NIST SP 800-53 Revision 4 Mapping: Protection Profile for Mobile Device Fundamentals Version 2.0 12 September 2014

27 April 2016

Introduction

Several of the NIST SP 800-53/CNSS 1253 controls are either fully or partially addressed by compliant TOEs. This document 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.

General Comments:

1. The Common Criteria applies to **products**, and NIST SP 800-53 applies to **systems**. Satisfaction or support of a control at a product level does not necessarily mean it is satisfied for the system as a whole.

2. A mapping between the Common Criteria and NIST SP 800-53 focuses on technical aspects and doesn't address all operational aspects.

3. Mappings assume that parameters (or derived requirements) are completed in a compatible manner between the mapped controls. For example, a mapping between FDP_ACC/FDP_ACF and AC-3 assumes that the completions and derived specifications that detail the enforced policy are essentially the same.

4. Mappings do not necessarily imply that all of the mapped controls are present. Often, there are many potential ways to implement a requirement. The mapping tables may include mappings to controls that are potential approaches to implementing the mapped requirement. The design of the product or system in question *must* be examined to determine the specific implementation approach used. Note that when this caveat applies, there is usually a note indicating that the control is a potential approach to addressing the requirement and not necessarily implemented.

5. NIST SP 800-53 does not, in general, dictate cryptographic algorithm usage, key size, etc. *However…* the SA-4(7) control, which is included in all CNSSI No. 1253 baselines, requires that 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 policy, that the cryptographic module is FIPS-validated. CCEVS requires NIST validation (either CAVP or CMVP) per its policies for cryptography used in products that have Protection Profiles for their specific technology type. If classified information is involved, SA-4(6) requires an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted. Lastly, the DoD completion for SC-13 requires that protection of classified information use NSA-approved cryptography (as does the CNSS Classified Information Overlay), and that provision of digital signatures and hashing requires FIPS-validated cryptography.

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**
FCS_CKM.1(1)	**Cryptographic Key Management** Refinement: Cryptographic Key Generation (Key Establishment) Product generates **asymmetric** cryptographic keys **for key establishment** in accordance with [*specified schemes and bit sizes*]	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.
		Note: See general comment regarding cryptographic algorithm usage.		
FCS_CKM.1(2)	**Cryptographic Key**	SC-12†	**Cryptographic Key**	Assignment must be

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
	Management Cryptographic Key Generation (Asymmetric Keys for Authentication) Product generates **symmetric** cryptographic keys **for key authentication** in accordance with [*PRF-384*] and specified cryptographic key sizes [*128 bits*] using a Random Bit Generator as specified in FCS_RBG_EXT.1 that meets the following [*IEEE 802.11-2012*]		**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*].	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(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.	FCS_CKM.1(2) calls for symmetric 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.
		Note: See general comment regarding cryptographic algorithm usage.		
FCS_CKM.1(2)	**Cryptographic Key Management** Cryptographic Key Generation (WLAN) Product generates **symmetric** cryptographic keys in accordance with [PRF-384] and specified cryptographic key sizes [*128 bits*] **using a Random Bit Generator … meeting [IEEE 802.11-2012]**	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(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.	FCS_CKM.1(3) calls for a PRF algorithm and a standard RBG; as NSA developed the PP, it is by implication an NSA-approved technology and process.
		Note: See general comment regarding cryptographic algorithm usage.		
FCS_CKM.2(1)	**Cryptographic Key Management** Cryptographic Key Establishment • Product performs cryptographic key establishment in accordance with a specified cryptographic	SC-12†	**Cryptographic Key Establishment and Management** • Organization establishes and manages cryptographic keys for required cryptography employed within the information	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

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
	key establishment method: [*RSA and its requirements*] and [*selection:, EC-base and its requirements; Finite-field and its requirements; no others*]		system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	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*].	The cited algorithms are all asymmetric, so SC-12(3) also applies.
		Note: See general comment regarding cryptographic algorithm usage.		
FCS_CKM.2(2)	**Cryptographic Key Management** Cryptographic Key Distribution (WLAN) - TSF decrypts Group Temporal Key (GTK) in accordance with a specified cryptographic key distribution method [*AES Key Wrap in an EAPOL-Key frame*] that meets the following: [*NIST SP 800-38F, IEEE 802.11-2012 for the packet format and timing considerations*] and does not expose the cryptographic keys.	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.
		Note: See general comment regarding cryptographic algorithm usage.		
FCS_CKM_EXT.1	**Cryptographic Key Support** Cryptographic Key Support (REK) - TSF supports a [*selection: hardware-isolated, hardware-protected*] REK with a key of size [*selection: 128 bits, 256 bits*]. - Software on the TSF can only request [*selection: AES encryption/decryption, NIST SP 800-108 key derivation*] by the key and can not read, import, or export a REK. - REK is generated by approved RBG	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.
		Note: Restrictions on use of the REK do not easily correspond to a particular control. Note: See general comment regarding cryptographic algorithm usage.		
FCS_CKM_EXT.2	**Cryptographic Data Encryption Keys**	SC-12†	**Cryptographic Key Establishment and**	Assignment must be completed congruent with 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**
	Cryptographic Key Random Generation - All DEKs are randomly generated with entropy corresponding to …		**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*].	completion, and the completed control must agree with the completed control in the System Security Plan for the system under analysis.
FCS_CKM_EXT.3	**Cryptographic Data Encryption Keys** Cryptographic Key Generation - All KEKs are [*128, 256 bit*] corresponding to at least the security strength of the key encrypted. - KEKs are generated from a Password Authentication Factor using PBKDF and [*how*]. - * 256 bit is required after 3Q2015	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.
		Note: See general comment regarding cryptographic algorithm usage.		
FCS_CKM_EXT.4	**Cryptographic Key Destruction** Key Destruction - Cryptographic keys are destroyed by [*clearing the KEK, sanitization approach*] - TSF destroys all plaintext keying material and parameters when no longer needed.	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.5	**TSF Wipe** TSF Wipe - TSF wipes all protected data by [*method*]. - TSF power cycles after wiping.	AC-7(2) †	**Unsuccessful Logon Attempts** | Purge / Wipe Mobile Device - Information system purges/wipes information from [*mobile devices*] based on [*purging / wiping requirements / techniques*] after [*number*] consecutive, unsuccessful device logon attempts.	FCS_CKM_EXT.5 supports the implementation of AC-7(2) by providing the underlying required capability.
		AC-19	**Access Control for Mobile Devices** Organization… - Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance	FCS_CKM_EXT.5 would broadly support the wiping requirements from the usage restrictions and configuration 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
			for organization-controlled mobile devices • Authorizes the connection of mobile devices to organizational information systems.	
		MP-6*	**Media Sanitization** Organization… • Sanitizes [*information system media*] prior to disposal, release out of organizational control, or release for reuse using [*sanitization techniques and procedures*] in accordance with applicable federal and organizational standards and policies; • Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.	The wipe performed by this SFR supports MP-6.
		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*].	FCS_CKM_EXT.5 supports the implementation of MP-6(8) by providing the underlying required capability.
		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.6	**Cryptographic Salt Generation** Salt Generation • TSF generates all salts using an RBG that meets FCS_RBG_EXT.1	Note: This mapping is unclear. Perhaps SC-12, but this could also be so low level it isn't visible at the control level.		
FCS_COP.1(1)	**Cryptographic Operation**	SC-13 †	**Cryptographic Protection** • Information system	The assignment in the SFR must be completed

