Mapping Between

Protection Profile for Mobile Device Management, 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**
TOE Security Functional Requirements				
FAU_ALT_EXT.1	**Server Alerts**	AU-2 or SI-4(5)	**Audit Events** -or-	A conformant TOE will automatically generate alerts when certain behaviors occur as a method of detecting suspicious activity. The

			Information System Monitoring: System-Generated Alerts	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_NET_EXT.1	**Network Reachability**	N/A	**N/A**	This SFR does not map to any controls. The requirement provides network monitoring which does not independently address any controls.
FIA_ENR_EXT.1	**Enrollment of Mobile Device into Management**	IA-2	**Device Identification and Authentication**	A conformant TOE has the ability to authenticate the user during the enrollment of 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 addresses FIA_ENR_EXT.1.2 of this SFR which deals with enrollment of the device, not user.

		AC-3	**Access Enforcement**	A conformant TOE has the ability to provide access or restrictions to resources based on access policy implementation.
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 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(10)	**Least Privilege:** Prohibit Non-Privileged Users from Executing Privileged Functions	A conformant TOE supports this control by defining some management functionality as privileged such that ordinary users cannot perform these functions.

FMT_MOF.1(2)	**Management of Functions Behavior:** Enrollment	AC-3	**Access Control**	A conformant TOE has the ability to restrict access to functions upon enrollment.
		AC-3(7)	**Access Control:** 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**	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.
		AC-19	**Access Control for Mobile Devices**	A conformant TOE will provide a mechanism to update the security configuration of the underlying mobile device.
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 there are no controls that 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 Functions:** Server Configuration of 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 upon 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:** Role-Based Schemes	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_TUD_EXT.1	**Trusted Update**	CM-5(3)	**Access Restrictions For Change:** Signed Components	A conformant TOE has the ability to require that third-party applications running on it use signed updates. This control addresses the optional elements in FPT_TUD_EXT.1.3
		SI-7(1)	**Software, Firmware and Information Integrity:** Integrity Checks	A conformant TOE has the ability to verify the integrity of updates to itself. This control addresses the optional elements in FPT_TUD_EXT.1.2.
TOE or Platform Security Functional Requirements				
FAU_GEN.1(1)	**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 has the ability 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 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_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.
FCS_CKM.1	**Cryptographic Key Generation**	SC-12	**Cryptographic Key Establishment and Management**	The ability of the TOE 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's 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 by providing a key establishment function.

		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	A conformant TOE supports the production of asymmetric keys by providing a key establishment function.
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.
FCS_COP.1(1)	**Cryptographic Operation**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform signature verification using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(2)	**Cryptographic Operation:** Hashing Algoritms	SC-13	**Cryptographic Protection**	A conformant TOE has the ability 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 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 keyed-hash message authentication using NSA-approved and FIPS-validated algorithms.
FCS_RBG_EXT.1	**Random Bit Generation**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to generate random bits for use in cryptographic services using FIPS and NSA-approved standards.

FCS_STG_EXT.1	**Cryptographic Key Storage**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely store cryptographic keys.
FIA_UAU.1	**Timing of Authentication**	AC-14	**Permitted Actions without Identification and Authentication**	A conformant TOE has the ability to identify the actions allowed prior to authentication. This requires all users to be successfully identified and authentication prior to performing any management activities.
FIA_X509_EXT.1	**Validation of Certificates**	IA-5(2)	**Authenticator Management:** PKI-Based Authentication	A conformant TOE has the ability to certificate path and status, 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.
FIA_X509_EXT.2	**Certificate Authentication**	IA-5	**Authenticator Management**	A conformant TOE has the ability to generate certificate request messages that can be used to establish initial authenticator content, satisfying part (b) of this control.
		IA-5(2)	**Authenticator Management:** PKI-Based Authentication	A conformant TOE will validate certificate responses, satisfying part (a) of this control.

FPT_TST_EXT.1	**TSF Functionality Testing**	SI-6	**Security Function Verification**	A conformant TOE will run automatic tests to ensure correct operation of its own functionality.
		SI-7(1)	**Software, Firmware and Information Integrity:** Integrity Checks	The TOE has the ability to verify the integrity of the boot chain prior to execution.
		SI-7(6)	**Software, Firmware and Information Integrity:** Cryptographically-validated integrity	A conformant TOE has the ability to implement cryptographic mechanisms to detect unauthorized change.
		SI-7(9)	**Software, Firmware and Information Integrity:** Integrity of system boot	A conformant TOE has the ability to verify the integrity of the boot process.
FPT_TUD_EXT.1	**Trusted Update**	CM-5(3)	**Access Restrictions For Change:** 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.
FTP_ITC.1(1)	**Inter-TSF Trusted Channel:** Authorized 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.

