NIST SP 800-53 Revision 4 Mapping: Protection Profile for Mobile Device Management Version 1.1 7 March 2014

Introduction

Several of the NIST SP 800-53/CNSS 1253 controls are either fully or partially addressed by compliant TOEs. This section outlines the requirements that are addressed, and can be used by certification personnel to determine what, if any, additional testing is required when the TOE is incorporated into its operational configuration.

Additionally, as most of the requirements are in place to support implementation of DISA STIG requirements, overall, the requirements can be seen as supporting CM-6, which deals with implementation of configuration settings.

Security Functional Requirements

Base Security Functional Requirements

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects	Comments and Observations
FAU_ALT_EXT.1	**Security Audit** Extended: Agent Alerts • MDM agent provides an alert via the trusted channel to the MDM Server in the event of any of the following: (a) successful application of policies (b) [change in enrollment state, [other events], no other events] • MDM server provides the ability to query for Agent network connectivity status.	**Correspondence is unclear**. There is no directly corresponding control, although it might support AC-3, Access Enforcement. If the alert is provided by the audit mechanism, with the proper assignments, it would support the basic auditable/audited event requirements: AU-2 and AU-12.	
FAU_ALT_EXT.2	**Security Audit** Extended: Server Alerts • MDM server alerts the administrators in the event of (a) change in enrollment status, (b) failure to apply policies, (c) [[other events], no other events]	**No Correspondence.** This does not appear to support or implement any NIST SP 800-53 Rev 4 controls.	

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
FAU_GEN.1.1(1) *Note: This is really only half of FAU_GEN (violating CC rules on splitting components) and it makes changes that are not valid refinements.*	**Security Audit Data Generation** Audit Data Generation • MDM Server generates MDM Server audit records for [*set of events*] that includes startup and shutdown of MDM Server software, all administrative actions, commands issued from the MDM server to an MDM agent, events in Table 7, and [other events].	AC-6(9)	**Least Privilege** | Auditing Use of Privileged Functions • Information system audits the execution of privileged functions.	The auditing aspect of AC-6(9) is satisfied if the assignment in FAU_GEN is completed to include execution of privileged functions.
		AU-2†	**Audit Events ‡** Organization… • Determines system can audit [events] • [⋮] • Determines the following events are to be audited: [events]	FAU_GEN.1.1 gives the definition of what events should be audited (addressing the bulk of this control), but the assignments in AU-2 and AU-12 need to cover at least what is in FAU_GEN.1.1 for the mapping to be valid. Note also that FAU_GEN implies both auditable and audited, which is two distinct controls under 800-53.
FIA_ENR_EXT.1	**Identification and Authentication** Extended: Enrollment of Mobile Device into Management • MDM Server shall authenticate the remote user over a trusted channel during the enrollment of a mobile device.	IA-2	**Identification and Authentication (Organizational Users)** • Information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	IA-2 addresses the authentication of organizational users. It does not appear that non-organizational users would be enrolling devices; if they are, IA-8 would come into play.
		IA-3*	**Device Identification and Authentication** • Information system uniquely identifies and authenticates [*specific and/or types of devices*] before establishing a [*(one or more): local; remote; network*] connection.	Enrollment of a device could be seen as supporting future device identification and authentication.
		IA-5	**Authenticator Management** Organization manages information system authenticators by… • […] • Protecting authenticator content from unauthorized disclosure and modification • […]	Use of a trusted channel supports protection of the authenticator content.
		Note: 800-53 does not have controls that directly address enrollment of mobile devices, or direct requirements that authentication is over a trusted channel other than the requirement that authentication credentials be protected from disclosure.		

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
FMT_MOF.1(1)	**Management of Functions in TSF** Management of Security Functions Behavior - Product restricts the ability to [perform] the functions [(a) listed in SMF.1(1); enable, disable, and modify polices in SMF.1(1); listed in SMF.1(3)] to [authorized administrators].	AC-3	**Access Enforcement** - Information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	This would appear to fall under the general rubric of AC-3, but the system policy would need to match the device policy.
		AC-3(7) †	**Access Enforcement** | Role-Based Access Control - Information system enforces a role-based access control policy over defined subjects and objects and controls access based upon [*roles and users authorized to assume such roles*].	Given that this SFR is restricting functions to a role, this would support a role-based access control policy if there was one in the overall system.
		AC-6	**Least Privilege** - Organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Assigning specific functions to administrators would support a least privilege implementation, depending on the granularity of the privilege.
FMT_MOF.1(2)	**Management of Functions in TSF** Management of Enrollment Function - MDM Server restricts the ability to [initiate] the functions [enrollment process] to [the authorized administrator and MD users].	AC-3	**Access Enforcement** - Information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	This would appear to fall under the general rubric of AC-3, but the system policy would need to match the device policy.
		Note: Given that this includes the administrator and users, it is difficult to argue that this supports role based access control or least privilege.		
FMT_POL_EXT.1	**Trusted Policy Update** Extended: Trusted Policy Update (MDM Agent) - MDM Agent reports successful installation of each policy update to the server.	**No Correspondence**. This does not appear to correspond to or support any NIST SP 800-53r4 control.		
FMT_SMF.1(1)	**Specification of Management Functions** Specification of Management Functions (Server configuration of Agent) - MDM Server is capable of communicating the following commands to the MDM agent: (1) transition to the locked state;	**Note**: The selection of functions dictates the controls addressed – this cannot be determined apriori. Note that many of these functions do not correspond to control as NIST SP 800-53 does not go to that level of detail. Some of the support is noted below:		
		CM-6	**Configuration Settings** Organization… - Establishes and documents configuration settings for information technology	In general, a number of these options would support setting configuration options defined by the DOD in

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
	(2) full wipe of protected data; (3) unenroll from management (4) install policies; (5) query connectivity status; (6) query MD FW/SW version; (7) query hardware version; (8) query application versions; (8) Import X.509v3 certs; (9) Remove X.509v3 certs [*and other certs*] - …and the following commands to the MDM agent [*list of potential commands*] - …and the following MD configuration policies: (21) password policy (22) session locking policy (23) wireless networks to which the MD can connect (24) security policy for each network (25) application installation policy (26) enable/disable policy for A/V devices - …and the following MD configuration policies: [*list of potential policies*].		products employed within the information system using [*security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements; - Implements the configuration settings; - […]	their STIGs.
		AC-11	**Session Lock** Information system… - Prevents further access to the system by initiating a session lock after [*time period*] of inactivity or upon receiving a request from a user - Retains the session lock until the user reestablishes access using established identification and authentication procedures.	Item (1) , *transition to a locked state*, would support this. MD Configuration Item (22), *Session Locking Policy*, supports this control.
		MP-6(8)	**Media Sanitization** | Remote Purging / Wiping of Information - Organization provides the capability to purge/wipe information from [*information systems, system components, or devices*] either remotely or under the following conditions: [*conditions*].	Item (2), *full wipe of protected data*, would support this control.
		IA-5(2)	**Authenticator Management** | PKI-Based Authentication Information system, for PKI-based authentication… - Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; - […]	Items (9) and (10), *dealing with importing and exporting trust anchors*, would support this control. MD configuration item (43), dealing with the trust anchor database, also supports this.
		CM-11	**User-Installed Software** Organization… - Establishes [*policies*] governing the installation of software by users; - Enforces software installation policies through [*methods*]; and	MDM Agent optional items 13, *Remove Enterprise Applications*, 16, *Remove* Applications, and 18, *Install* Applications, would support this control. MD Configuration item