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**
	Cryptographic Operation • Product performs [***encryption/decryption***] in accordance with [AES-CBC, AES_CCMP, [others]] and [***128*** *[and 256, no others]*] • Support for 256 bits is required after 3Q2015.		implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	to include all the cryptographic operations, algorithms, key sizes, and standards specified in the iterations of the FCS_COP.1 SFR.
		Note: See general comment regarding cryptographic algorithm usage.		
FCS_COP.1(2)	**Hashing Algorithms** Cryptographic Operation • Product performs [***cryptographic hashing***] in accordance with SHA-1 and [other SHAs] and [***MD Sizes 160 and others***]	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.
		Note: See general comment regarding cryptographic algorithm usage.		
FCS_COP.1(3)	**Signature Algorithms** Cryptographic Operation • Product performs [***cryptographic signature services (generation and verification)***] in accordance with [RSA schemes] using cryptographic key sizes [of 2048-bit or greater] that meet the following: [FIPS PUB 186-4…] and [*selection:[ECDSA schemes] using [“NIST curves” P-256, P-384 and [selection: P-521, no other curves]] that meet the following: [FIPS PUB 186-4…]; No other algorithms*]. • ECDSA is required after 3Q2015	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*].	Depending on the use of the digital signatures, support could be provided for the implementation of AU-10.
		Note: See general comment regarding cryptographic algorithm usage.		
FCS_COP.1(4)	**Keyed Hash Algorithms** Cryptographic Operation • Product performs [*keyed-hash message authentication*] in accordance with a specified cryptographic algorithm HMAC-SHA-1 and [*selection: other HMAC-SHAs, no other algorithms*] and cryptographic key sizes [*assignment: key size (in bits)*] and message digest sizes 160 and [*selection: 256, 384, 512, no other*] bits that meet the following: [***FIPS Pub 198-1, …, and FIPS Pub 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.
		Note: See general comment regarding cryptographic algorithm usage.		

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(5)	**Password-Based Key Derivation Functions** Cryptographic Operation • Product performs [***password-based key derivation functions***] in accordance with HMAC SHA 1 and [other HMAC SHA] and key sizes of 128,256 that meet FIPS 800-132 • Use of 256 bit key sizes required after 3Q2015.	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.
		Note: See general comment regarding cryptographic algorithm usage.		
FCS_HTTPS_EXT.1	**HTTPS Protocol** Extended: HTTPS Protocol • TSF implements the HTTPS protocol that complies with RFC 2818, using TLS (FCS_TLSC_EXT.2). • TSF notifies the application and [*selection: not establish the connection, request application authorization to establish the connection, no other action*] if the peer certificate is deemed invalid.	SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	Use of HTTPS supports transmission 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*].	Use of HTTPS supports transmission confidentiality and integrity through use of cryptography.
FCS_IV_EXT.1	**Initialization Vector Generation** Initialization Vector Generation • Product generates IVs in accordance with Table 14: References and IV Requirements for NIST-approved Cipher Modes	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_RBG_EXT.1	**Random Bit Generation** Random Bit Generation • Product 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 … • Product can provide output of the RBG to applications • Note: NIST SP 800-90B Appx. C will be required in future versions.	Note: Unclear. This might fit within SC-12 and key generation, but it could also be below the level of any existing NIST 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
FCS_SRV_EXT.1	**Cryptographic Algorithm Services** Cryptographic Algorithm Services • Product provides a mechanism for [applications] to request the following crypto operations [list of FCS SFRs]	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.
		Note: The extent to which other controls are covered depends on what applications are invoking the cryptographic services, and to what purpose they are using them. Note: See general comment regarding cryptographic algorithm usage.		
FCS_STG_EXT.1	**Cryptographic Key Storage** Cryptographic Key Storage • Product provides [*selection: hardware, hardware-isolated, software-based*] secure key storage for symmetric private keys and [*selection: symmetric keys, persistent secrets, no other keys*] • Product can import keys into the secure key storage upon request of [who] and [applications] • Product can destroy keys upon request of [who] • Product can restrict who can use the key/secret. • Product can restrict who can destroy the key/secret.	AC-3	**Access Enforcement** • Information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	In general, this is one aspect of an access enforcement policy, and thus supports the overall system access control policy.
		AC-3(5)	**Access Enforcement** | Security-Relevant Information • Information system prevents access to [*security-relevant information*] except during secure, non-operable system states.	Although the states are not mentioned in the SFR, this SFR may serve to support restrictions to specific security information.
		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.

