Mapping Between
Protection Profile for Mobile Device Management, Version 4.0, 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 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.
- **TOE vs OE implementation.** Many SFRs in this PP 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 Supports		Comments and Observations
TOE Security Functional Requirements				
FAU_ALT_EXT.1	**Server Alerts**	SI-4 (5)	**System Monitoring:** System-Generated Alerts	A conformant TOE will automatically generate alerts when certain behaviors occur as a method of detecting suspicious activity.
FAU_GEN.1(1)*	**Audit Data Generation**	AU-2	**Event Logging**	A conformant TOE has the ability to generate (or invoke its operational environment 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 has the ability to generate (or invoke its operational environment to generate) audit records that give details about the type of audit event that took place.
		AU-3(1)	**Content of Audit Records:** Additional Audit Information	A conformant TOE has the ability to capture additional details about the event depending on the contents of the audit record.
		AU-12	**Audit Record Generation**	A conformant TOE has the ability to generate (or invoke its operational environment 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_NET_EXT.1	Network Reachability Review	N/A	N/A	This SFR does not map to any controls. The requirement provides network monitoring which

				does not independently address any controls.
FAU_STG_EXT.1*	**External Trail Storage**	AU-9	**Protection of Audit Information**	A conformant TOE has the ability to write audit data to a trusted location.
		AU-9(2)	**Protection of Audit Information:** Store on Separate Physical Systems or Components	A conformant TOE must be able to transmit audit data to a logically remote location. It can be used to support the enforcement of this control if the recipient of the audit data is physically remote from the TOE.
FCS_CKM.1*	**Cryptographic Key Generation**	SC-12	**Cryptographic Key Establishment and Management**	The ability of the TOE to generate (or invoke its operational environment to generate) asymmetric keys satisfies the key generation portion of this control.
		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	A conformant TOE ensures that generated asymmetric keys provide an appropriate level of security.
FCS_CKM.2*	**Cryptographic Key Establishment**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports this control either by providing its own key establishment function or invoking an environmental one.
		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	A conformant TOE supports the production of asymmetric keys either by providing its own key establishment function or invoking an environmental one.
FCS_CKM_EXT.4*	**Cryptographic Key Destruction**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely destroy cryptographic keys through either its own mechanisms or environmental ones.
FCS_COP.1(1)*	**Cryptographic Operation (Confidentiality Algorithms)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform (or invoke environmental methods to perform) symmetric encryption using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(2)*	**Cryptographic Operation (Hashing Algorithms)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform (or invoke environmental methods to

				perform) cryptographic hashing using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(3)*	**Cryptographic Operation (Signature Algorithms)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform (or invoke environmental methods to perform) cryptographic signature operations using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(4)*	**Cryptographic Operation (Keyed-Hash Message Authentication)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform (or invoke environmental methods to perform) keyed-hash message authentication using NSA-approved and FIPS-validated algorithms.
FCS_RBG_EXT.1*	**Extended: Random Bit Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to generate (or invoke environmental methods to generate) random bits for use in cryptographic services using FIPS- and NSA-approved standards.
FCS_STG_EXT.1*	**Cryptographic Key Storage**	IA-5	**Authenticator Management**	A conformant TOE or its environment protects private key data used as authenticators from unauthorized disclosure, either through its own mechanisms or through environmental ones, in support of part g) of this control.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE or its environment supports the enforcement of this control by protecting stored cryptographic data, either through its own mechanisms or through invocation of environmental ones.
FIA_ENR_EXT.1	**Enrollment of Mobile Device into Management**	AC-3	**Access Enforcement**	A conformant TOE has the ability to limit the devices that users can enroll based on certain device characteristics.
		IA-2	**Identification and Authentication**	A conformant TOE has the ability to authenticate the

			(Organizational Users)	user during enrollment of the device. This control addresses FIA_ENR_EXT.1.1 of this SFR, which deals with user authentication.
		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. This control specifically addresses FIA_ENR_EXT.1.2, which deals with enrollment of the device, not the user.
FIA_UAU.1*	**Timing of Authentication**	AC-14	**Permitted Actions without Identification or Authentication**	A conformant TOE or its environment has the ability to identify the actions allowed prior to authentication. This requires all users to be successfully identified and authenticated prior to performing any management activities.
		IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE or its environment has the ability to authenticate users prior to TSF functionality access.
FIA_X509_EXT.1(1)*	**X.509 Certificate Validation**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE or its environment has the ability to validate certificate path and status, or invoke an environmental service to do this.
		SC-23	**Session Authenticity**	Depending on the TOE's use of trusted communications channels, it may use X.509 certificate validation in support of session authentication.
		SC-23(5)	**Session Authenticity:** Allowed Certificate Authorities	If the TOE uses X.509 certificates as part of session authentication, it will include the functionality needed (or invoke the functionality from its environment) to validate certificate authorities.
FIA_X509_EXT.2*	**X.509 Certificate Authentication**	IA-5(2)	**Authenticator Management:**	A conformant TOE or its environment has the ability