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
			• Monitors policy compliance at [*frequency*].	(25), related to the application installation policy, would also support this control.
		SC-12	**Cryptographic Key Establishment and Management** • Organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	MDM Agent optional items 14 and 15, *importing and removing keys*, would support this control. MD configuration items 44, 45, and 46 would also support this.
		SI-2	**Flaw Remediation** Organization… • […] • Installs security-relevant software and firmware updates within [*time period*] of the release of the updates; • […]	MDM Agent optional item 17, *Update System Software*, would support this control.
		AU-7	**Audit Reduction and Report Generation** Information system provides an audit reduction and report generation capability that: • Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents • Does not alter the original content or time ordering of audit records.	MDM Agent optional item 19, *Read Audit Logs kept by the MD*, would support this control.
		IA-5(1)	**Authenticator Management** | Password-Based Authentication Information system, for password-based authentication… • Enforces minimum password complexity of [*complexity requirements*]; • […] • Enforces password minimum and maximum lifetime restrictions of [*minimum, maximum*];	MD Configuration item (21), *Password Policy*, supports this control.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
			• […]	
		SC-7	**Boundary Protection** Information system… • Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system • Implements subnetworks for publicly accessible system components that are [*physically; logically*] separated from internal organizational networks • Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	MD Configuration Items (23) and (24), which specify the permitted SSIDs and the security policy for each, would seem to support boundary protection rules regarding allowed communications and controlling communications.
		CM-7(5)	**Least Functionality** | Authorized Software / Whitelisting Organization… • Identifies [*software programs authorized to execute on the information system*]; • Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system • Reviews and updates the list of authorized software programs [*frequency*].	MD Configuration item (25), the application installation policy, is effectively a whitelist for allowed applications, and thus supports this control.
		SC-15	**Collaborative Computing Devices** Information system… • Prohibits remote activation of collaborative computing devices with the following exceptions: [*exceptions where remote activation is to be allowed*]; • Provides an explicit indication of use to users physically present at the devices.	MD Configuration item (26), the enable/disable policy for audio/visual devices, would appear to support this control.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
		SC-42	**Sensor Capability and Data** Information system… • Prohibits the remote activation of environmental sensing capabilities with the following exceptions: [*exceptions where remote activation of sensors is allowed*]; • Provides an explicit indication of sensor use to [*class of users*].	MD Configuration item (26), the enable/disable policy for audio/visual devices, would appear to support this control. Configuration of other environmental sensors, such as the GPS sensor, would also support this control.
		SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	A number of the optional MD configuration policies affect transmission confidentiality, and confidentiality using encryption, which would support these controls.
		SC-8(1)	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection • Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	
		CM-7	**Least Functionality** Organization… • Configures the information system to provide only essential capabilities • Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*prohibited or restricted functions, ports, protocols, and/or services*].	The optional MD configuration policy (31), addressing enabling or disabling protocols where the device acts as a server supports ports, protocols, and service restrictions. Policy (41), which addresses cellular protocols, also supports this.
		SC-28	**Protection of Information at Rest** • Information system protects the [*(one or more): confidentiality; integrity*] of [*information at rest*].	The optional MD configuration policy items (32) and (33) address data at rest protections.
		SC-28(1)	**Protection of Information at Rest** | Cryptographic	

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
			Protection • Information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [*information*] on [*information system components*].	
FMT_SMR.1	**Security Management Roles** Security Roles • MDM Server maintains the roles [*authorized identified roles*]. • MDM Server can associate users with roles.	AC-2(7)	**Account Management** | Role-Based Schemes Organization… • Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles • Monitors privileged role assignments • Takes [*actions*] when privileged role assignments are no longer appropriate.	Supporting multiple roles supports use of role-based access schemes.
		AC-3(7)	**Access Enforcement** | Role-Based Access Control • Information system enforces a role-based access control policy over defined subjects and objects and controls access based upon [*roles and users authorized to assume such roles*].	Supporting multiple roles supports a Role-Based policy.
		AC-5	**Separation of Duties** Organization… • Separates [*duties of individuals*] • Documents separation of duties of individuals • Defines information system access authorizations to support separation of duties.	Supporting multiple roles supports separation of duties.
		AC-6	**Least Privilege** • Organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and	Supporting multiple roles supports the principle of least privilege.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
			business functions.	
FPT_ITT.1	**Internal TOE TSF Data Transfer** Basic Internal TSF Data Transfer Protection • MDM Agent and MDM Server protect **all data** from [*disclosure, modification*] through the use of [IPsec, TLS, DTLS] when it is transmitted between the MDM Agent and MDM Server.	IA-5(1) †*	**Authenticator Management** | Password-Based Authentication ‡ Information system, for password-based authentication… • [⋮] • Stores and transmits only encrypted representations of passwords • [⋮]	The SFR supports ensuring that passwords are transmitted encrypted to a distributed component of the product, addressing IA-5(1) item c. FPT_ITT.1 should be completed to specify protection from disclosure, and refined to use encryption. Note that this does not mandate the password itself is encrypted; that requires an explicitly-specified component.
		SC-8	**Transmission Confidentiality and Integrity** Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	To support the control, it must be completed to require both confidentiality and integrity protection.
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection Information system implements cryptographic mechanisms to [*(one or more): prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	To support the control, it must be completed to require both confidentiality and integrity protection.
		SC-13	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	Depending on the completion of SC-13, this would support provision of particular types of cryptography and protocols.

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
FPT_TUD_EXT.1(1)	**Trusted Update** Extended: Trusted Update (MDMServer) • (.1) MDM Server provides authorized users with the ability to query the current version of the MDM Server software	Note: There does not appear to be a control in the 800-53 catalog that corresponds to this SFR.		

MDM Server or Platform Security Functional Requirements

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
FCS_CKM.1(1)	**Cryptographic Key Management** Refinement: Cryptographic Key Generation (Key Establishment) • [MDM Server, MDM Server platform] generates **asymmetric** cryptographic keys **for key establishment** in accordance with [*NIST SP 800-56B, -56A*] and specified cryptographic key sizes [*112 bits*]	SC-12†	**Cryptographic Key Establishment and Management** • Organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	Assignment must be completed congruent with the SFR completion, and the completed control must agree with the completed control in the System Security Plan for the system under analysis.
		SC-12(3)†	**Cryptographic Key Establishment and Management** | Asymmetric Keys • Organization produces, controls, and distributes asymmetric cryptographic keys using [NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key].	FCS_CKM.1(1) calls for asymmetric key in accordance with the NIST process; as NSA developed the PP, it is by implication an NSA-approved technology and process.

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
FCS_CKM.1(2)	**Cryptographic Key Management** Cryptographic Key Generation (Asymmetric Keys for Authentication) [MDM Server, MDM Server platform] generates **asymmetric** cryptographic keys **for key authentication** in accordance with [*FIPS PUB 168-4, ANSI X9.31-1998*] and specified cryptographic key sizes [*112 bits*]	SC-12†	**Cryptographic Key Establishment and Management** - Organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	Assignment must be completed congruent with the SFR completion, and the completed control must agree with the completed control in the System Security Plan for the system under analysis.
		SC-12(3) †	**Cryptographic Key Establishment and Management** | Asymmetric Keys - Organization produces, controls, and distributes asymmetric cryptographic keys using [NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key].	FCS_CKM.1(2) calls for asymmetric key in accordance with the NIST (FIPS) or ANSI process; as NSA developed the PP, it is by implication an NSA-approved technology and process.
FCS_CKM_EXT.2(1)	**Cryptographic Key Storage** Cryptographic Key Storage (MDM Server) [MDM Server, MDM Server Platform] stores persistant secrets and private keys when not in use in [platform key storage, per FCS_STG_EXT.1]	IA-5	**Authenticator Management** Organization manages information system authenticators by… - […] - Protecting authenticator content from unauthorized disclosure and modification - […]	Addresses secure key storage.
		IA-5(1) †*	**Authenticator Management** | Password-Based Authentication ‡ Information system, for password-based authentication… - [⋮] - Stores and transmits only encrypted representations of passwords - [⋮]	Addresses secure key storage.
		SC-12†	**Cryptographic Key Establishment and Management** - Organization establishes and manages cryptographic	Assignment must be completed congruent with the SFR completion, and the completed control must agree with the