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(2)	**Authenticator Management** | PKI-Based Authentication Information system, for PKI-based authentication… • […] • Enforces authorized access to the corresponding private key; • […]	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_STG_EXT.2	**Cryptographic Key Storage** Encrypted Cryptographic Key Storage • Product encrypts all DEKs and KEKs and [others] that are [how protected]	AC-3	**Access Enforcement** • Information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	In general, this is one aspect of an access enforcement policy, and thus supports the overall system access control policy.
		AC-3(5)	**Access Enforcement** | Security-Relevant Information • Information system prevents access to [*security-relevant information*] except during secure, non-operable system states.	Although the states are not mentioned in the SFR, this SFR may serve to support restrictions to specific security information.
		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_STG_EXT.3	**Cryptographic Key Storage** Integrity of Encrypted Key Storage	SC-12†	**Cryptographic Key Establishment and Management**	Assignment must be completed congruent with the SFR completion, and 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**
	- Product protects integrity of any encrypted KEK by [method] - Product verifies the integrity of the [*hash, digital signature, MAC*] of the stored key prior to use of the key		- 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*].	completed control must agree with the completed control in the System Security Plan for the system under analysis.
FCS_TLSC_EXT.1	**EAP TLS Protocol** EAP TLS Protocol - Product implements EAP-TLS procotol as specified in RFC 5216… - Product verifies that the server certificate…	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.	The SG for IA-3 discusses use of EAP-TLS for device identification.
		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.	This covers verification of the certificate.
		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	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

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**
			implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	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 for EAL-TLS.
		SC-23 †	**Session Authenticity** • Information system protects the authenticity of communications sessions.	EAL-TLS is used for communication sessions.
		SC-23(5) †	**Session Authenticity** | Allowed Certificate Authorities • Information system only allows the use of [*certificate authorities*] for verification of the establishment of protected sessions.	The assignment in 1.2 addresses the approved CAs.
FCS_TLSC_EXT.2	**TLS Client Protocol** Extended: TLS Protocol • Product implements TLS 1.2 (RFC 5246) supporting the following ciphersuites: [*mandatory suites*] [*optional suites*]. • Product verifies that the presented identifier matches the reference identifier according to RFC 6125. • Product does not establish a trusted channel if the peer certificate is invalid. • Product supports mutual authentication using X.509v3 certificates.	AC-17(2)*	**Remote Access** | Protection of Confidentiality / Integrity Using Encryption • Information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	Use of TLS provides supports cryptography for remote access
		IA-3(1)	**Device Identification and Authentication** | Cryptographic Bidirectional Authentication • Information system authenticates [*specific devices and/or types of devices*] before establishing [*local; remote; network*] connection using bidirectional authentication that is cryptographically based.	Identifier matching per TLS may support device authentication. It is unclear if it rises to the level of user authentication, but other than IA-5(2) (which deals with PKI authenticators), there is not an IA-2 or AC-2 requirement to use certificates.
		IA-5(2)	**Authenticator Management** | PKI-Based Authentication Information system, for PKI-based authentication…	The X509v3 validation supports 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
			• Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; • […]	
		SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	TLS provides transmission 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*].	TLS provides transmission confidentiality and integrity.
		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.	Dictation of specific algorithms occurs through SC-13.
		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. Note: See general comment regarding cryptographic algorithm usage.		
FDP_ACF_EXT.1	**Access Control** Security Access Control • Product provides a mechanism to restrict system services that are accessible to an application. • Product provides an access control policy that prevents	AC-3†	**Access Enforcement** • Information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	The FDP_ACF_EXT.1 would have to align with the organization access control policy.

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
	[*selection: application processes, groups of application processes*] from accessing [*selection: all, private*] data stored by other [*selection: application processes, groups of application processes*]. Exceptions may only be explicitly authorized for such sharing by [*selection: the user, the administrator, a common application developer*].	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 system services is a form of least privilege, allowing only authorized access for processes acting on a user's behalf.
		AC-6(10)	**Least Privilege** | Prohibit Non-Privileged Users From Executing Privileged Functions - Information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards / countermeasures.	Restricting system services would include restriction of use of privileged functions.
FDP_DAR_EXT.1	**Access Control** Data-at-Rest Protection - Encryption covers all protected data - Encryption performed using DEKs with AES in the [mode] with key size [sizes]	AC-19(5)	**Access Control for Mobile Devices** | Full Device / Container-Based Encryption - Organization employs [*full-device encryption; container encryption*] to protect the confidentiality and integrity of information on [*mobile devices*].	This supports satisfaction of this control, as this is the Mobile Device PP.
		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 DAR protection.
		SC-28†	**Protection of Information at Rest** - Information system protects the [(*one or more): confidentiality; integrity*] of [*information at rest*].	Complete the assignment to cover protected data. This needs to agree with organizational requirements.
		SC-28(1)†	**Protection of Information at Rest** | Cryptographic Protection - Information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of	This addresses the use of cryptography

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*] on [*information system components*].	
		Note: See general comment regarding cryptographic algorithm usage.		
FDP_IFC_EXT.1	**Subset Information Flow Control** Extended: Subset information flow control - VPN • Product [*selection: provides an interface to VPN clients to enable all IP traffic (other than IP traffic required to establish the VPN connection) to flow through the IPsec VPN client; enables all IP traffic (other than IP traffic required to establish the VPN connection) to flow through the IPsec VPN client*].	AC-4†	**Information Flow Enforcement** • Information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [*information flow control policies*].	This would be supporting one aspect of the information flow policy.
		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.	Providing or requiring the VPN supports enforcement of boundary protection.
		SC-7(7) †	**Boundary Protection** | Prevent Split Tunneling for Remote Devices • Information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.	The second option in the selection prevents split tunneling.
FDP_STG_EXT.1	**Access Control** Certificate Data Storage • Product provides protected storage for the Trust Anchor	IA-5	**Authenticator Management** Organization manages information system authenticators by…	Protecting the trust anchor is part of protecting the authenticator content.

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
	Database		• […] • Protecting authenticator content from unauthorized disclosure and modification • […]	
		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; • […]	Protecting the trust anchor supports the validation of certificates.
		IA-5(14)	**Authenticator Management** | Managing Content of PKI Trust Stores • For PKI-based authentication, Organization employs a deliberate organization-wide methodology for managing the content of PKI trust stores installed across all platforms including networks, operating systems, browsers, and applications.	Protecting the trust anchor database is part of managing the trust anchor stores.
		SC-17*	**Public Key Infrastructure Certificates** • Organization issues public key certificates under an [*certificate policy*] or obtains public key certificates from an approved service provider.	Use of PKI certificates requires valid trust anchors.
FDP_UPC_EXT.1	**Inter-TSF User Data Protected Channel** Extended: Inter-TSF user data transfer protection • Product provide a means for non-TSF applications executing on the TOE to use TLS, HTTPS, Bluetooth BR/EDR, and [*selection: DTLS, Bluetooth LE, no other protocol*] to provide a protected communication channel between the non-TSF application and another IT product that is logically distinct from other communication channels, provides assured identification of	SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	SFR provides a protected communication channel.
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection • Information system implements cryptographic mechanisms to [*prevent*	SFR provides a protected communication channel through encryption.

