Mapping Between
Protection Profile Module for MDM Agents, Version 1.0, 25 April 2019
and
NIST SP 800-53 Revision 5

Important Caveats

- **Product vs. System.** The Common Criteria is designed for the evaluation of products; the Risk Management Framework (NIST SP 800-37 Revision 2, DOD 8510.01) and associated control/control interpretations (NIST SP 800-53 Revision 5, CNSSI № 1253) are used for the assessment and authorization of mission systems. **Products cannot satisfy controls outside of the system context**. Products may support a system satisfying particular controls, but typically satisfaction also requires the implementation of operational procedures; further, given that systems are typically the product of integration of multiple products configured to meet mission requirements, an overall system assessment is required to determine if the control is satisfied in the overall system context.
- **SA-4(7).** Perhaps it is needless to say, but satisfaction of any NIAP PP-Module supports system satisfaction of SA-4(7), which is the implementation of CNSSP № 11.
- **AC-19.** Independent of any individual SFRs, the primary purpose of this TOE is to support the enforcement of AC-19 by facilitating the application of access control restrictions to mobile devices.
- **System context of supported controls.** For a conformant TOE to support these controls in the context of an information system, the selections and assignments completed in the TOE's Security Target must be congruent with those made for the supported controls. For example, the TOE's ability to generate audit records only supports AU-2 to the extent that the TOE's audit records are included in the set of "organization-defined auditable events" assigned by that control. The security control assessor must compare the TOE's functional claims to the behavior required for the system to determine the extent to which the applicable controls are supported.
- **TOE vs OE implementation.** Many SFRs in this PP-Module describe functionality that may be implemented either by the TOE itself or through TSF implication of a similarly-validated component in its operational environment (i.e., a general-purpose operating system). Those SFRs that may be implemented in this manner are denoted with an asterisk (*).

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
MDF PP Additional Requirements				
FCS_STG_EXT.4*	**Cryptographic Key Storage**	AC-3(11)	**Access Enforcement:** Restrict Access to Specific Information Types	The access restrictions enforced by a conformant TOE include restriction of access to cryptographic keys, which is an example of an information type referenced by this control.
		SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE will ensure that its cryptographic keys are protected at rest using an appropriate method. For this PP-Module, the TOE is expected to interface with platform-provided storage.
FTP_ITC_EXT.1(2)	**Trusted Channel Communication**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	A conformant TOE supports the enforcement of this control through use of mutually-authenticated cryptographic protocols.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting data in transit.
FTP_TRP.1(2)	**Trusted Path (for Enrollment)**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	A conformant TOE may support the enforcement of this control if the protocol(s) used to establish trusted communications uses mutual authentication.
		SC-8(1)	**Transmission Confidentiality and Integrity:**	A conformant TOE will have the ability to prevent unauthorized disclosure of information and detect

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
			Cryptographic Protection	modification to that information.
		SC-11	**Trusted Path**	The TOE establishes a trusted communication path between remote users and itself.
MDM PP Additional Requirement				
FCS_STG_EXT.1(2)*	**Cryptographic Key Storage**	AC-3(11)	**Access Enforcement:** Restrict Access to Specific Information Types	The access restrictions enforced by a conformant TOE include restriction of access to cryptographic keys, which is an example of an information type referenced by this control.
		SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE will ensure that its cryptographic keys are protected at rest using an appropriate method. For this PP-Module, the TOE is expected to interface with platform-provided storage.
Mandatory Requirements				
FAU_ALT_EXT.2	**Agent Alerts**	AU-2 or SI-4 (5)	**Event Logging** **-or-** **System Monitoring:** System-Generated Alerts	A conformant TOE will automatically generate alerts when certain behaviors occur as a method of detecting suspicious activity. The control that is supported by this function depends on whether the 'alert' is delivered silently as an audit record or as a real-time notification.
		SI-6	**Security and Privacy Function Verification**	A conformant TOE has the ability to verify that periodic security events are taking place and to generate a notification upon detection of this activity.
FAU_GEN.1(2)*	**Audit Data Generation**	AU-2	**Event Logging**	A conformant TOE has the ability to generate audit records for various events.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
		AU-3	**Content of Audit Records**	A conformant TOE will ensure that audit records include date, type, outcome, and subject identity data. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
		AU-3(1)	**Content of Audit Records:** Additional Audit Information	A conformant TOE will ensure that audit records include date, type, outcome, and subject identity data. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
		AU-12	**Audit Record Generation**	A conformant TOE has the ability to generate audit logs. The TOE supports the enforcement of parts (a) and (c) of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
FAU_SEL.1(2)*	**Security Audit Event Selection**	AU-12	**Audit Record Generation**	A conformant TOE supports part (b) of the control by allowing for administrative control over the specific types of audit records that are generated.
FIA_ENR_EXT.2	**Agent Enrollment of Mobile Device into Management**	IA-3	**Device Identification and Authentication**	A conformant TOE supports the enforcement of this control by storing the machine identifier used for the MDM server from which it receives policy updates.
FMT_POL_EXT.2	**Agent Trusted Policy Update**	SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE supports this control by ensuring the integrity of policy data it receives from a remote MDM.
		SI-7(6)	**Software, Firmware, and Information Integrity:** Cryptographic Protection	A conformant TOE enforces the integrity of policy data using digital signatures.
FMT_SMF_EXT.4	**Specification of Management Functions**	AC-19	**Access Control for Mobile Devices**	A conformant TOE supports the enforcement of this control through a function where policies can be applied to a mobile device that can enforce configuration and connectivity requirements.
		SI-17	**Public Key Infrastructure Certificates**	A conformant TOE supports the enforcement of this control by facilitating the import of certificates into the TOE's trust store.
FMT_UNR_EXT.1	**User Unenrollment Prevention**	N/A	**N/A**	There is no security control that specifically relates to unenrollment prevention.
Optional Requirements				
This PP-Module has no optional requirements.				
Selection-Based Requirements				
This PP-Module has no selection-based requirements.				

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
Objective Requirements				
FAU_STG_EXT.3*	**Security Audit Event Storage**	AU-9	**Protection of Audit Information**	A conformant TOE supports the enforcement of this control by using platform-provided audit storage as a secure repository for audit records.
FPT_NET_EXT.1	**Network Reachability**	SI-4	**System Monitoring**	A conformant TOE supports the enforcement of this control by sending notifications of its availability such that a sustained absence of such notifications may indicate compromise or misuse of the platform on which the TOE is installed.