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
			keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	completed control in the System Security Plan for the system under analysis.
FCS_CKM_EXT.4(1)	**Cryptographic Key Destruction** Key Destruction • [MDM Server, MDM Server Platform] zeroizes all plaintext secret and private cryptographic keys and CSPs when no longer required.	SC-12†	**Cryptographic Key Establishment and Management** • Organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	Assignment must be completed congruent with the SFR completion, and the completed control must agree with the completed control in the System Security Plan for the system under analysis.
FCS_COP.1(1)	**Cryptographic Operation** Digital Signatures • [MDM Server, MDM Server Platform] performs [***cryptographic signature services***] in accordance with [FIPS PUB 186-4 RSA, ECDSA, DSA] with bit size of [bit size depends on algorithm]	SC-13 †	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	The assignment in the SFR must be completed to include all the cryptographic operations, algorithms, key sizes, and standards specified in the iterations of the FCS_COP.1 SFR.
		AU-10	**Non-Repudiation** • Information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [*actions to be covered by non-repudiation*].	Implementation of digital signatures supports non-repudiation.
FCS_COP.1(2)	**Cryptographic Operation** Keyed Hash Message Authentication • [MDM Server, MDM Server Platform] performs [***keyed-hash message authentication***] in accordance with HMAC-[HMAC SHA selection] and key sizes of [*key* sizes] and message digest sizes [*sizes*] that meet FIPS 198-1 and 180-4	SC-13 †	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	The assignment in the SFR must be completed to include all the cryptographic operations, algorithms, key sizes, and standards specified in the iterations of the FCS_COP.1 SFR.
FCS_COP.1(3)	**Cryptographic Operation** Encryption and Decryption • [MDM Server, MDM Server Platform] performs [***encryption/decryption***] in accordance with [AES-CBC, AES_CCMP, [other]] and [***128*** *and 256*]	SC-13 †	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	The assignment in the SFR must be completed to include all the cryptographic operations, algorithms, key sizes, and standards specified in the iterations of the FCS_COP.1 SFR.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
FCS_COP.1(4)	**Cryptographic Operation** Hashing • [MDM Server, MDM Server Platform] performs [***cryptographic hashing***] in accordance with [SHA selection] and key sizes of [*key* sizes] and message digest sizes [*sizes*] that meet FIPS 180-4	SC-13 †	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	The assignment in the SFR must be completed to include all the cryptographic operations, algorithms, key sizes, and standards specified in the iterations of the FCS_COP.1 SFR.
FCS_RBG_EXT.1(1)	**Random Bit Generation** Random Bit Generation • [MDM Server, MDM Server Platform] performs all deterministic random big generation in accordance with [NIST SP 800-90A algorithms, FIPS 140-2 Annex C algorithms] • Product seeds the algorithm by an entropy source that …	Note: Unclear. This might fit within SC-12 and key generation, but it could also be below the level of any existing NIST control.		
FIA_UAU.1	**User Authentication** Timing of Authentication • [MDM Server, MDM Server Platform] allows [*MDM-server mediated actions*] on behalf of the user to be performed before the user is authenticated **with the server**. • [MDM Server, MDM Server Platform] requires each user to be successfully authenticated **with the server** before allowing any other **MDM-server-**mediated actions on behalf of that user.	AC-14	**Permitted Actions without Identification or Authentication** Organization… • Identifies [*user actions*] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions • Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.	The identification of the actions in FIA_UAU.1.1 supports identification of the actions for AC-14. AC-14 goes beyond FIA_UAU in that it requires rationale for each permitted action. The assignments must be congruent between FIA_UAU and AC-14. **Note:** FIA_UAU addresses AC-14 only for the particular evaluated product. AC-14 must still be considered in an overall system context.
		IA-2	**Identification and Authentication (Organizational Users)** • Information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	FIA_UAU supports IA-2, which addresses the authentication of organizational users.
		IA-8	**Identification and Authentication (Non-Organizational Users)** • Information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	FIA_UAU supports IA-8, which addresses the authentication of non-organizational users.

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
		Note: NIST SP 800-53 does not explicitly require that identification and authentication must occur before other actions are permitted. The requirement is only implied through AC-14 specifying what can be done without identification and authentication; this creates the implication that any other action requires identification and authentication.		
FIA_X509_EXT.1(1)	**Validation of Certificates** X509 Validation • [MDM Server, MDM Server Platform] validates certificates in accordance with the following rules… • …validate the revocation status of the certificate using… • …validate the extendedKeyUsage field…	IA-5(2)	**Authenticator Management** | PKI-Based Authentication Information system, for PKI-based authentication… • Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; • […] • Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.	Addresses the certificate validation portion of IA-5(2).**Note that this does not address all of IA-5(2).**
FIA_X509_EXT.2(1)	**Validation of Certificates** X509 Validation • [MDM Server, MDM Server Platform] uses X.509 certificates as defined by RFC 5280 to support authentication for [*IPSec, TLS, HTTPS, DTLS*] and [*code signing for software updates, code signing for integrity verification, policy signing, no additional uses*]	IA-3†	**Device Identification and Authentication** • Information system uniquely identifies and authenticates [*specific and/or types of devices*] before establishing a [*(one or more): local; remote; network*] connection.	This would address use of X.509 certificates for device identification.
		IA-5(2)	**Authenticator Management** | PKI-Based Authentication Information system, for PKI-based authentication… • […] • Maps the authenticated identity to the account of the individual or group; • […]	This addresses mapping the authenticated identity. **Note that this does not address all of IA-5(2)**.
		CM-5(3)	**Access Restrictions for Change** | Signed Components • Information system prevents the installation of [*software and firmware components*] without verification that the component has been digitally signed using a certificate that is recognized and approved	This SFR supports CM-5(3) if code signing is selected.

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
			by the organization.	
		AU-10	**Non-Repudiation** - Information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [*actions to be covered by non-repudiation*].	Implementation of digital signatures supports non-repudiation.
FPT_TST_EXT.1(1)	**TSF Functionality Testing** TSF Testing - [MDM Server, MDM Server Platform] runs a suite of self-tests [during initial start-up] to demonstrate the correct operation of the MDM server. - [MDM Server, MDM Server Platform] provides the capability to verify the integrity of the stored MDM Server executable code when it is loaded for execution through the use of the [MDM Server, MDM Server Platform]-provided cryptographic services	SI-6	**Security Function Verification** Information system… - Verifies the correct operation of [*security functions*]; - Performs this verification [(*one or more): [system transitional states]; upon command by user with appropriate privilege; [frequency]*]; - […]	The SFR addresses the testing and when it is performed.
		SI-7†	**Software, Firmware, and Information Integrity** - Organization employs integrity verification tools to detect unauthorized changes to [*software, firmware, and information*].	Addresses the verification aspect.
		SI-7(6)	**Software, Firmware, and Information Integrity** | Cryptographic Protection - Information system implements cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.	Addresses the use of digital signatures or hashes
FPT_TUD_EXT.1(1)	**Trusted Update** Extended: Trusted Update (MDMServer) - (.1) See base SFR	Note: There does not appear to be a control in the 800-53 catalog that corresponds to this SFR.		
	- (.2) [MDM Server, MDM Server Platform] provides Authorized Administrators the ability to initiate updates to the MDM Server software - (.3) [MDM Server, MDM Server Platform] provides a means to verify software updates to the MDM Server using a digital signature mechanism prior to installing those updates.	SI-2	**Flaw Remediation** Organization… - Identifies, reports, and corrects information system flaws; - […] - Installs security-relevant software and firmware updates within [*time period*] of the release of the updates; - […]	The ability to initiate updates supports the ability to install updates.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
		SI-2(1)	**Flaw Remediation** | Central Management • Organization centrally manages the flaw remediation process.	The ability to remotely install updates supports central management.
		CM-5(3)	**Access Restrictions for Change** | Signed Components • Information system prevents the installation of [*software and firmware components*] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.	Supported by verification of the digital signature of updates.
FTP_TRP.1	**Trusted Path** Trusted Path • [MDM Server, MDM Server Platform] **shall use [IPsec, TLS, TLS/HTTPS] to** provides a communication path between itself and [*remote*] **administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [disclosure and detection of modification of the communicated data]. • [MDM Server, MDM Server Platform] permits [*remote administrators*] to initiate communication via the trusted path. • [MDM Server, MDM Server Platform] requires the use of the trusted path for [*all remote administrator actions*].	SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	Supports SC-8 for confidentiality and integrity.
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection • Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	The protocols cited provide the cryptographic implementation.
		SC-11†	**Trusted Path** • Information system establishes a trusted communications path between the user and the following security functions of the system: [*security functions to include at a minimum, information system authentication and re-authentication*].	Support of the SC-11 control depends on the completion of the assignments in the SFR.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
		SC-11(1) †*	**Trusted Path** | Logical Isolation • Information system provides a trusted communications path that is logically isolated and distinguishable from other paths.	SC-11(1) addresses the "logically distinct" aspect.
		SC-23 *	**Session Authenticity** • Information system protects the authenticity of communications sessions.	The normal use of trusted path provides identification of the endpoints, supporting session authenticity.
FTP_TRP.2 (Note: CC Part 2 does not define a FTP_TRP.2; this should have been FTP_TRP.1(2)	**Trusted Path** Trusted Path • [MDM Server, MDM Server Platform] **shall use [TLS, TLS/HTTPS] to** provides a communication path between itself and **MD Users** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [disclosure and detection of modification of the communicated data]. • [MDM Server, MDM Server Platform] permits **MD users** to initiate communication via the trusted path. • [MDM Server, MDM Server Platform] requires the use of the trusted path for **all MD user actions**.	SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	Supports SC-8 for confidentiality and integrity.
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection • Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	The protocols cited provide the cryptographic implementation.
		SC-11†	**Trusted Path** • Information system establishes a trusted communications path between the user and the following security functions of the system: [*security functions to include at a minimum, information system authentication and re-authentication*].	Support of the SC-11 control depends on the completion of the assignments in the SFR.
		SC-11(1) †*	**Trusted Path** | Logical Isolation • Information system provides a trusted communications path that is logically isolated and distinguishable from other paths.	SC-11(1) addresses the "logically distinct" aspect.
		SC-23 *	**Session Authenticity** • Information system protects	The normal use of trusted path provides