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**
	its end points, protects channel data from disclosure, and detects modification of the channel data. - Product permits the non-TSF applications to initiate communication via the trusted channel.		*unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	
FIA_AFL_EXT.1	**Authentication Failure** Authentication Failure Handling - Product detects when [*an administrator configurable positive integer within[range of acceptable values]*] unsuccessful authentication attempts occur related to [*last successful authentication by that user*]. - When the defined number of unsuccessful authentication attempts has been [*met, surpassed*], the product [*performs [full wipe, remediation]*]. - Product maintains the number of unsuccessful authentication attempts that have occurred upon power off.	AC-7†	**Unsuccessful Logon Attempts** Information system… - Enforces a limit of [*number*] consecutive invalid logon attempts by a user during a [*time period*] - Automatically [*locks the account/node for an [time period]; locks the account/node until released by an administrator; delays next logon prompt according to [delay algorithm]*] when the maximum number of unsuccessful attempts is exceeded.	Depending on the assignment completions, it is possible for AC-7 to be satisfied. The SFR is much broader, possibly dictating management capabilities, and providing the possibility for a greater range of actions than is permitted in the AC-7 control. Note that AC-7 is specific about “consecutive” attempts; this is not explicit but is typically assumed in the implementation of the SFR.
		AC-7(2) †	**Unsuccessful Logon Attempts** | Purge / Wipe Mobile Device - Information system purges/wipes information from [*mobile devices*] based on [*purging / wiping requirements / techniques*] after [*number*] consecutive, unsuccessful device logon attempts.	This addresses the purge requirements.
FIA_BLT_EXT.1	**Bluetooth Authorization and Authentication** Extended: Bluetooth User Authorization - Product requires explicit user authorization before pairing with a remote Bluetooth device.	AC-19	**Access Control for Mobile Devices** Organization… - Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices - Authorizes the connection of mobile devices to organizational information systems.	Bluetooth authorization would support the broad usage restrictions for mobile devices.
		IA-3†	**Device Identification and Authentication** - Information system uniquely identifies and authenticates [*specific and/or types of devices*] before establishing a [*(one*	Unclear, but Bluetooth may support device authentication.

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
			or more): local; remote; network] connection.	
FIA_PAE_EXT.1	**Port Access Entity Authentication** Port Access Entity Authentication • Product conforms to IEEE 802.1X for a PAE in the "Supplicant" role	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.	Addresses device authentication.
		IA-3(1) †	**Device Identification and Authentication** | Cryptographic Bidirectional Authentication • Information system authenticates [*specific devices and/or types of devices*] before establishing [*local; remote; network*] connection using bidirectional authentication that is cryptographically based.	Addresses device authentication.
FIA_PMG_EXT.1	**Password Management** Password Management • Product supports the following for the Password Authentication Factor: [complexity stuff]	IA-5(1)	**Authenticator Management** | Password-Based Authentication Information system, for password-based authentication… • Enforces minimum password complexity of [*complexity requirements*]; • Enforces at least the following number of changed characters when new passwords are created: [*number*] • Stores and transmits only encrypted representations of passwords • Enforces password minimum and maximum lifetime restrictions of [*minimum, maximum*]; • Prohibits password reuse for [*number*] generations • Allows the use of a temporary password for system logons with an immediate change to a permanent password.	This only satisfies a portion of this control.
FIA_TRT_EXT.1	**Authentication Throttling** Authentication Throttling • Product limits automated user	AC-7†	**Unsuccessful Logon Attempts** Information system…	Depending on the assignment completions, it is possible for AC-7 to be satisfied. The SFR is

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
	authentication attempts by [action] with a minimum delay.		• Enforces a limit of [*number*] consecutive invalid logon attempts by a user during a [*time period*] • Automatically [*locks the account/node for an [time period]; locks the account/node until released by an administrator; delays next logon prompt according to [delay algorithm]*] when the maximum number of unsuccessful attempts is exceeded.	much broader, possibly dictating management capabilities, and providing the possibility for a greater range of actions than is permitted in the AC-7 control. Note that AC-7 is specific about “consecutive” attempts; this is not explicit but is typically assumed in the implementation of the SFR.
FIA_UAU.7	**User Authentication** Protected Authentication Feedback • Product provides only [*list of feedback*] to the user while the authentication is in progress.	IA-6	**Authenticator Feedback** • Information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	Presuming that FIA_UAU.7 was completed to require obscured feedback, IA-6 is satisfied at the product level.
FIA_UAU_EXT.1	**Authentication for Cryptographic Operation** Authentication for Cryptographic Operation • Product requires user to present the PAF prior to decryption of protected data.	IA-7	**Cryptographic Module Authentication** • Information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, […] for such authentication.	Unclear is this is the correct mapping. UAU_EXT.1 clearly *does not* map to IA-2 or IA-8, because it does not include unique identification. IA-7 is authentication to a cryptographic module for cryptographic operations, which this seems to be.
FIA_UAU_EXT.2	**Timing of Authentication** Timing of Authentication • Product allows [actions] to be performed before authentication. • Product requires authentication before any other TSF-mediated actions	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.

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-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. ***Note that IA-2 is only partially addressed – mobile devices do not provide unique identification.***
FIA_UAU_EXT.3	**Re-Authentication** Re-Authentication • Product requires the user to enter the PAF when the user changes the PAF, to unlock the device, and [other conditions]	IA-11†	**Re-Authentication** • Organization requires users and devices to re-authenticate when [*circumstances or situations requiring re-authentication*].	Assignments must be completed in a congruent fashion.
FIA_X509_EXT.1	**Validation of Certificates** Validation of Certificates • Product validates certificates in accordance with the following rules…	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.	Addresses the certificate validation portion of IA-5(2).**Note that this does not address all of IA-5(2).**
FIA_X509_EXT.2	**X509 Certificate Authentication** X509 Certificate Authentication • Product uses X.509v3 certificates as defined by RFC 5280 to support authentication for EAP-TLS exchanges, and [protocol] and [other 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… • […]	This addresses mapping the authenticated identity. **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
			• Maps the authenticated identity to the account of the individual or group; • […]	
FIA_X509_EXT.3	**Request Validation of Certificate** Request Validation of Certificate • Product provides a certificate validation service.	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; • […]	**SUPPORTS**. FIA_X509_EXT.3 does not correspond to a specific control in 800-53, but the SFR would support satisfaction by other product software of IA-5(2), item a.
FMT_MOF_EXT.1	**Management of Functions in TSF** Extended: Management of Security Functions Behavior • Product restricts the ability to [perform] the functions [functions] to [the user].	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) (Role Based Access Control) is a possibility, but the only role appears to be user and perhaps administrator, and given the FMT_SMR is not included, this really isn't role based access control.
		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 the ability to perform particular functions is a form of least privilege.
		AC-6(10)	**Least Privilege** | Prohibit Non-Privileged Users From Executing Privileged Functions • Information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards / countermeasures.	Restricting the ability to perform particular functions would include restriction of use of privileged functions.