FTP_TRP.1(1)	**Trusted Paths:** Remote Entities	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-11	**Trusted Path**	The TOE establishes a trusted communication path between remote users and itself upon enrollment.
Optional TSF Requirements				
FAU_SEL.1	**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.
FPT_ITT.1 *(This requirement is only optional if FTP_ITC.1(2) is already claimed)*	**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.
		SC-8(1)	**Transmission Confidentiality and Integrity**	The protected communications implemented by the TOE use cryptographic methods to secure data in transit.
FTA_TAB.1	**TOE Access Banner**	AC-8	**System Use Notification**	The TOE displays an advisory warning to the user prior to authentication.
FTP_ITC.1(2) *(This requirement is only optional if FTP_ITT.1 is already claimed)*	**Inter-TSF Trusted Channel:** MDM Agent	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.
Optional TOE or Platform Requirements				
FAU_SAR.1	**Audit Review**	AU-7	**Audit Reduction and Report Generation**	A conformant TOE provides audit review mechanisms to administrators.
		AU-6(7)	**Audit Review, Analysis, and Reporting:** Permitted Actions	A conformant TOE will allow designation of permitted actions to their respective roles.
FCS_TLSC_EXT.1	**TLS Client Protocol**	IA-5(2)	**Authenticator Management:** PKI-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications, supporting this control.
		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 Integrity:** Cryptographic or Alternate Physical Protection	The TOE supports a cryptographic method of protecting 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.
Optional Requirements to Support MAS Server				
FAU_GEN.1(2)	**<u>Audit Generation:</u>** MAS Server	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_STG_EXT.1 (2)	**External Audit Trail Storage:** MAS Server	AU-9	**Protection of Audit Information**	A conformant TOE has the ability to write audit data to a trusted location.
FMT_MOF.1(3)	**Management of Functions:** MAS Server	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 from users to administrators.

FMT_MOF.1(4)	**Management of Functions:** MAS Server Download	AC-3	**Access Enforcement**	A conformant TOE supports this control by providing an interface to implement access enforcement to users of enrolled mobile devices.
FMT_SMF.1(3)	**Specification of Functions:** MAS Server	AC-3	**Access Enforcement**	A conformant TOE supports this control by providing an interface to implement access enforcement to users of enrolled mobile devices.
FMT_SMR.1(2)	**Security Management Roles:** MAS Server	AC-2 (7)	**Account Management:** Role-Based Schemes	A conformant TOE has the ability to associate users to roles that would restrict them from performing management activities beyond their assigned role.
FTP_ITC.1(3)	**Inter-TSF Trusted Channel:** MAS Server	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.

Selection-Based Requirements				
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.
FCS_DTLS_EXT.1	**DTLS Protocol**	IA-5(2)	**Authenticator Management:** PKI-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications, supporting this control.
		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 Integrity:** Cryptographic or Alternate Physical Protection	The TOE supports a cryptographic method of protecting 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_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 Integrity:** Cryptographic or Alternate Physical Protection	The ability of a conformant TOE to implement HTTPS using TLS 1.2 ensures the confidentiality and integrity of data and transit.
FCS_IV_EXT.1	**Initialization Vector Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to generate initialization vectors that ensure the secure operation of cryptographic functions.
FCS_STG_EXT.2	**Cryptographic Key Storage**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE will use a key hierarchy to ensure the secure storage of cryptographic keys.
		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 or Alternate Physical 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.
		IA-5(6)	**Authenticator Management:** Protection of Authenticators	A conformant TOE has the ability to prevent unauthorized access to authenticators.
FCS_TLSC_EXT.1	**TLS Client Protocol:** Elliptic Curves Extension	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 Integrity:** Cryptographic or Alternate Physical Protection	The ability of a conformant TOE to implement TLS with supported elliptic curves which ensures the confidentiality and integrity of data and transit.
FCS_TLSS_EXT.1	**TLS Server Protocol**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE implements TLS as a method of ensuring confidentiality and integrity of data in transit.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic or Alternate Physical Protection	The TOE's use of TLS provides a cryptographic means to protect data in transit.
		SC-13	**Cryptographic Protection**	A conformant TOE's use of specific ciphersuites to establish a TLS channel allows it to conform with NSA standards.
Objective Requirements				
FAU_CRP_EXT.1	**Support for Compliance Reporting of Mobile Device Configuration**	CM-6(1)	**Configuration Settings:** Automated Central Management, Application, Verification	A conformant TOE enforces configuration compliance with central verification of mobile devices.
		IA-5(2)	**Authenticator Management:** PKI-Based Authentication	A conformant TOE has the ability to certificate path and status, which satisfies this control.

		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to securely transmit configuration data.
FIA_UAU_EXT. 4(1)	**User Authentication:** Re-Use Prevention	IA-5	**Identification and Authentication**	A compliant TOE has the ability to prevent the re-use of authenticator data by establishing minimum and maximum lifetime restrictions.
FIA_UAU_EXT. 4(2)	**User Authentication:** Re-Use Prevention for Device Enrollment	IA-4	**Identifier Management**	A compliant TOE has the ability to assign a user a unique identifier to prevent the re-use of that information by implementing policy restrictions.
FMT_SAE_EXT.1	**Security Attribute Expiration**	N/A	**N/A**	A conformant TOE has the ability to expire the authentication data that is entered upon enrollment.
Objective TOE or Platform Security Functional Requirements				
FCS_TLSC_EXT.1	**TLS Client Protocol**: Signature Algorithms	SC-13	**Cryptographic Protection**	A conformant TOE's use of specific hash algorithms in the establishment of a TLS session allows it to conform with NSA standards.
FCS_TLSS_EXT.1	**TLS Server Protocol**: Signature Algorithms	SC-13	**Cryptographic Protection**	A conformant TOE's use of specific hash algorithms in the establishment of a TLS session allows it to conform with NSA standards.
FIA_X509_EXT.3	**X.509 Enrollment**	IA-5(2)	**Authenticator Management:** PKI-Based Authentication	A conformant TOE supports this control in part by providing an interface to have certificate enrollment.

FIA_X509_EXT.4	**Alternate X.509 Enrollment**	IA-5(2)	**Authenticator Management:** PKI-Based Authentication	A conformant TOE will support the implementation of PKI-based authentication by validating peer certificates as part of the HTTPS authentication process.