DoD Annex
for
Mobile Device Fundamentals (MDF) Protection Profile

Version 1, Release 1

29 January 2014

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 FSO of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

This page is intentionally left blank.

1. INTRODUCTION

1.1 Background

A National Information Assurance Partnership (NIAP) approved Protection Profile (PP) includes requirements to ensure particular functionality is present and can be tested in a commercial product. It is possible there will be cases in which selections meet PP requirements but do not meet DoD-mandated specific values.

In accordance with the NIAP *Protection Profile for Mobile Device Fundamentals* (Version 1.0, Revision 1, dated 27 January 2014), selections, assignments, and objective requirements may be included in the NIAP Common Criteria Security Target (ST) such that the product still conforms to the Protection Profile. This document addresses the DoD specificity needed for mobile devices to be used within the DoD. As such, any vendor that wishes to be certified for DoD use must indicate that they are claiming compliance with both the PP and the DoD Annex, and include the specified selections, assignments, and requirements in the ST upon initiation of a NIAP evaluation.

While a NIAP certificate can be awarded as long as the product meets all requirements in the PP, for use in the DoD, it is also mandated that the product address all requirements listed in this DoD Annex.

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 STIGs

This Annex for Mobile Device Fundamentals Protection Profile (MDFPP) addresses the DoD specificity to the NIST SP 800-53 controls identified in the MDFPP. As a result, the Annex, in conjunction with the PP, serves as a single specification, within the DoD, for security of Mobile Devices and supersedes the current DISA MOS SRG Version 1, Release 3.

The publication of the Annex does not eliminate the DoD need for a product-specific Security Technical Implementation Guide (STIG); however, the results of the Common Criteria evaluation will be used to formulate a STIG. The benefit of this approach is that at the conclusion of a successful NIAP evaluation, a vendor's product will be certified as meeting the requisite NIST SP 800-53 controls and the information needed for a STIG will be available. The product may then be used within the DoD. STIGs will continue to be published in XCCDF format along with automation where applicable for assessment, as well as baseline configuration guidance for DoD.

1.4 Document Revisions

Comments or proposed revisions to this document should be sent via email to: disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil.

2. DOD-MANDATED INFORMATION

Convention: Underlined text indicates assignments to be included in the MDFPP that are applicable in the DoD environment. ~~Strikethrough text~~ indicates a selection not applicable in the DoD environment.

2.1 DoD Assignments and Selections

The following assignments and selections from Security Functional Requirements are mandated for the DoD:

FCS_STG_EXT.1.4	[selection: ~~the user,~~ the administrator, a common application developer]
FIA_AFL_EXT.1.2	[selection: full wipe of all protected data~~, a remediation action set by the administrator~~].
FMT_MOF.1.1(1)	enable/disable [assignment: personal Hotspot connections] (5) enable/disable [assignment: tethered connections] (5) Note: Personal Hotspot service is defined as the mobile device serving as a Wi-Fi access point providing mobile broadband wireless Internet access to a wirelessly connected device. Tethered connections are defined as wired connections to the mobile device via a USB or other hardware port.
FMT_MOF.1.1(2)	enable/disable [assignment: wireless remote access connections except for personal Hotspot service, personal Hotspot connections, tethered connections] (8) enable/disable developer modes (11) enable/disable data-at-rest protection (12) enable/disable removable media's data-at-rest protection (13) enable/disable local authentication bypass (14) [assignment: enable/disable Location services, enable/disable USB mass storage mode] (31)
FMT_SMF.1.1	enable/disable [assignment: wireless remote access connections to the TOE except for personal Hotspot service, personal Hotspot connections, tethered connections] (20) enable/disable developer modes (21) enable/disable data-at-rest protection (22) enable/disable removable media's data-at-rest protection (23) enable/disable local authentication bypass (24) [assignment: enable/disable Location services, authenticate wired connections to the device via [selection: pre-shared key, passcode, [assignment: other specified authentication method], authenticate personal Hotspot connections to the device via [selection: pre-shared key, passcode, [assignment: other specified authentication method]], enable/disable USB mass storage mode] (42)

FMT_SMF_EXT.1	[selection: ~~*transition to the locked state*~~, *full wipe of protected data, wipe of sensitive data, alert the administrator, remove Enterprise applications*, ~~[assignment: *list other available remediation actions*~~]] upon unenrollment and [selection: ~~[assignment: *other administrator-configured triggers*], *no other triggers*~~].

2.2 Objective/Optional Functions Mandated for DoD

The following objective and optional Security Functional Requirements are mandated for the DoD:

- FCS_TLS_EXT.2.1
- FDP_IFC_EXT.1.1
- FPT_BBD_EXT.1.1
- FPT_TST_EXT.2.2
- FPT_TUD_EXT.2.5
- FTA_TAB.1.1

2.3 DoD-Mandated Configuration

The following value assignments are mandated for the DoD:

SFR ID	DoD Selections and Values
FCS	The TOE must be FIPS 140-2 validated.
FMT_MOF.1.1(2)	For Function 1 o minimum password length: 6 characters o minimum password complexity: no complexity rules required o maximum password lifetime: password expiration not required For Function 2 o screen lock enabled o screen lock timeout: 15 minutes or less o number of authentication failures: 10 or less For Function 4 o authorized application repository(s) must be listed o authorized applications and versions must be listed For Function 8 o disable wireless remote access connections except for personal Hotspot service For Function 11

	o disable developer modes For Function 12 o enable data-at-rest protection For Function 13 o enable removable media's data-at-rest protection For Function 14 o disable local authentication bypass For Function 31 o disable USB mass storage mode
FMT_SMF.1.1	For Function 1 o minimum password length: 6 characters o minimum password complexity: no complexity rules required maximum password lifetime: password expiration not required For Function 2 o screen lock enabled o screen lock timeout: 15 minutes or less o number of authentication failures (10 or less) For Function 10 o authorized application repository(s) must be listed o authorized applications and versions must be listed For Function 20 o disable wireless remote access connections except for personal Hotspot service For Function 21 o disable developer modes For Function 22 o enable data-at-rest protection For Function 23 o enable removable media's data-at-rest protection For Function 24 o disable local authentication bypass For Function 42

	o disable USB mass storage mode
FMT_SMF.1.1	For Function 41 The non-bracketed text below (either A or B) must be used without any changes as the warning banner. [A. Use this banner for desktops, laptops, and other devices accommodating banners of 1300 characters. The banner shall be implemented as a click-through banner at logon (to the extent permitted by the operating system); meaning it prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating "OK."] 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. -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. [B. For Blackberries and other PDAs/PEDs with severe character limitations:] I've read & consent to terms in IS user agreem't.