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_SMF.1	**Specification of Management Functions** Specification of Management Functions • Product is of performing the following management functions: [*list of management functions*].	Note: The selection of functions dictates the controls addressed – this cannot be determined apriori. Note that many of these functions do not correspond to controls as NIST SP 800-53 does not go to that level of detail. However, the following correspond to some of the non-optional functions:		
		AC-3*	**Access Enforcement** • Information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Those functions that support definition of access control rules support AC-3
		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.	By defining the management functions, the capability is provided to then restrict those functions.
		AC-18(4)*	**Wireless Access** | Restrict Configurations By Users • Organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.	One of the non-optional functions relates to the ability to configure wireless networking.
		AC-19*	**Access Control for Mobile Devices** Organization… • Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices • Authorizes the connection of mobile devices to organizational information systems.	A number of the capabilities listed go to the establishment of usage restrictions and configuration of the device.
		CM-6*	**Configuration Settings** Organization… • Establishes and documents configuration settings for information technology products employed within the information system using [*security configuration checklists*] that reflect the most restrictive mode consistent	A number of the functions provide the ability to configure the product in accordance with the security configuration checklist.

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 operational requirements; • Implements the configuration settings; • Identifies, documents, and approves any deviations from established configuration settings for [*information system components*] based on [*operational requirements*]; and • Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	
		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*].	A number of non-optional functions allow the configuration of what services are available.
		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*].	Non-optional functions include the ability to define what software is authorized to execute on the platform.
		IA-7*	**Cryptographic Module Authentication** • Information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, […] for such authentication.	Another non-optional function deals with loading keys into the crypto module, which would involve IA-7.

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*	**Flaw Remediation** Organization… • Identifies, reports, and corrects information system flaws; • Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; • Installs security-relevant software and firmware updates within [*time period*] of the release of the updates; • Incorporates flaw remediation into the organizational configuration management process.	Another non-optional function deals with the loading up updates.
		Note: Other controls possible depending on selection might include AU-12 (dealing with selection of audit events) and CP-9 (dealing with backup).		
FMT_SMF_EXT.1	**Specification of Management Functions** Specification of Remedial Actions • Product shall offer [options] upon unenrollment and [other triggers]	AC-19	**Access Control for Mobile Devices** Organization… • Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices • Authorizes the connection of mobile devices to organizational information systems.	This SFR may support AC-19, depending on the organizational policy, but there is no explicit control for the information system to perform these actions.
		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*].	As some of the options including wiping of the device, this control is supported.
FPT_AEX_EXT.1	**Anti-Exploitation Services** Address Space Randomization • Product shall provide address space randomization	SI-16†	**Memory Protection** • Information system implements [*security safeguards*] to protect its memory from unauthorized code execution.	Assignment must be completed in a congruent fashion.
FPT_AEX_EXT.2	**Anti-Exploitation Services**	SI-16†	**Memory Protection**	Assignment must be

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
	Memory Page Permissions • Product shall be able to enforce permissions on every page of physical memory.		• Information system implements [*security safeguards*] to protect its memory from unauthorized code execution.	completed in a congruent fashion.
FPT_AEX_EXT.3	**Anti-Exploitation Services** Stack Overflow Protection • Processes executing in a non-privileged domain shall implement stack-based buffer overflow protection.	SI-16†	**Memory Protection** • Information system implements [*security safeguards*] to protect its memory from unauthorized code execution.	Assignment must be completed in a congruent fashion.
FPT_AEX_EXT.4	**Anti-Exploitation Services** Domain Isolation • Product shall protect itself from modification by untrusted subjects • Product shall enforce isolation of address space between applications	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.	Domain isolation is a form of least privilege, as least when the trust level of a process can be controlled.
		SC-3	**Security Function Isolation** • Information system isolates security functions from nonsecurity functions.	Isolation is protection from modification by untrusted subjects.
		SC-39	**Process Isolation** • Information system maintains a separate execution domain for each executing process.	The presumption is that processes correspond to applications.
FPT_KST_EXT.1	**Key Storage** Plaintext Key Storage • Product shall not store any plaintext key material in readable non-volatile memory	IA-5	**Authenticator Management** Organization manages information system authenticators by… • […] • Protecting authenticator content from unauthorized disclosure and modification • […]	Presuming keys correspond to authenticators, a portion of IA-5 is met.
		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.

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(2)	**Authenticator Management** | PKI-Based Authentication Information system, for PKI-based authentication… • […] • Enforces authorized access to the corresponding private key; • […]	Addresses secure key storage.
		IA-5(6)	**Authenticator Management** | Protection of Authenticators • Organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access.	In some sense, this SFR provides information system support to this control.
		SC-3	**Security Function Isolation** • Information system isolates security functions from nonsecurity functions.	The SFR would support implementation of SC-3.
		Note: There appear to be no explicit controls related to key storage other than their use as authenticators.		
FPT_KST_EXT.2	**Key Storage** No Key Transmission • Product shall not transmit any plaintext key material from the cryptographic module	IA-5	**Authenticator Management** Organization manages information system authenticators by… • […] • Protecting authenticator content from unauthorized disclosure and modification • […]	Addresses authenticator transmission
		IA-5(1) †*	**Authenticator Management** | Password-Based Authentication ‡ Information system, for password-based authentication… • [⋮] • Stores and transmits only encrypted representations of passwords • [⋮]	Addresses password transmission; keys are a form of password.
		IA-5(2)	**Authenticator Management** | PKI-Based Authentication Information system, for PKI-based authentication… • […]	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**
			• Enforces authorized access to the corresponding private key; • […]	
		IA-5(6)	**Authenticator Management** | Protection of Authenticators • Organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access.	In some sense, this SFR provides information system support to 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*].	Addresses requirements for key transmission.
FPT_KST_EXT.3	**Key Storage** No Plaintext Key Export • Product shall ensure is it not possible to export plaintext keys.	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*].	Addresses requirements for key transmission.
FPT_NOT_EXT.1	**Self-Test Event Notification** Event Notification • Product shall transition to non-operational mode and [notification action] when the following types of failures occur: * Self Test Failures; * Software integrity verification failures; * [other failures]	SI-6†	**Security Function Verification** Information system… • […] • Notifies [*personnel or roles*] of failed security verification tests; • [*(one or more): shuts the information system down; restarts the information system; [alternative action(s)]*] when anomalies are discovered.	Addresses the notification and actions for self-test failures
		SI-7†	**Software, Firmware, and Information Integrity** • Organization employs	Addresses the verification aspect.