			Public Key-Based Authentication	to authenticate trusted channel communications using X.509 certificates. Other controls apply If the TOE also uses code signing certificates for software updates (CM-14, SI-7(15)), policies (SI-7, SI-7(1), SI-7(6)), integrity verification (SI-7, SI-7(1), SI-7(6)). IA-3(1) also applies if the TOE's use of an X.509 authentication mechanism is to support the case where the TOE is a server that validates the X.509 certificate of a client.
FIA_X509_EXT.5*	**X.509 Unique Certificate**	IA-3	**Device Identification and Authentication**	A conformant TOE or its environment enforces each enrolled device being uniquely identified through a unique certificate.
		IA-4	**Identifier Management**	A conformant TOE or its environment requires a unique certificate for each client device, satisfying part (b) of this control.
FMT_MOF.1(1)	**Management of Functions Behavior**	AC-3	**Access Enforcement**	A conformant TOE supports this control by providing access control restrictions to various functions. Note that the extent of support depends on the extent to which this behavior is captured in the organizational access control policies defined by AC-1.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE supports this control by providing different role-based levels of management functionality to users, administrators, and the MDM.
		AC-6	**Least Privilege**	A conformant TOE supports the concept of least privilege by limiting device management functions to only the roles that are needed to perform them.

		AC-6(1)	**Least Privilege:** Authorize Access to Security Functions	A conformant TOE defines its management authorizations so that explicit authorization is required to perform a management function.
		AC-6(10)	**Least Privilege:** Prohibit Non-Privileged Users from Executing Privileged Functions	A conformant TOE supports this control by defining some management functionality as privileged, so ordinary users cannot perform these functions.
FMT_MOF.1(2)	**Management of Functions Behavior (Enrollment)**	AC-3	**Access Enforcement**	A conformant TOE has the ability to restrict access to functions during enrollment.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE has the ability to provide access control by assigning privileges to roles.
FMT_POL_EXT.1	**Trusted Policy Update**	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.
		SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE supports this control by ensuring the integrity of policy data it transmits to remote MDM agents.
		SI-7(6)	**Software, Firmware, and Information Integrity:** Cryptographic Protection	A conformant TOE enforces the integrity of policy data using digital signatures.
FMT_SMF.1(1)	**Specification of Management Functions (Server Configuration of Agent)**	N/A	**N/A**	There are no controls that map to this SFR because no controls address the issuing of commands. However, it is possible the commands listed in this SFR directly relate to a control.
FMT_SMF.1(2)	**Specification of Management**	N/A	**N/A**	There are no controls that map to this SFR because

	Functions (Server Configuration of Server)			there are no controls that address performing these management functions during server configuration. However, it is possible the functions listed in this SFR directly relate to a control.
FMT_SMR.1(1)	**Security Management Roles**	AC-2(7)	**Account Management:** Privileged User Accounts	A conformant TOE defines a role-based access model that allows individual users to be assigned to different administrative roles.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE has the ability to enforce differing levels of access control to individual management roles.
FPT_API_EXT.1	**Use of Supported Services and APIs**	SA-15(5)	**Development Process, Standards, and Tools:** Attack Surface Reduction	The developer of a conformant TOE identifies the application programming interfaces to reduce the attack surface.
FPT_LIB_EXT.1	**Use of Third Party Libraries**	SA-15(5)	**Development Process, Standards, and Tools:** Attack Surface Reduction	A conformant TOE supports the enforcement of this control because enumerating the third party libraries used by the TOE reduces the attack surface of the TSF to known components.
FPT_TST_EXT.1*	**TSF Functionality Testing**	SI-6	**Security and Privacy Function Verification**	A conformant TOE will run automatic tests to ensure correct operation of its own functionality.
		SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE supports the enforcement of this control by providing a means (either through itself or its environment) to verify its own integrity.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	The TOE ensures that its integrity is checked at startup.
		SI-7(6)	**Software, Firmware, and Information Integrity:** Cryptographic Protection	The TOE uses a cryptographic mechanism (either internal to the TSF or in its environment) to validate its own integrity.