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
			the authenticity of communications sessions.	identification of the endpoints, supporting session authenticity.

MDM Agent or Platform Security Functional Requirements

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
FCS_CKM.1(3)	**Cryptographic Key Management** Refinement: Cryptographic Key Generation (Key Establishment) • [MDM Agent, MDM Agent Platform] generates **asymmetric** cryptographic keys **for key establishment** in accordance with [*NIST SP 800-56B, -56A*] and specified cryptographic key sizes [*112 bits*]	SC-12†	**Cryptographic Key Establishment and Management** • Organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	Assignment must be completed congruent with the SFR completion, and the completed control must agree with the completed control in the System Security Plan for the system under analysis.
		SC-12(3)†	**Cryptographic Key Establishment and Management** | Asymmetric Keys • Organization produces, controls, and distributes asymmetric cryptographic keys using [*NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key*].	FCS_CKM.1(1) calls for asymmetric key in accordance with the NIST process; as NSA developed the PP, it is by implication an NSA-approved technology and process.
FCS_CKM_EXT.2(2)	**Cryptographic Key Storage** Cryptographic Key Storage (MDM Agent) [MDM Agent, MDM Agent Platform] stores persistant secrets and private keys when not in use in [platform key storage]	IA-5	**Authenticator Management** Organization manages information system authenticators by… • […] • Protecting authenticator content from unauthorized	Addresses secure key storage.

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
			disclosure and modification - […]	
		IA-5(1) †*	**Authenticator Management** | Password-Based Authentication ‡ Information system, for password-based authentication… - [⁝] - Stores and transmits only encrypted representations of passwords - [⁝]	Addresses secure key storage.
		SC-12†	**Cryptographic Key Establishment and Management** - Organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	Assignment must be completed congruent with the SFR completion, and the completed control must agree with the completed control in the System Security Plan for the system under analysis.
FCS_CKM_EXT.4(2)	**Cryptographic Key Destruction** Key Destruction - [MDM Agent, MDM Agent Platform] zeroizes all plaintext secret and private cryptographic keys and CSPs when no longer required.	SC-12†	**Cryptographic Key Establishment and Management** - Organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	Assignment must be completed congruent with the SFR completion, and the completed control must agree with the completed control in the System Security Plan for the system under analysis.
FCS_COP.1(5)	**Cryptographic Operation** Digital Signatures - [MDM Agent, MDM Agent Platform] performs [***cryptographic signature services***] in accordance with [FIPS PUB 186-4 RSA, ECDSA, DSA] with bit size of [bit size depends on algorithm]	SC-13 †	**Cryptographic Protection** - Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	The assignment in the SFR must be completed to include all the cryptographic operations, algorithms, key sizes, and standards specified in the iterations of the FCS_COP.1 SFR.
		AU-10	**Non-Repudiation** - Information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [*actions to be covered by non-repudiation*].	Implementation of digital signatures supports non-repudiation.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
FCS_COP.1(6)	**Cryptographic Operation** Keyed Hash Message Authentication • [MDM Agent, MDM Agent Platform] performs [***keyed-hash message authentication***] in accordance with HMAC-[HMAC SHA selection] and key sizes of [*key* sizes] and message digest sizes [*sizes*] that meet FIPS 198-1 and 180-4	SC-13 †	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	The assignment in the SFR must be completed to include all the cryptographic operations, algorithms, key sizes, and standards specified in the iterations of the FCS_COP.1 SFR.
FCS_COP.1(7)	**Cryptographic Operation** Encryption and Decryption • [MDM Agent, MDM Agent Platform] performs [***encryption/decryption***] in accordance with [AES-CBC, AES_CCMP, [other]] and [***128** and 256*]	SC-13 †	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	The assignment in the SFR must be completed to include all the cryptographic operations, algorithms, key sizes, and standards specified in the iterations of the FCS_COP.1 SFR.
FCS_COP.1(8)	**Cryptographic Operation** Hashing • [MDM Agent, MDM Agent Platform] performs [***cryptographic hashing***] in accordance with [SHA selection] and key sizes of [*key* sizes] and message digest sizes [*sizes*] that meet FIPS 180-4	SC-13 †	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	The assignment in the SFR must be completed to include all the cryptographic operations, algorithms, key sizes, and standards specified in the iterations of the FCS_COP.1 SFR.
FCS_RBG_EXT.1(2)	**Random Bit Generation** Random Bit Generation • [MDM Agent, MDM Agent Platform] performs all deterministic random big generation in accordance with [NIST SP 800-90A algorithms, FIPS 140-2 Annex C algorithms] • Product seeds the algorithm by an entropy source that …	Note: Unclear. This might fit within SC-12 and key generation, but it could also be below the level of any existing NIST control.		
FIA_X509_EXT.1(2)	**Validation of Certificates** X509 Validation • [MDM Agent, MDM Agent Platform] validates certificates in accordance with the following rules… • …validate the revocation status of the certificate using… • …validate the extendedKeyUsage field…	IA-5(2)	**Authenticator Management** | PKI-Based Authentication Information system, for PKI-based authentication… • Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; • […] • Implements a local cache of revocation data to support path discovery and validation in case of inability to access	Addresses the certificate validation portion of IA-5(2).**Note that this does not address all of IA-5(2).**