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**
			integrity verification tools to detect unauthorized changes to [*software, firmware, and information*].	
		SI-7(2)†	**Software, Firmware, and Information Integrity** | Automated Notifications of Integrity Violations • Organization employs automated tools that provide notification to [*personnel or roles*] upon discovering discrepancies during integrity verification.	Addresses the notification aspects
		SI-7(5) †	**Software, Firmware, and Information Integrity** | Automated Response to Integrity Violations • Information system automatically [*(one or more): shuts the information system down; restarts the information system; implements [security safeguards]*] when integrity violations are discovered.	Addresses the actions
FPT_STM.1	**Time Stamps** Reliable Time Stamps • Product is able to provide reliable time stamps.	AU-8	**Time Stamps** Information system… • Uses internal system clocks to generate time stamps for audit records • Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [*organization-defined granularity of time measurement*].	The SFR talks about providing reliable time stamps, presumably for auditing purposes.
FPT_TST_EXT.1	**TSF Functionality Testing** Cryptographic Functionality Testing • Product runs a suite of self-tests [when] to demonstrate the correct operation of all cryptographic functions.	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.

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_TST_EXT.2	**TSF Functionality Testing** TSF Integrity Testing - Product verifies the integrity of the Application Processor bootloader software, OS kernel, and [other executable code] through [a digital signature or hardware protected hash]	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
		SI-7(9)	**Software, Firmware, and Information Integrity** | Verify Boot Process - Information system verifies the integrity of the boot process of [*devices*].	Addresses the integrity of the bootloader software.
FPT_TUD_EXT.1	**Trusted Update** TSF Version Query - Product provides authorized users with the ability to query the current version of the firmware - … of the hardware model - … of installed mobile applications	Note: There does not appear to be a control in the 800-53 catalog that corresponds to this SFR.		
FPT_TUD_EXT.2	**Trusted Update** Trusted Update Verification - Product verifies software update to the TSF using a digital signature prior to installation. - Boot integrity key/hash only updated by verified software - Digital signature key shall [how it is validated] - Product verifies mobile applications using a digital signature prior to installation	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.	
		SI-7(15)	**Software, Firmware, and Information Integrity** | Code Authentication - Information system implements cryptographic mechanisms to authenticate [*software or firmware components*] prior to installation.	
		Note: All aspects of the SFR are not covered by the 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**
FTA_SSL_EXT.1	**Session Locking** TSF- and User-Initiated Locked State • Product transitions to a locked state after a time interval of inactivity, upon user request. • Locking overwrites or clears the display and [other actions]	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.	The SFR provides the system-initiated session lock of AC-11.
		AC-11(1)	**Session Lock** | Pattern-Hiding Displays • Information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.	This addresses the portion of the SFR that requires overwriting or obscuring the display.
FTA_WSE_EXT.1	**Wireless Network Access** Wireless Network Access • Product is able to attempt connections to wireless networks specified as acceptable networks	AC-18	**Wireless Access** Organization… • Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access • Authorizes wireless access to the information system prior to allowing such connections.	This looks to be an implementation and enforcement of the usage restrictions.
FTP_ITC_EXT.1	**Trusted Path/Channels** Trusted Channel Communications • Product uses 802.11-2012, 802.1X and EAP-TLS and [at least one of …] to provide a communications channel between itself and another trusted IT product that is that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. • Product permits [*the TSF, another trusted IT product*] to initiate communication via the trusted channel. • Product initiates communication via the trusted channel for [*list of functions for which a trusted channel is required*].	AC-17(2) †*	**Remote Access** | Protection of Confidentiality / Integrity Using Encryption • Information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	Depending on the nature of the endpoints, FTP_ITC.1 can be used to provide a trusted channel for remote access. The assignment in FTP_ITC.1.3 must indicate the channel is used for remote access.
		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.	FTP_ITC.1 discusses provision of a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. This control provides 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**
				identification of the end-points.
		IA-3(1)	**Device Identification and Authentication** | Cryptographic Bidirectional Authentication • Information system authenticates [*specific devices and/or types of devices*] before establishing [*local; remote; network*] connection using bidirectional authentication that is cryptographically based.	FTP_ITC.1 discusses provision of a communication channel between itself and another trusted IT product. If that trusted channel is provided using cryptographic mechanisms, this control is also addressed **at the product level**.
		IA-5(1) †	**Authenticator Management** | Password-Based Authentication ‡ Information system, for password-based authentication… • [⋮] • Stores and transmits only encrypted representations of passwords • [⋮]	FTP_ITC.1 requires protection of channel data from disclosure. If it is refined to use encryption, it would serve to ensure that passwords are transmitted encrypted, addressing IA-5(1) item c. 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.	FTP_ITC.1 calls for protection of channel data “from modification or disclosure”. SC-8 should be completed to provide such protection (note: the SFR is ambiguous as to whether the “or” is inclusive or exclusive, but inclusive is a reasonable assumption).
		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.

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; 9. [⁝] • [⁝]	Supports this.
		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	

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 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 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-	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.

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
	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(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, 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	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 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;	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**
	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.		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 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.	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.
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	At the product level, identification of the configuration items would include identification of the product with a unique reference.