		SI-7(12)	**Software, Firmware, and Information Integrity:** Integrity Verification	A conformant TOE supports the enforcement of this control by ensuring its integrity is verified when it is executed.
FPT_TUD_EXT.1*	**Trusted Update**	CM-14	**Signed Components**	A conformant TOE has the ability to require a signed update.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	The TOE has the ability to verify the integrity of updates to itself or to invoke an environmental function to do this.
FTP_ITC_EXT.1	**Trusted Channel**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	A conformant TOE may support the enforcement of this control if the protocols used to establish trusted communications use mutual authentication.
		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_ITC.1(1)*	**Inter-TSF Trusted Channel (Authorized Entities)**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	A conformant TOE may support the enforcement of this control if the protocols used to establish trusted communications use mutual authentication.
		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(1)*	**Trusted Path (for Remote Administration)**	SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE will have the ability to prevent unauthorized disclosure of information and detect

				modification to that information.
		SC-11	**Trusted Path**	The TOE establishes a trusted communication path between remote users and itself.
FTP_TRP.1(2)*	**Trusted Paths (for Enrollment)**	SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE will have the ability to prevent unauthorized disclosure of information and detect modification to that information.
		SC-11	**Trusted Path**	The TOE establishes a trusted communication path between remote users and itself upon enrollment.
Optional Requirements				
FAU_SAR.1	**Audit Review**	AU-6(7)	**Audit Record Review, Analysis, and Reporting:** Permitted Actions	A conformant TOE will allow designation of permitted actions to the respective roles.
		AU-7	**Audit Record Reduction and Report Generation**	A conformant TOE provides audit review mechanisms to administrators.
FAU_SEL.1	**Security Audit Event Selection**	AU-12	**Audit Record 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.
FTA_TAB.1	**Default TOE Access Banners**	AC-8	**System Use Notification**	The TOE displays an advisory warning to the user prior to authentication.
Selection-Based Requirements				
FAU_GEN.1(2)*	**Audit Generation (MAS Server)**	AU-2	**Event Logging**	A conformant TOE has the ability to generate audit records for various events or invoke platform functionality that does this. 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, either generated by it or by its environment, 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 Record Generation**	A conformant TOE has the ability to generate audit logs or to invoke platform functionality that does this. 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_STG_EXT.2*	**Audit Event Storage**	AU-9	**Protection of Audit Information**	A conformant TOE has the ability to prevent unauthorized modification and deletion of audit records, or to store this data in its environment where it is subject to the same protections.

FCS_HTTPS_EXT.1	**HTTPS Protocol**	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 ability of a conformant TOE to implement HTTPS using TLS 1.2 ensures the confidentiality and integrity of data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FCS_IV_EXT.1*	**Initialization Vector Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE or its environment has the ability to generate initialization vectors that ensure the secure operation of cryptographic functions.
FCS_STG_EXT.2*	**Cryptographic Key Storage**	IA-5(6)	**Authenticator Management:** Protection of Authenticators	A conformant TOE has the ability to prevent unauthorized access to authenticators.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE ensures 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 use of the protocols specified in the SFR ensures the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE will use a key hierarchy to ensure the secure storage of cryptographic keys.
FIA_X509_EXT.1(2)*	**X.509 Certificate Validation**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE has the ability to validate the certificate path and status, or invoke an environmental

				service to do this, which satisfies this control.
		SC-23	**Session Authenticity**	Depending on the TOE's use of trusted communications channels, it may use X.509 certificate validation in support of session authentication.
		SC-23(5)	**Session Authenticity:** Allowed Certificate Authorities	If the TOE uses X.509 certificates as part of session authentication, it will include the functionality needed to validate certificate authorities, or invoke this functionality in its operational environment.
FMT_MOF.1(3)	**Management of Functions in (MAS Server Downloads)**	AC-3	**Access Enforcement**	A conformant TOE supports this control by providing access control restrictions to various functions. Note that the extent of support depends on the extent that this behavior is captured in the organizational access control policies defined by AC-1.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE supports this control by providing different role-based levels of management functionality from users to administrators.
FMT_SMF.1(3)	**Specification of Functions (MAS Server)**	N/A	**N/A**	There are no controls that map to this SFR because there are no controls that address performing these management functions during server configuration. However, it is possible the functions listed in this SFR directly relate to a control.
FMT_SMR.1(2)	**Security Management Roles (MAS Server)**	AC-2(7)	**Account Management:** Privileged User Accounts	A conformant TOE has the ability to associate users with roles such that only members of an authorized role can administer the MAS Server.
FPT_ITT.1(1)*	**Internal TOE TSF Data Transfer**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE will support this control by providing a protected communication channel