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
			revocation information via the network.	
FIA_X509_EXT.2(2)	**Validation of Certificates** X509 Validation • [MDM Agent, MDM Agent Platform] uses X.509 certificates as defined by RFC 5280 to support authentication for [*IPSec, TLS, HTTPS, DTLS*] and [*code signing for software updates, code signing for integrity verification, policy signing, no additional uses*]	IA-3†	**Device Identification and Authentication** • Information system uniquely identifies and authenticates [*specific and/or types of devices*] before establishing a [*(one or more): local; remote; network*] connection.	This would address use of X.509 certificates for device identification.
		IA-5(2)	**Authenticator Management** | PKI-Based Authentication Information system, for PKI-based authentication… • […] • Maps the authenticated identity to the account of the individual or group; • […]	This addresses mapping the authenticated identity. **Note that this does not address all of IA-5(2)**.
		CM-5(3)	**Access Restrictions for Change** | Signed Components • Information system prevents the installation of [*software and firmware components*] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.	This SFR supports CM-5(3) if code signing is selected.
		AU-10	**Non-Repudiation** • Information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [*actions to be covered by non-repudiation*].	Implementation of digital signatures supports non-repudiation.
FPT_TST_EXT.1(2)	**TSF Functionality Testing** TSF Testing • [MDM Agent, MDM Agent Platform] runs a suite of self-tests [during initial start-up] to demonstrate the correct operation of the MDM Agent. • [MDM Agent, MDM Agent	SI-6	**Security Function Verification** Information system… • Verifies the correct operation of [*security functions*]; • Performs this verification [*(one or more): [system*	The SFR addresses the testing and when it is performed.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
	Platform] provides the capability to verify the integrity of the stored MDM Agent executable code when it is loaded for execution through the use of the [MDM Agent, MDM Agent Platform]-provided cryptographic services		*transitional states]; upon command by user with appropriate privilege; [frequency]*]; • […]	
		SI-7†	**Software, Firmware, and Information Integrity** • Organization employs integrity verification tools to detect unauthorized changes to [*software, firmware, and information*].	Addresses the verification aspect.
		SI-7(6)	**Software, Firmware, and Information Integrity** | Cryptographic Protection • Information system implements cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.	Addresses the use of digital signatures or hashes

Security Assurance Requirements

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
ASE_*	**Security Target Requirements**	PL-2	**System Security Plan ‡** Organization… • Develops a security plan for the information system that: 1. [⋮] 6. Provides an overview of the security requirements for the system; 7. [⋮] 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions;	Supports this.

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
			9. [⋮] • [⋮]	
		SA-4	**Acquisition Process ‡** Organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service […]: a. Security functional requirements; b. Security strength requirements; c. Security assurance requirements; d. Security-related documentation requirements; e. Requirements for protecting security-related documentation; f. Description of the information system development environment and environment in which the system is intended to operate; and g. Acceptance criteria.	
		SA-4(7)	**Acquisition Process |** NIAP-Approved Protection Profiles Organization… • Limits the use of commercially provided information assurance (IA) and IA-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists; • Requires, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security	

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
			policy, that the cryptographic module is FIPS-validated.	
ADV_FSP.1	**Functional Specification** Security-Enforcing Functional Specification - Developer provides a functional specification and a tracing from the functional specification to the SFRs. - Functional specification: 1. Describe the purpose and method of use for each SFR-enforcing and SFR-supporting interface. 2. Identifies all parameters associated with each SFR-enforcing and SFR-supporting interface. 3. Provides rationale for the implicit categorisation of interfaces as SFR-non-interfering. - Tracing demonstrates that the SFRs trace to interfaces in the functional specification. - Evaluator confirms that the information provided meets all requirements for content and presentation of evidence. - Evaluator determines that the functional specification is an accurate and complete instantiation of the SFRs.	SA-4(1)	**Acquisition Process** | Functional Properties of Security Controls - Organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.	The ADV_FSP family provides information about functional interfaces. The SA-4(1) control requires describing the functionality (i.e., security capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.
		SA-4(2)	**Acquisition Process** | Design / Implementation Information for Security Controls - Organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [*(one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [design/implementation information]*] at [*level of detail*].	The ADV_FSP family provides information about functional interfaces. The SA-4(2) control requires design and implementation information; it should be completed to require them at the level of the security-relevant external system interfaces. **Note**: There is no requirement that requires separation of interfaces into security-enforcing, security non-enforcing, security non-interfering, etc.
AGD_OPE.1	**Operational User Guidance** Operational User Guidance - Developer provides operational user guidance. - Operational user guidance: 1. Describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. 2. Describes, for each user role,	SA-5	**Information System Documentation‡** Organization… - Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and	AGD_OPE is the combined requirement for administrator and user documentation.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
	how to use the available interfaces provided by the product in a secure manner. 3. Describes, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate. 4. For each user role, clearly presents each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the product. 5. Identifies all possible modes of operation of the product (including operation following failure or operational error), their consequences and implications for maintaining secure operation. 6. For each user role, describes the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST. 7. Is written to be clear and reasonable. - Evaluator confirms that the information provided meets all requirements for content and presentation of evidence.		maintenance of security functions/mechanisms; 3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; - Obtains user documentation for the information system, system component, or information system service that describes: 1. User-accessible security functions/mechanisms and how to effectively use those security functions / mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; 3. User responsibilities in maintaining the security of the system, component, or service; - [⁝]	
		Note: NIST SP 800-53 parallels the CC v2 approach, which distinguished administrator and user documentation (AGD_USR, AGD_ADM). CC v3 combined these into a single SAR, reflecting the situation that some products do not have non-administrative users.		
AGD_PRE.1	**Preparative Procedures** Preparative Procedures - Developer provides the product including its preparative procedures. - Preparative procedures: 1. Describe all the steps necessary for secure acceptance of the delivered product in accordance with the developer's delivery procedures. 2. Describe all the steps necessary for secure installation of the product and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as	SA-5	**Information System Documentation ‡** Organization… - Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. [⁝] - [⁝]	AGD_PRE.1 calls for describing all the steps necessary for secure acceptance and secure delivery. The control calls for documentation or secure configuration and installation.

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
	described in the ST. • Evaluator confirms that the information provided meets all requirements for content and presentation of evidence. • Evaluator applies the preparative procedures to confirm that the product can be prepared securely for operation.			
ALC_CMC.1	**CM Capabilities** Labeling of the TOE • Developer provides the product and a reference for the product. • The product is labelled with its unique reference. • Evaluator confirms that the information provided meets all requirements for content and presentation of evidence.	CM-9	**Configuration Management Plan ‡** Organization develops, documents, and implements a configuration management plan for the information system that… • [⋮] • Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; • [⋮]	At the product level, identification of the configuration items would include identification of the product with a unique reference.
ALC_CMS.1	**CM Scope** TOE CM Coverage • Developer provides a configuration list for the TOE. • Configuration list includes the following: the TOE itself; and the evaluation evidence required by the SARs. • Configuration list uniquely identifies the configuration items. • Evaluator confirms that the information provided meets all requirements for content and presentation of evidence.	CM-3(6)*	**Configuration Change Control** | Cryptography Management • Organization ensures that cryptographic mechanisms used to provide [*security safeguards*] are under configuration management.	At the product level, if the cryptographic mechanisms providing the safeguards are part of the TOE, they would be covered by CM.
		CM-9	**Configuration Management Plan ‡** Organization develops, documents, and implements a configuration management plan for the information system that… • [⋮] • Defines the configuration items for the information system and places the configuration items under configuration management;. • [⋮]	This addresses defining the configuration items and the CM system. Note that ALC_CMC focuses on the *product*, whereas CM-9 focuses on the *system.*
		SA-10	**Developer Configuration Management ‡** Organization requires the developer of the information system, system component, or information system service to: • […] • Document, manage, and	ALC_CMS captures the "[*configuration items under configuration management*]"