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
			configuration items; • [⋮]	
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 control the integrity of changes to [*configuration items under configuration management*]; • [⋮]	ALC_CMS captures the "[*configuration items under configuration management*]"
ALC_TSU_EXT.1	**Timely Security Updates** Timely Security Updates • Developer has a process for creating and deploying security updates • The process defines a time window between public disclosure of a vulnerability and its correction. • Process describes mechanisms available for reporting security issues	SA-10	**Developer Configuration Management ‡** Organization requires the developer of the information system, system component, or information system service to: • [⋮] • Track security flaws and flaw resolution within the system, component, or service and report findings to [*personnel*].	This provides the flaw remediation aspects of SA-10.
		SA-11	**Developer Security Testing and Evaluation ‡** Organization requires the developer of the information system, system component, or	One of the items in this control requires a verifiable flaw remediation process and correction of any flaws

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 service to: • [⋮] • Implement a verifiable flaw remediation process; • Correct flaws identified during security testing/evaluation.	identified during testing.
		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.
		CA-8	**Penetration Testing** • Organization conducts penetration testing [*frequency*] on [*information systems or system components*].	AVA_VAN.1.3E supports CA-8 with respect to testing on the product.
		CA-8(1)	**Penetration Testing** | Independent Penetration Agent or Team • Organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components.	

Selection-Based 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_EXT.1	**Cryptographic Key Support** Cryptographic Key Support (REK) • (1.4) A REK shall not be able to be read from or exported from the hardware.	No changes from controls supported by base requirement.		

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	**DTLS Protocol** DTLS Protocol • Product implements DTLS protocol in accordance with DTLS 1.0, DTLS 1.2 • Product 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.
		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_TLSC_EXT.1	**EAP TLS Protocol** EAP TLS Protocol • (1.5) Product presents the Supported Elliptic Curves Extension in the Client Hello with the following NIST curves: [*selection: secp256r1, secp384r1, secp521r1*] and no other curves.	No changes from controls supported by base requirement.		
FCS_TLSC_EXT.2	**TLS Protocol** TLS Protocol • (2.5) Product presents the Supported Elliptic Curves Extension in the Client Hello with the following NIST curves: [*selection: secp256r1, secp384r1, secp521r1*] and no other curves.	No changes from controls supported by base requirement.		
FPT_TST_EXT.2	**TSF Functionality Testing** TSF Integrity Testing • Product does not execute code if the code signing certificate is deemed invalid.	No changes from controls supported by base requirement.		

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.2	**Trusted Update** Trusted Update Verification • Product does not install code if the code signing certificate is deemed invalid.	No changes from controls supported by base requirement.		

Objective 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	**Security Audit Data Generation** Audit Data Generation • Product generates audit records for [*set of events*] that includes startup and shutdown of audit. • Product records within the audit record at least date, time, type, instigator, outcome, and [*event specific information*]	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.
		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).

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
		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.	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.
		SI-7(8) †	**Software, Firmware, and Information Integrity** | Auditing Capability for Significant Events • Information system, upon detection of a potential integrity violation, provides the capability to audit the event and initiates the following actions: [*(one or more): generates an audit record; alerts current user; alerts [personnel or roles]; [other actions]*].	To address SI-7(8), FAU_GEN.1 should be completed to include auditing of integrity violations.
FAU_SAR.1	**Security Audit Review** Audit Review • The product provides [**the administrator**] with the ability to read [**[all audited events and record contents**] from audit records. • The product provides audit records in a usable form.	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.	AU-6(7) specifies the permitted actions for specific users/roles with respect to audit. The SFR prohibits read access; this is a special case of AU-6(7).
		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.	AU-7 requires an audit reduction and report capability. FAU_SAR.1 appears to address that, although it does not cover all aspects of AU-7 explicitly. **Note:** The SFR doesn't address or mention "on-demand" aspects, although those are inferred. The SFR also does not address not altering the content or time sequencing of audit records.
		AU-9	**Protection of Audit Information** Information system	AU-9 protects audit information from unauthorized access,

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
			protects audit information and audit tools from unauthorized access, modification, and deletion	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 users*].	AU-9(6) authorizes read-only access to a specific list of users. Depending upon the implementation of FAU_SAR.1, it may be addressed.
FAU_SEL.1	**Security Audit Event Selection** Selective Audit • Product can select the events to be audited from the set of auditable events based on [*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.
FAU_STG.1	**Security Audit Event Storage** Protected Audit Trail Storage • Product protects stored audit records from unauthorized deletion. • Product can [**prevent**] unauthorized modifications to stored audit records.	AU-9	**Protection of Audit Information** • Information system protects audit information and audit tools from unauthorized access, modification, and deletion	AU-9 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.
FAU_STG.4	**Security Audit Event Storage** Prevention of Audit Data Loss • Product [***overwriteS***] if the audit trail **is full**.	AU-4	**Audit Storage Capacity** • Organization allocates audit record storage in accordance with [*storage requirements*]	Implicit in the taking of actions if the audit trail is full is allocation of sufficient audit storage capability, which is part of AU-4
		AU-5	**Response to Audit Processing Failures** Information system… • Alerts [*personnel or roles*] in the event of an audit processing failure • Takes [additional actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].	AU-5 item b provides an assignment of actions to be taken for audit processing failures. FAU_STG.4 would support AU-5 item b if that assignment is completed in a congruent manner.

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 (WLAN) Product generates **symmetric** cryptographic keys in accordance with [PRF-704] and specified cryptographic key size [256 bits] using a Random Bit Generator as specified in FCS_RBG_EXT.1 that meet the following: [IEEE 802.11ac-2013].	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(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.	FCS_CKM.1(3) calls for a PRF algorithm and a standard RBG; as NSA developed the PP, it is by implication an NSA-approved technology and process.
		Note: See general comment regarding cryptographic algorithm usage.		
FCS_CKM_EXT.7	**Cryptographic Key Management** Extended: Bluetooth Key Generation Product randomly generates public/private ECDH key pairs every [assignment: frequency of and/or criteria for new key pair generation].	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.
		Note: See general comment regarding cryptographic algorithm usage.		

