Mapping Between

Extended Package for Mobile Device Management Agents, Version 3.0, 21-November-2016

and

NIST SP 800-53 Revision 4

Important Caveats

- **Product vs. System.** The Common Criteria is designed for the evaluation of products; the Risk Management Framework (NIST SP 800-37 Revision 1, DOD 8510.01) and associated control/control interpretations (NIST SP 800-53 Revision 4, 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 supports system satisfaction of SA-4(7), which is the implementation of CNSSP № 11.
- **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.

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 4 Control Supports**		**Comments and Observations**
MDF PP Security Functional Requirements Direction				
FCS_STG_EXT.4	**Cryptographic Key Storage**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE will help satisfy the key storage portion of this control.
FTP_ITC_EXT.1	**Trusted Channel Communication**	AC-18(1)	**Wireless Access:** Authentication and Encryption	A conformant TOE requires authentication and encryption to be performed in order to establish wireless communications.

		IA-3(1)	**Device Identification and Authentication**: Cryptographic Bidirectional Authentication	The use of the cryptographic protocols specified in the SFR implies that the TOE can perform mutual authentication with trusted remote entities.
		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 or Alternate Physical Protection	The TOE supports a cryptographic method of protecting data in transit.
MDM PP Security Functional Requirements Direction				
FCS_STG_EXT.1(2)	**Cryptographic Key Storage**	IA-5	**Authenticator Management**	A conformant TOE will protect credential data from unauthorized modification or disclosure.
		SC-12	**Cryptographic Protection**	A conformant TOE will help satisfy the key storage portion of this control.
TOE Security Functional Requirements				
FAU_ALT_EXT.2	**Agent Alerts**	AU-2 or SI-4(5)	**Audit Events** -or- **Information 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 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	**Auditable Events**	A conformant TOE has the ability to generate audit records for various events. 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 generate audit information for some auditable events beyond what is mandated in AU-3. This may or may not be sufficient to satisfy this control based on the additional audit information required by the organization. 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 Generation**	A conformant TOE has the ability to generate audit logs. 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.
FAU_SEL.1(2)	**Security Audit Event Selection**	AU-12	**Audit Generation**	A conformant TOE has the ability to support part (b) of this control by providing a mechanism to determine the set of auditable events that result in the generation of audit records. 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.
FIA_ENR_EXT.2	**Enrollment of Mobile Device into Management**	IA-3	**Device Identification and Authentication**	A conformant TOE will have the ability to record the reference identifier of its enrolled MDM Server as a part of the authentication process.
FMT_POL_EXT.2	**Trusted Policy Update**	AC-3	**Access Enforcement**	A conformant TOE supports this control by providing an interface to implement access enforcement to users of enrolled mobile devices.

		AC-18	**Wireless Access**	A conformant TOE will provide a mechanism to update the wireless access policy configuration of the mobile device.
		AC-19	**Access Control for Mobile Devices**	A conformant TOE will provide a mechanism to update the security configuration of the underlying mobile device.
		CM-6	**Configuration Settings**	The TOE supports part b of this control by providing a mechanism to define and enforce configuration settings for enrolled mobile devices.
		CM-6(1)	**Configuration Settings:** Automated Central Management / Application / Verification	A conformant TOE supports this control by automatically pushing policy changes to all applicable enrolled devices.
FMT_SMF_EXT.3	**Specification of Management Functions**	CM-6	**Configuration Settings**	A conformant TOE may satisfy one or more optional capabilities defined in this SFR. In general, a conformant TOE will satisfy this control to the extent that the TOE provides a method to configure its behavior in accordance with STIGs or other organizational requirements. Specific additional controls may be supported depending on the functionality claimed by the TOE; the security control assessor must review what has been selected in the Security Target and determine what

				additional support is provided, if any.
		IA-5	**Authenticator Management**	A conformant TOE supports this control by providing a mechanism to import X.509 certificates.
FMT_UNR_EXT.1	**User Unenrollment Prevention**	AC-19	**Access Control for Mobile Devices**	A conformant TOE will enforce mobile device access control by preventing the application of access control policies from bypass via unenrollment.
TOE or Platform Security Functional Requirements				
FAU_GEN.1.2(2)	**Audit Data Generation**	AU-2	**Auditable Events**	A conformant TOE has the ability to generate audit records for various events. 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 generate audit information for some auditable events beyond what is mandated in AU-3. This may or may not be sufficient to satisfy this control based on the additional audit information required by the organization. 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 Generation**	A conformant TOE has the ability to generate audit logs. 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.
Optional Requirements				
N/A	**N/A**	**N/A**	**N/A**	**N/A**
Selection-based Requirements				
N/A	**N/A**	**N/A**	**N/A**	**N/A**
Objective Requirements				
FAU_STG_EXT.1	**Security Audit Event Storage**	AU-9	**Protection of Audit Information**	A conformant TOE has the ability to write audit

				data to a trusted location.
FPT_NET_EXT.1	**Network Reachability**	SI-4	**Information System Monitoring**	A conformant TOE will support this control by detecting when server communications are unavailable, which is a potential indicator of malicious use. Note that the underlying mobile device and not the MDM Agent TOE specifically is responsible for taking any action in response to this detection.