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
			control the integrity of changes to [*configuration items under configuration management*]; • [⋮]	
		Note: This is a *developer* process – a missing area in SA. Installation of remediated flaws is SI-2.		
ATE_IND.1	**Independent Testing** Independent Testing – Conformance • Developer provides the product for testing. • The product shall be suitable for testing. • Evaluator confirms that the information provided meets all requirements for content and presentation of evidence. • Evaluator tests a subset of the TSF to confirm that the TSF operates as specified.	CA-2	**Security Assessments** Organization… • Develops a security assessment plan that describes the scope of the assessment including: (1) Security controls and control enhancements under assessment; (2) Assessment procedures to be used to determine security control effectiveness; and (3) Assessment environment, assessment team, and assessment roles and responsibilities; • Assesses the security controls in the information system and its environment of operation [*frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; • Produces a security assessment report that documents the results of the assessment • Provides the results of the security control assessment to [*individuals or roles*].	Independent testing *at the product level* supports testing of the overall system. As such, the *product-level* test plan can support the system-level test plans in terms of eliminating test redundancy, and the results of testing can feed into the system results.
		CA-2(1)	**Security Assessments** | Independent Assessors • Organization employs assessors or assessment teams with [*level of independence*] to conduct security control assessments.	Assessment teams for ATE_IND are drawn from NIAP-approved CCTLs that are independent from the developer. However, the CCTLs may not meet the *level of independence* dictated by the SCA.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
AVA_VAN.1	**Vulnerability Analysis** Vulnerability Survey • Developer provides the product for testing. • The product is suitable for testing. • Evaluator confirms that the information provided meets all requirements for content and presentation of evidence. • Evaluator performs a search of public domain sources to identify potential vulnerabilities in the product. • Evaluator conducts penetration testing, based on the identified potential vulnerabilities, to determine that the product is resistant to attacks performed by an attacker possessing Basic attack potential.	CA-2(2)	**Security Assessments** | Specialized Assessments • Organization includes as part of security control assessments, [*frequency*], [*announced; unannounced*], [(*one or more*): *in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; [other forms of security assessment]*].	If the assignment in CA-2(2) is completed to include a public domain search and subsequent testing of any potential vulnerabilities identified, then AVA_VAN.1 addresses CA-2(2) *at the product level*. **Note:** Vulnerability testing at the product level does not ensure the product integrated into the complete system is configured correctly, nor does it ensure there are no other integration flaws.

Optional Requirements

Optional TSF Requirements

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
FAU_SEL.1(1)	**Security Audit Event Selection** Selective Audit (MDM Server) • MDM Server can select the events to be audited from the set of auditable events based on (a) event type; (b) success of events; (c) failure of events; (d) [*attributes*]	AU-12	**Audit Generation** Information system… • Provides audit record generation capability for the auditable events defined in AU-2 a. at [*components*]; • Allows [*personnel or roles*] to select which auditable events are to be audited by specific components of the information system • Generates audit records for the events defined in AU-2 d. with the content defined	AU-12 item b. allows specific roles to select what will be audited fro the set of auditable events, but it does not do it based on particular attributes. It would satisfy selection based on event type.

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
			in AU-3.	

Optional MDM Server or MDM Server Platform Requirements

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
FAU_SAR.1	**Security Audit Review** Audit Review • [MDM Server, MDM Server platform] provides [*authorized administrators*] with the ability to read [*all audit data*] from audit records. • [MDM Server, MDM Server platform] provides audit records in a manner suitable for the Authorized Administrators to interpret the information.	AU-6(7)	**Audit Review, Analysis, and Reporting** | Permitted Actions • Organization specifies the permitted actions for each [*process; role; user*] associated with the review, analysis, and reporting of audit information.	Supports AU-6(7) restricting access to audit administrators.
		AU-7	**Audit Reduction and Report Generation** Information system provides an audit reduction and report generation capability that: • Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents • Does not alter the original content or time ordering of audit records.	Supports provision of the AU-7 audit reduction and report capability.
		AU-9	**Protection of Audit Information** • Information system protects audit information and audit tools from unauthorized access, modification, and deletion	Supports AU-9 protection of audit information from unauthorized access, modification, or deletion. The restriction to read access would address this. There is an implication that users not listed in FAU_SAR.1 are not authorized to read audit records.
		AU-9(6)	**Protection of Audit Information** | Read-Only Access • Organization authorizes read-only access to audit information to [*privileged*	AU-9(6) authorizes read-only access to a specific list of users.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
			users].	
FAU_STG_EXT.2	**Security Audit Event Storage** Audit Event Storage • [MDM Server, MDM Server platform] protects stored audit records from unauthorized modification.	AU-9	**Protection of Audit Information** • Information system protects audit information and audit tools from unauthorized access, modification, and deletion	Supports AU-9, which requires that audit information is protected "from unauthorized access, modification, and deletion ".However, the AU-9 control goes beyond the SFR to protect not only the audit trail, but also audit tools.

Selection-Based Requirements

Selection-Based TSF Requirements

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
FCS_IV_EXT.1(1)	**Cryptographic Support** Extended: Initialization Vector Generalization • MDM server generates IV in accordance with Table 9	Note: Unclear. This might fit within SC-12 and key generation, but it could also be below the level of any existing NIST control.		
FCS_STG_EXT.1	**Cryptographic Key Storage** Encrypted Cryptographic Key Storage (MDM Server) • MDM Server encrypts all keys using AES in the [*mode*]	SC-12†	**Cryptographic Key Establishment and Management** • Organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	Assignment must be completed congruent with the SFR completion, and the completed control must agree with the completed control in the System Security Plan for the system under analysis.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
		IA-5	**Authenticator Management** Organization manages information system authenticators by… • […] • Protecting authenticator content from unauthorized disclosure and modification • […]	Addresses secure key storage.
		IA-5(1) †*	**Authenticator Management** | Password-Based Authentication ‡ Information system, for password-based authentication… • [⋮] • Stores and transmits only encrypted representations of passwords • [⋮]	Addresses secure key storage.

Selection-Based MDM Server or MDM Server Platform Requirements

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
FCS_DTLS_EXT.1(1)	**DTLS Implementation** DTLS Implementation • [MDM Server, MDM Server Platform] implements DTLS protocol in accordance with DTLS 1.0, DTLS 1.2 • [MDM Server, MDM Server Platform] implements requirements in TLS for the DTLS implementation…	SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	The assignment in SC-8 should be completed to correspond with the requirement for protection from disclosure / modification in the SFR.
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection • Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	Whether this control is satisfied depends on the implementation method for meeting the SFR. At the SFR level, this can be addressed either through refinement of the SFR, or through appropriate specifications in the TSS that would indicated FDP_ITT is implemented through FCS operations.

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
		SC-13 †	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	This would specific the specific encryption approaches fo r DTLS.
		SC-23 †	**Session Authenticity** • Information system protects the authenticity of communications sessions.	DTLS is used for communication sessions.
FCS_HTTPS_EXT.1(1)	**HTTPS Implementation** HTTPS Implementation • [MDM Server, MDM Server Platform] implements HTTPS protocol in accordance with RFC 2818 • [MDM Server, MDM Server Platform] implements HTTPS using TLS	SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [(*one or more): confidentiality; integrity*] of transmitted information.	The assignment in SC-8 should be completed to correspond with the requirement for protection from disclosure / modification in the SFR.
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	Use of HTTPS supports SC-8(1)
		SC-13 †	**Cryptographic Protection** Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	This would specific the specific encryption approaches for HTTPS.
		SC-23 †	**Session Authenticity** Information system protects the authenticity of communications sessions.	HTTPS is used for communication sessions.
FCS_IPSEC_EXT.1(1)	**IPSEC Communications** IPSEC Communications • (.1) [MDM Server, MDM Server Platform] implements IPSEC protocol in accordance with RFC 4301 • (.2) [MDM Server, MDM Server Platform] implements [*tunnel mode and/or transport mode*]	AC-3(7) †	**Access Enforcement** | Role-Based Access Control • Information system enforces a role-based access control policy over defined subjects and objects and controls access based upon [*roles and users authorized to assume such*	Given that this SFR is restricting functions to a role, this would support a role-based access control policy if there was one in the overall system.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
	• (.6) [MDM Server, MDM Server Platform] ensures the encrypted payload in the [IKEv1, IKEv2] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256, and [AES-GCM-alsos] • (.7) [MDM Server, MDM Server Platform] ensures that IKEv1 Phase 1 exchanges only use main mode. • (.8) [MDM Server, MDM Server Platform] ensures that [IKEv2 SA lifetimes can be configured by an Authorized Administrators based one …] • (.9) [MDM Server, MDM Server Platform] generates the secret value x used … using the random bit generator… • (.10) [MDM Server, MDM Server Platform] generates nonces use in IKE exchanges …. • (.11) [MDM Server, MDM Server Platform] ensures all IKE protocols implement DH Groups 14… • (.12) [MDM Server, MDM Server Platform] ensures all IKE protocols perform peer authentication using… • (.13) [MDM Server, MDM Server Platform] does not establish an SA if the DN contained in a certificate does not match the expected DN… • (.14) [MDM Server, MDM Server Platform] ensures by default that the strength of the symmetric algorithm…		*roles*].	
		AC-6	**Least Privilege** • Organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Restricting activities to authorized administrators supports this.
		IA-5(2)	**Authenticator Management** | PKI-Based Authentication Information system, for PKI-based authentication… • Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; • Enforces authorized access to the corresponding private key; • Maps the authenticated identity to the account of the individual or group; • Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.	The checking of the DN may support this.
		SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	The assignment in SC-8 should be completed to correspond with the requirement for protection from disclosure / modification in the SFR.
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless	Use of IPSEC supports SC-8(1)