				between mobile applications and remote trusted IT products or by using an environmental channel for the same purpose.
		SC-8(1)	**Transmission Confidentiality and Integrity** Cryptographic Protection	The protected communications implemented or invoked by the TOE use cryptographic methods to secure data in transit.
FPT_ITT.1(2)*	**Internal TOE TSF Data Transfer (MDM Agent)**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	A conformant TOE may support the enforcement of this control if the protocols it uses or invokes from its environment to establish trusted communications use mutual authentication.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE will support this control by providing a protected communication channel between mobile applications and remote trusted IT products or by using an environmental channel for the same purpose.
		SC-8(1)	**Transmission Confidentiality and Integrity** Cryptographic Protection	The protected communications implemented or invoked by the TOE use cryptographic methods to secure data in transit.
FTP_ITC.1(2)*	**Inter-TSF Trusted Channel (MDM Agent)**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	A conformant TOE may support the enforcement of this control if the protocols it uses or invokes to establish trusted communications use mutual authentication.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE will support this control by providing or invoking a protected communication channel between mobile applications and remote trusted IT products.
		SC-8(1)	**Transmission Confidentiality and Integrity**	The protected communications implemented by the TOE or

			Cryptographic Protection	its environment use cryptographic methods to secure data in transit.
Objective Requirements				
FAU_CRP_EXT.1	**Support for Compliance Reporting of Mobile Device Configuration**	CM-6(1)	**Configuration Settings:** Automated Management, Application, and Verification	A conformant TOE supports the enforcement of this control by allowing other components of the information system to obtain configuration data about organizational assets from the TOE.
		IA-3(4)	**Device Identification and Authentication:** Device Attestation	A conformant TOE supports the enforcement of this control by collecting data about enrolled devices that can be used for attestation purposes.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to securely transmit configuration data.
		SC-8(1)	**Transmission Confidentiality and Integrity** Cryptographic Protection	The protected communications implemented by the TOE or its environment use cryptographic methods to secure data in transit.
FCO_CPC_EXT.1*	**Component Registration Channel Definition**	AC-4	**Information Flow Enforcement**	A conformant TOE supports the enforcement of this control by providing a registration mechanism that is used as a condition for distributed TOE components to establish information flow between them, or by invoking an environmental facility that performs the same function.
FIA_UAU_EXT.4(1)	**User Authentication (Re-Use Prevention)**	IA-2(8)	**Identification and Authentication (Organizational Users:** Access to Accounts – Replay Resistant	A conformant TOE supports enforcement of this control by preventing re-use of user credentials that were already used for enrollment of a mobile device.
FIA_UAU_EXT.4(2)	**User Authentication (Re-Use Prevention for Device Enrollment)**	IA-3	**Device Identification and Authentication**	A conformant TOE supports the enforcement of this control by ensuring that the uniqueness of device identifiers is enforced.

FIA_X509_EXT.3*	**X.509 Enrollment**	SC-17	**Public Key Infrastructure Certificates**	This function, whether implemented by the TSF or by its environment, supports behavior related to certificate issuance.
FIA_X509_EXT.4	**Alternate X.509 Enrollment**	SC-17	**Public Key Infrastructure Certificates**	This function, whether implemented by the TSF or by its environment, supports behavior related to certificate issuance.
FMT_SAE_EXT.1	**Security Attribute Expiration**	AC-3(8)	**Access Enforcement:** Revocation of Access Authorizations	A conformant TOE has the ability to support revocation of access authorizations by specifying a maximum time limit for the validity of credentials used to gain access to protected resources.
FTP_TRP.1(3)*	**Trusted Path (for Joining)**	SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE has the ability to protect communications between a joining component and the TOE using either its own functionality or by invocation of an environmental function. Note that while integrity protection is assured by this SFR, confidentiality is supported but not required.
		SC-11(1)	**Trusted Path:** Irrefutable Communications Path	A conformant TOE that claims this SFR ensures that the registration channel is logically isolated from other communications.