DEVICE FUNDAMENTALS (MDF)
PROTECTION PROFILE (PP) V2.0

Version 1, Release 4

22 April 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	8 Nov 2014	Initial Release
1.2	8 Apr 2015	Updated email address in section 1.4 Updated format conventions in Section 2. Updated table 2-1: -added FCS_STG_EXT.1.4 -added application note for FMT_SMF_EXT.1.1 #10 -added selections c-f for FMT_SMF_EXT.1.1 #45 -added FIA_X509_EXT.1.1 Updated table 3-1: -added list of prohibited application types for function #10 -added function #20 -added DoD values for 5 selections for function #45 Updated section 3-1: - added “to include applications” after validation
1.3	6 July 2015	Updated table 2-1: -added Application note for FDP_ACF_EXT.1.2 -added Application note for FMT_SMF_EXT.1.1 -added new selections for FMT_SMF_EXT.2.1
1.4	22 April 2016	Updated table 2-1: -added FIA_X509_EXT.2.1 and FIA_X509_EXT.2.2

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

2.1 DoD-Mandated Selections and Assignments....3
2.2 DoD-Mandated Selection-Based and Objective Functions....6

3. OTHER DOD MANDATES....7

3.1 Federal Information Processing Standard (FIPS) 140-2....7
3.2 Federal Information Processing Standard (FIPS) 201-2....7
3.3 Core and Carrier-installed Applications on Mobile Devices....7
3.4 DoD-Mandated Configuration....7

LIST OF TABLES

Page

Table 2-1: PP SFR Selections 3
Table 3-1: Configuration Values 7

1. INTRODUCTION

1.1 Background

This Annex to the Protection Profile (PP) for Mobile Device Fundamentals (Version 2.0, dated 17 September 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 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 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. 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 PP selections:
  - 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.
  - Underlined text indicates a selection.
  - *Italicized and underlined* text indicates an assignment within a selection.
  - ~~Strikethrough~~ text indicates that the ST author must either (a) exclude the selection, or (b) select both FMT_SMF_EXT.1 and FMT_MOF_EXT.1.2 for an assignment to MDF PP Table 1 Function 45 that enables an administrator to disable the functionality.
- For PP assignments:
  - The DoD-mandated assignments are listed after the assignment parameter.
  - If an assignment value appears in ~~strikethrough~~ text, this indicates that the assignment must not include this value.
  - *Italicized* text indicates an assignment.

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.

2.1 DoD-Mandated Selections and Assignments

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

Table 2-1: PP SFR Selections

SFR	Selections, Assignments, and Application Notes
FCS_STG_EXT.1.4	~~the user~~
FDP_ACF_EXT.1.2	~~the user~~ Application note: The MD 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 with both application process groups will be enabled.
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.

SFR	Selections, Assignments, and Application Notes
FIA_X509_EXT.1.1	The Online Certificate Status Protocol (OCSP) as specified in RFC 2560
FIA_X509_EXT.2.1	*code signing for system software updates, code signing for mobile applications, code signing for integrity verification*
FIA_X509_EXT.2.2	~~*accept the certificate*~~
FMT_MOF_EXT.1.2	Functions marked "O" in Table 1 that must be selected (with function selection and assignment detail provided in FMT_SMF_EXT.1 below.): 21, 23, 24, 25, 26, 27, 28, 33, 34, 36, 37, 39, 40, 42, 44, 45. Application note: For functions 21, 23 and 44, it is permissible for the user to have the capability to enable a more restrictive setting than the one configured the administrator. For function 28, the administrator must have access to this function, but it is permissible for the user to also have access to it. Function 42 must be selected only if it also selected under FMT_SMF_EXT.1 (i.e., if data-sharing exceptions are permitted, an administrator must approve them). The selection of Function 45 pertains to each of the DoD-required other management functions listed in the assignment for Function 45 in FMT_SMF_EXT.1.
FMT_SMF_EXT.1.1	Selections for mandatory functions in Table 1: 10. a. restricting the sources of application, b. specifying a set of allowed applications based on [assignment: application characteristics = digital signature or cryptographic hash or app name and version] (an application whitelist), Application note: Both *a* and *b* must be selected. Application note: The application whitelist, in addition to controlling the installation of applications on the MD, must control user access/execution of all core applications (included in the operating system (OS) by the OS vendor) and preinstalled applications (provided by the MD vendor and wireless carrier), or the MD must provide an alternate method of restricting user access/execution to core and pre-installed applications. 21. f. all notifications Application note: 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 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. Functions marked "O" in Table 1 that must be selected:

SFR	Selections, Assignments, and Application Notes
	23, 24, 25, 26, 27, 28, 32, 33, 36, 39, 40, 41 Selections and assignments for DoD-mandatory functions marked "O" in Table 1: 23. *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 mobile device support for wireless remote access and 41 is selected for devices that can serve as a personal hotspot. 39. USB mass storage mode 40. locally connected system, remote system 41. a. pre-shared key, ~~passcode~~, ~~no authentication~~, b. ~~no authentication~~ Application note: 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. 44. across device 45. *list of other management functions to be provided by the TSF =* *(a) enable/disable automatic transfer of diagnostic data to an external device or service other than an MDM service with which the device has enrolled;* *(b) enable/disable authentication mechanisms providing user access to protected data other than a Password Authentication Factor (e.g., using a fingerprint).* *(c) disenroll the TOE in management* Application note: An acceptable alternative to restricting a user's ability to disenroll an MD in management is for the MD to perform a wipe of protected data upon disenrollment. *(d) enable/disable multi-user modes* *(e) enable/disable automatic updates of system software (see function 17)* *(f) enable/disable access control policy (for FDP_ACF_EXT.1.2)* *(g) wipe non-enterprise data* Application note: The ST will designate which functions are supported for the full device, Work environment/profile/group, and Personal environment/profile/group. The following functions must be supported for the Personal environment/profile/group: 16, 25, 26, 45(g).
FMT_SMF_EXT.2.1	wipe of protected data OR wipe of sensitive data (provided that the ST author has identified

SFR	Selections, Assignments, and Application Notes
	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 Enterprise applications and email, calendar and contact applications. Alternatively, the ST author may include the selection assignment for *list of other remediation actions* provided below for "remove Enterprise applications" OR remove Enterprise applications (provided that is it is accompanied by the selection assignment *list other remediation actions* = wipe data associated with Enterprise applications, wipe data associated with enterprise email, calendar and contact information, wipe local data storage accessible from Enterprise applications) OR remove all non-core applications (any non-factory installed application) OR wipe all user data. Application note: The selection alerts the administrator, and additional assignments for the list of other available remediation actions may be included as a supplement to, but not in lieu of, one of the selections above.

2.2 DoD-Mandated Selection-Based 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_GEN.1.1: *Audit records reaching [assignment: integer value less than 100] percentage of audit capacity*
- FAU_GEN.1.2
- FAU_SAR.1.1
- FAU_STG.1.1
- FAU_STG.1.2
- FAU_STG.4.1
- FIA_BLT_EXT.1.2: For untrusted remote devices, *list of Bluetooth profiles* = all available Bluetooth profiles.
- FIA_BLT_EXT.2.1
- 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
- FTA_TAB.1.1

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

3.2 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).

3.3 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 10b in FMF_MOF_EXT.1.2 and FMF_SMF_EXT.1 regardless of the fact that they were not installed by the user of the device.

3.4 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. Non-binary configuration values are shown in *italics*.

Table 3-1: 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 supported complexity scheme offers equivalent or stronger protection

FMT_SMF_EXT.1 Function	DoD Selections and Values
	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 10	Sources of applications = *DoD-approved commercial app repository, MDM server, or mobile application store*. Application whitelist = *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, display screens (screen mirroring), or printers.
Function 20	Disable all Bluetooth profiles except for HSP (Headset Profile), HFP (HandsFree Profile), and SPP (Serial Port Profile)
Function 21	Disable *all notifications* (unless implementation follows per app approach discussed in Section 2.1)
Function 23	Disable *protocols supporting wireless remote access*. Application note: A mobile device providing personal hotspot functionality is not considered to support 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 local applications or data.
Function 24	Disable
Function 25	Enable
Function 26	Enable
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 no requirement that it be configurable; such certificates or public-keys may be pre-populated with the operating system software.
Function 36	For devices accommodating advisory warning messages of 1300 characters: *You are accessing a U.S. Government (USG) Information System (IS)*

FMT_SMF_EXT.1 Function	DoD Selections and Values
	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 39	Disable USB mass storage mode
Function 40	Disable backup to locally connected system Disable backup to remote system
Function 41	Enable USB tethering authentication Application note: If USB tethering is permitted, the connection must be authenticated. There is no requirement to enable USB tethering.
Function 45	Enable user acknowledgment of advisory message configured for Function 36. Disable automatic transfer of diagnostic data to an external device

FMT_SMF_EXT.1 Function	DoD Selections and Values
	other than an MDM service with which the device has enrolled. Disable authentication mechanisms providing user access to protected data other than a Password Authentication Factor (e.g., using a fingerprint), unless mechanism is DoD approved. Disable VPN split-tunneling (if the MD provides a configurable control for FDP_IFC_EXT.1.1). Disable multi-user modes. Enable access control policy (for FDP_ACF_EXT.1.2).