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
			otherwise protected by [*alternative physical safeguards*].	
		SC-12	**Cryptographic Key Establishment and Management** • Organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	Some of the specific crypto requirements support this control.
		SC-12(2)	**Cryptographic Key Establishment and Management** | Symmetric Keys • Organization produces, controls, and distributes symmetric cryptographic keys using [*NIST FIPS-compliant; NSA-approved*] key management technology and processes.	The SFR supports this control through the approaches used for symmetric key distribution.
		SC-13 †	**Cryptographic Protection** Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	This would specific the specific encryption approaches.
		SC-23 †	**Session Authenticity** Information system protects the authenticity of communications sessions.	IPSEC is used for communication sessions.
FCS_SSH_EXT.1	**SSH Implementation** SSH Implementation • [MDM Server, MDM Server Platform] implements SSH protocol in accordance with RFCs 4251… • [MDM Server, MDM Server Platform] ensures the SSH protocol supports the following authentication methods: public key based, password based • [MDM Server, MDM Server Platform] ensures that packets greater than [*bytes*] bytes are dropped • [MDM Server, MDM Server Platform] ensures that the SSH	IA-2	**Identification and Authentication (Organizational Users)** • Information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	The requirement to support password or PKI authentication supports IA-2 and IA-8
		IA-8	**Identification and Authentication (Non-Organizational Users)** • Information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational	The requirement to support password or PKI authentication supports IA-2 and IA-8

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
	transport implementation uses the following encryption algorithms… • [MDM Server, MDM Server Platform] ensures that SSH transport implementation uses SSH_RSA and … as its public key algorithms • [MDM Server, MDM Server Platform] ensures that data integrity algorithms used in the SSH transport connection is …		users).	
		SC-5	**Denial of Service Protection** • Information system protects against or limits the effects of the following types of denial of service attacks: [*types of denial of service attacks*] by employing [*security safeguards*].	The requirement to drop packets larger than a certain size protects against denial of service.
		SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	The assignment in SC-8 should be completed to correspond with the requirement for protection from disclosure / modification in the SFR.
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	Use of SSH supports SC-8(1)
		SC-13 †	**Cryptographic Protection** Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	This would specific the specific encryption approaches for SSH.
		SC-23 †	**Session Authenticity** Information system protects the authenticity of communications sessions.	SSH is used for communication sessions.
FCS_TLS_EXT.2	**TLS Implementation** TLS Implementation • [MDM Server, MDM Server Platform] implements one or more of TLS 1.2, TLS 1.0, TLS 1.1 with the following cyphersuites [list] • [MDM Server, MDM Server Platform] does not establish a trusted channel if the DN contained in a certificate does not match the expected DN	SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	The assignment in SC-8 should be completed to correspond with the requirement for protection from disclosure / modification in the SFR.
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection	Whether this control is satisfied depends on the implementation method for meeting the SFR. At the SFR level, this can

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
			• Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	be addressed either through refinement of the SFR, or through appropriate specifications in the TSS that would indicated FDP_ITT is implemented through FCS operations.
		SC-13 †	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	This would specific the specific encryption approaches fo r TLS.
		SC-23 †	**Session Authenticity** • Information system protects the authenticity of communications sessions.	TLS is used for communication sessions.
		Note: The second part of the SFR does not correspond to an 800-53 control.		
FIA_X509_EXT,2(1)	**X509 Authenticaion** X509 Authenticaion • (.1) [MDM Server, MDM Server Platform] shall not [install, execute] code if the code signing certificate is invalid.	CM-5(3)	**Access Restrictions for Change** | Signed Components • Information system prevents the installation of [*software and firmware components*] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.	This SFR supports CM-5(3) if code signing is selected.

Selection-Based MDM Agent or MDM Agent Platform Requirements

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
FCS_DTLS_EXT.1(2)	**DTLS Implementation** DTLS Implementation • [MDM Agent, MDM Agent Platform] implements DTLS protocol in accordance with	SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of	The assignment in SC-8 should be completed to correspond with the requirement for protection from disclosure / modification

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
	DTLS 1.0, DTLS 1.2 • [MDM Agent, MDM Agent Platform] implements requirements in TLS for the DTLS implementation…		transmitted information.	in the SFR.
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection • Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	Whether this control is satisfied depends on the implementation method for meeting the SFR. At the SFR level, this can be addressed either through refinement of the SFR, or through appropriate specifications in the TSS that would indicated FDP_ITT is implemented through FCS operations.
		SC-13 †	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	This would specific the specific encryption approaches fo r DTLS.
		SC-23 †	**Session Authenticity** • Information system protects the authenticity of communications sessions.	DTLS is used for communication sessions.
FCS_HTTPS_EXT.1(2)	**HTTPS Implementation** HTTPS Implementation • [MDM Agent, MDM Agent Platform] implements HTTPS protocol in accordance with RFC 2818 • [MDM Agent, MDM Agent Platform] implements HTTPS using TLS	SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	The assignment in SC-8 should be completed to correspond with the requirement for protection from disclosure / modification in the SFR.
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	Use of HTTPS supports SC-8(1)
		SC-13 †	**Cryptographic Protection** Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance	This would specific the specific encryption approaches for HTTPS.

