DoD ANNEX
FOR
EXTENDED PACKAGE FOR MOBILE DEVICE MANAGEMENT AGENTS V2.0

Version 1, Release 1

29 April 2015

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.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Background

This Annex to the Extended Package (EP) for Mobile Device Management Agents (Version 2.0, dated 31 December 2014) delineates EP 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 EP selections and assignments and EP security functional requirements (SFRs) listed as objective in the EP 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 EP specificity described in this Annex in its ST.

The EP for MDM Agents, 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 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 EP. 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 an EP SFR is not listed, there is no DoD-mandated selection or assignment for that SFR.
- For EP 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 exclude the selection.
- For EP 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 EP and the DoD Annex simultaneously to place the Annex information in context.

2.1 DoD-Mandated Assignments and Selections

DoD mandates the following EP SFR selections and assignments for SFRs in Section 4 of the EP:

Table 2-1: EP SFR Selections

SFR	Selections, Assignments, and Application Notes
FTP_ITC_EXT.1.2	MAS Server (if the MDM Agent supports the capability to interact with a MAS server)
FAU_ALT_EXT.2.1	c. change in enrollment state The following selections are required if the MDM Agent supports the capability to interact with a MAS server: d. failure to install an application from the MAS server e. failure to update an application from the MAS server
FMT_SMF_EXT.3.1	Application note: The function "read audit logs" encompasses the ability of the agent to transfer the logs to an MDM server. Regarding selection b, this function includes administrative functions related to the MAS Server if the MDM Agent supports the capability

SFR	Selections, Assignments, and Application Notes
	to interact with a MAS server.
FMT_SMF_EXT.3.2	configure periodicity of reachability events

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

The following SFRs (and associated selections and assignments) listed as objectives in the EP are mandated for the DoD:

- FAU_GEN.1.1(2) Refinement
- FAU_GEN.1.2(2) Refinement
- FMT_POL_EXT.2.1
- FMT_POL_EXT.2.2

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 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	DoD Selections and Values
FMT_SMF_EXT.3.2	periodicity of reachability events = *6 hours or less*