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
			with applicable federal laws … and standards.	
		SC-23 †	**Session Authenticity** Information system protects the authenticity of communications sessions.	HTTPS is used for communication sessions.
FCS_IPSEC_EXT.1(2)	**IPSEC Communications** IPSEC Communications - (.1) [MDM Agent, MDM Agent Platform] implements IPSEC protocol in accordance with RFC 4301 - (.2) [MDM Agent, MDM Agent Platform] implements [*tunnel mode and/or transport mode*] - (.3) [MDM Agent, MDM Agent Platform] has a nominal final entry in the SPD that matches anything… - (.4) [MDM Agent, MDM Agent Platform] implements IPsec ESP as defined by RFC 4303 using the cryptographic algorithms … - (.5) [MDM Agent, MDM Agent Platform] implements the protocol [IKEv1 as defined in RFC 2407…[… - (.6) [MDM Agent, MDM Agent Platform] ensures the encrypted payload in the [IKEv1, IKEv2] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256, and [AES-GCM-alsos] - (.7) [MDM Agent, MDM Agent Platform] ensures that IKEv1 Phase 1 exchanges only use main mode. - (.8) [MDM Agent, MDM Agent Platform] ensures that [IKEv2 SA lifetimes can be configured by an Authorized Administrators based one …] - (.9) [MDM Agent, MDM Agent Platform] generates the secret value x used … using the random bit generator… - (.10) [MDM Agent, MDM Agent Platform] generates nonces use in IKE exchanges …. - (.11) [MDM Agent, MDM Agent Platform] ensures all IKE protocols implement DH Groups 14…	AC-3(7) †	**Access Enforcement** | Role-Based Access Control - Information system enforces a role-based access control policy over defined subjects and objects and controls access based upon [*roles and users authorized to assume such roles*].	Given that this SFR is restricting functions to a role, this would support a role-based access control policy if there was one in the overall system.
		AC-6	**Least Privilege** - Organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Restricting activities to authorized administrators supports this.
		IA-5(2)	**Authenticator Management** | PKI-Based Authentication Information system, for PKI-based authentication… - Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; - Enforces authorized access to the corresponding private key; - Maps the authenticated identity to the account of the individual or group; - Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.	The checking of the DN may support this.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
	- (.12) [MDM Agent, MDM Agent Platform] ensures all IKE protocols perform peer authentication using… - (.13) [MDM Agent, MDM Agent Platform] does not establish an SA if the DN contained in a certificate does not match the expected DN… - (.14) [MDM Agent, MDM Agent Platform] ensures by default that the strength of the symmetric algorithm…	SC-8	**Transmission Confidentiality and Integrity** - Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	The assignment in SC-8 should be completed to correspond with the requirement for protection from disclosure / modification in the SFR.
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	Use of IPSEC supports SC-8(1)
		SC-12	**Cryptographic Key Establishment and Management** - Organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	Some of the specific crypto requirements support this control.
		SC-12(2)	**Cryptographic Key Establishment and Management** | Symmetric Keys - Organization produces, controls, and distributes symmetric cryptographic keys using [*NIST FIPS-compliant; NSA-approved*] key management technology and processes.	The SFR supports this control through the approaches used for symmetric key distribution.
		SC-13 †	**Cryptographic Protection** Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	This would specific the specific encryption approaches.
		SC-23 †	**Session Authenticity** Information system protects the authenticity of	IPSEC is used for communication sessions.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
			communications sessions.	
FCS_TLS_EXT.1(2)	**TLS Implementation** TLS Implementation • [MDM Agent, MDM Agent Platform] implements one or more of TLS 1.2, TLS 1.0, TLS 1.1 with the following cyphersuites [list] • [MDM Agent, MDM Agent Platform] does not establish a trusted channel if the DN contained in a certificate does not match the expected DN	SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	The assignment in SC-8 should be completed to correspond with the requirement for protection from disclosure / modification in the SFR.
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection • Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	Whether this control is satisfied depends on the implementation method for meeting the SFR. At the SFR level, this can be addressed either through refinement of the SFR, or through appropriate specifications in the TSS that would indicated FDP_ITT is implemented through FCS operations.
		SC-13 †	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	This would specific the specific encryption approaches fo r TLS.
		SC-23 †	**Session Authenticity** • Information system protects the authenticity of communications sessions.	TLS is used for communication sessions.
		Note: The second part of the SFR does not correspond to an 800-53 control.		
FIA_X509_EXT,2(1)	**X509 Authenticaion** X509 Authenticaion • (.1) [MDM Agent, MDM Agent Platform] shall not [install, execute] code if the code signing certificate is invalid.	CM-5(3)	**Access Restrictions for Change** | Signed Components • Information system prevents the installation of [*software and firmware components*] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.	This SFR supports CM-5(3) if code signing is selected.

Objective Requirements

Objective TSF Requirements

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
FAU_GEN.1(2)	**Security Audit Data Generation** Audit Data Generation (MDM Agent) • MDM Agent generates audit records for: * Startup and shutdown of audit * Change in MDM policy * Any modifications from MDM Server * [*set of events in Table 8*] * and [*other events*] Note that FAU_GEN.1.2 was not included	AU-2	**Audit Events** Organization… • Determines system can audit [events] • [⋮] • Determines the following events are to be audited: [events]	FAU_GEN.1.1 gives the definition of what events should be audited (addressing the bulk of this control), but the assignments in AU-2 and AU-12 need to cover at least what is in FAU_GEN.1.1 for the mapping to be valid. Note also that FAU_GEN implies both auditable and audited, which is two distinct controls under 800-53.
FAU_SEL.1(2)	**Security Audit Event Selection** Selective Audit (MDM Agent) • MDM Agent can select the events to be audited from the set of auditable events based on (a) event type; (b) success of events; (c) failure of events; (d) [*attributes*]	AU-12	**Audit Generation** Information system… • Provides audit record generation capability for the auditable events defined in AU-2 a. at [*components*]; • Allows [*personnel or roles*] to select which auditable events are to be audited by specific components of the information system • Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	AU-12 item b. allows specific roles to select what will be audited fro the set of auditable events, but it does not do it based on particular attributes. It would satisfy selection based on event type.
FMT_POL_EXT.1	**Trusted Policy Update** Extended: Trusted Policy Update (MDM Agent) • MDM Server provides digitally signed polices and policy updates to the MDM Agent • MDM Agent only accepts policies and policy updates that are digitally signed.	Note: No correspondence. NIST SP 800-53 has controls dealing with signed executables, but policies are not executables. Digital signatures are also used for non-repudiation, but this SFR does not use the non-repudiation sense. There are controls for central management, but they don't reference signatures.		

Objective MDM Server or MDM Server Platform Requirements

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
FTA_TAB.1	**TOE Access Banners** Default TOE Access Banners • Before establishing a user session, product displays an advisory warning message regarding unauthorized use of the product.	AC-8	**System Use Notification** Information system… • Displays to users [*system use notification message or banner*] before granting access to the system that provides privacy and security notices consistent with applicable federal laws … and states that: (1) users are accessing a U.S. Government information system; (2) usage may be monitored, recorded, and subject to audit; (3) unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and (4) use of the information system indicates consent to monitoring and recording; • Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system • For publicly accessible systems: (1) displays system use information [*conditions*], before granting further access; (2) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (3) includes a description of the authorized uses of the system.	The AC-8 control is much more specific than the FTA_TAB.1 SFR regarding the content of the message and the fact that acknowledgement is required.

Objective MDM Agent or MDM Agent Platform Requirements

FAU_GEN.1(2)	**Security Audit Data Generation** Audit Data Generation • (2) [MDM Agent, MDM Agent platform] records within the audit record at least date, time, type, instigator, outcome, and [*event specific information*]	AU-3	**Content of Audit Records** • Information system generates records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event	FAU_GEN.1.2 details the list of what must be contained in each audit record. AU-3 covers the information identified it FAU_GEN.1.2 a).
		AU-3(1)	**Content of Audit Records** | Additional Audit Information • Information System generates records containing [*additional information*]	FAU_GEN.1.2 details the list of what must be contained in each audit record. AU-3(1) provides the means to address the event specific information in the FAU_GEN.1.2 b) assignment. The assignment in AU-3(1) must be completed to agree with FAU_GEN.1.2 b).
FAU_CRP_EXT.1	**Compliance Reporting** Support for Compliance Reporting of Mobile Device Configuration • MDM Server provides [interface that provides responses to queries about configuration of enrolled device, interface that permits export of data about the configuration of enrolled devices]	CM-6(1)	**Configuration Settings** | Automated Central Management / Application / Verification • Organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [*information system components*].	The SFR would appear to support the control.
FCS_CKM.1(4)	**Cryptographic Key Management** Cryptographic Key Generation (Asymmetric Keys for Authentication) [MDM Agent, MDM Agent platform] generates **asymmetric** cryptographic keys **for key authentication** in accordance with [*FIPS PUB 168-4, ANSI X9.31-1998*] and specified cryptographic key sizes [*112 bits*]	SC-12†	**Cryptographic Key Establishment and Management** • Organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	Assignment must be completed congruent with the SFR completion, and the completed control must agree with the completed control in the System Security Plan for the system under analysis.
		SC-12(3) †	**Cryptographic Key Establishment and Management** | Asymmetric Keys • Organization produces, controls, and distributes asymmetric cryptographic keys using [NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4	FCS_CKM.1(2) calls for asymmetric key in accordance with the NIST (FIPS) or ANSI process; as NSA developed the PP, it is by implication an NSA-approved technology and process.

			certificates and hardware security tokens that protect the user's private key].	