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_RBG_EXT.1.4/5	**Cryptographic Services** Random Bit Generation • Product can allow applications to add data to the deterministic RBG… using 800-90A	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_SRV_EXT.1	**Cryptographic Algorithm Services** Cryptographic Algorithm Services • (1.2) Product provides a mechanism for applications to request the TSF to perform the following cryptographic operations: □ Algorithms in FCS_COP.1(1) □ Algorithms in FCS_COP.1(3) by keys stored in the secure key storage.	No changes from controls supported by base requirement.	
FCS_TLSC_EXT.1	**EAP TLS Protocol** EAP TLS Protocol • (1.6) Product presents the signature_algorithms extension in the Client Hello with the supported_signature_algorithms value containing the following hash algorithms: [selection: SHA256, SHA384, SHA512] and no other hash algorithms. • (1.7) Product supports secure renegotiation through use of the "renegotiation_info" TLS extension in accordance with RFC 5746. • (1.8) Product includes [selection: choose only one of: renegotiation_info extension, TLS_EMPTY_RENEGOTIATION_INFO_SCSV ciphersuite] in the ClientHello message.	No changes from controls supported by base requirement.	
FCS_TLSC_EXT.2	**TLS Protocol** TLS Protocol • (2.6) Product presents the signature_algorithms extension in the Client Hello with the supported_signature_algorithms value containing the following hash algorithms: [selection: SHA256, SHA384, SHA512] and no other hash algorithms. • (2.7) Product supports secure renegotiation through use of the "renegotiation_info" TLS extension in accordance with RFC 5746. • (2.8) Product includes [selection: choose only one of:	No changes from controls supported by base requirement.	

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
	renegotiation_info extension, TLS_EMPTY_RENEGOTIATION_INFO_SCSV ciphersuite] in the ClientHello message.			
FDP_ACF_EXT.1	**Access Control** Security Access Control • (1.3) Product enforces access control policy that prohibits an application from granting both write and execute permission to a file.	AC-3†	**Access Enforcement** • Information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	The FDP_ACF_EXT.1 would have to align with the organization access control policy.
FDP_BLT_EXT.1.1	**Application Bluetooth Device Access** Extended: Limitation of Bluetooth Device Access • Product limits the applications that may communicate with a particular paired Bluetooth device	AC-4†	**Information Flow Enforcement** • Information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [*information flow control policies*].	The SFR appears to limit the flow of information between interconnected systems.
FDP_DAR_EXT.2	**Access Control** Data-at-Rest Protection • Encryption covers all sensitive data • Product uses asymmetric schcme to protect sensitive data received while the product is locked. • Product encrypts any stored symmetric key and any stored prive key of the asymmetric key… • Product decrypts the sensitive data received while in the locked state upon transitioning to the unlocked state using the asymmetric key scheme…	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 DAR protection.
		SC-28†	**Protection of Information at Rest** • Information system protects the [*(one or more): confidentiality; integrity*] of [*information at rest*].	Complete the assignment to cover protected data. This needs to agree with organizational requirements.
		SC-28(1)†	**Protection of Information at Rest** | Cryptographic Protection • Information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [*information*] on [*information system components*].	This addresses the use of cryptography
FIA_BLT_EXT.1	**Identification and Authentication** Bluetooth Authentication • (1.2) Product requires require explicit user authorization before granting trusted remote devices access to services associated with	No changes from controls supported by base requirement.		

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 following Bluetooth profiles: [assignment: list of Bluetooth profiles], and shall require explicit user authorization before granting untrusted remote devices access to services associated with the following Bluetooth profiles: [assignment: list of Bluetooth profiles].			
FIA_BLT_EXT.2	**Identification and Authentication** Bluetooth Authentication • Product requires Bluetooth mutual authentication between devices prior to any data transfer • Product discards connection attempts from a Bluetooth device address (BD_ADDR) to which a current connection already exists..	AC-18(1) †	**Wireless Access** | Authentication and Encryption • Information system protects wireless access to the system using authentication of [*(one or more): users; devices*] and encryption.	Assignment must be completed congruent with requirement.
		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.	Assignment must be completed congruent with requirement.
FIA_X509_EXT.2	**X509 Certificate Authentication** X509 Certificate Authentication • (2.3) Product generates a Certificate Request Message as specified in RFC 2986 and be able to provide the following information in the request: public key and [selection: device-specific information, Common Name, Organization, Organizational Unit, Country]. • (2.4) Product validates the chain of certificates from the Root CA upon receiving the CA Certificate Response.	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; • […]	
		SC-17†	**Public Key Infrastructure Certificates** • Organization issues public key certificates under an [*certificate policy*] or obtains public key certificates from an approved service provider.	SFR supports implementation of PKI.
FIA_X509_EXT.4	**X509 Certificate Authentication** X509 Certificate Enrollment • Product uses the Enrollment over Secure Transport (EST) protocol as specified in RFC 7030 to request certificate enrollment using the simple enrollment method described in RFC 7030	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	

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
	Section 4.2. • Product is capable of authenticating EST requests using an existing certificate and corresponding private key as specified by RFC 7030 Section 3.3.2. • Product is capable of authenticating EST requests using HTTP Basic Authentication with a username and password as specified by RFC 7030 Section 3.2.3. • Product performs authentication of the EST server using an Explicit Trust Anchor following the rules described in RFC 7030, section 3.6.1. • Product is capable of requesting server-provided private keys as specified in RFC 7030 Section 4.4. • Product is capable of updating its EST-specific Trust Anchor Database using the "Root CA Key Update" process described in RFC 7030 Section 4.1.3. • Product generates a Certificate Request Message for EST as specified in RFC 2986 and be able to provide the following information in the request: public key and [selection: device-specific information, Common Name, Organization, Organizational Unit, Country].		including checking certificate status information; • […]	
FPT_AEX_EXT.1	**Anti-Exploitation Services** Address Space Randomization • (1.3) Product shall provide address space randomization to the kernel	SI-16†	**Memory Protection** • Information system implements [*security safeguards*] to protect its memory from unauthorized code execution.	Assignment must be completed in a congruent fashion.
FPT_AEX_EXT.2	**Anti-Exploitation Services** Memory Page Permissions • (2.2) Product shall be able to enforce that write and execute permissions are not simultaneously granted on every page of physical memory.	SI-16†	**Memory Protection** • Information system implements [*security safeguards*] to protect its memory from unauthorized code execution.	Assignment must be completed in a congruent fashion.
FPT_AEX_EXT.3	**Anti-Exploitation Services** Memory Page Permissions • (3.2) Product includes heap-based buffer overflow protections in the runtime environment it provides to processes that execute on the application processor.	SI-16†	**Memory Protection** • Information system implements [*security safeguards*] to protect its memory from unauthorized code execution.	Assignment must be completed in a congruent fashion.

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_BBD_EXT.1	**Isolation of Baseband** Application Processor Mediation • Code executing on any baseband processor shall not be able to access application processor resources.	SC-2	**Application Partitioning** • Information system separates user functionality (including user interface services) from information system management functionality.	The SFR appears to support this.
		SI-16†	**Memory Protection** • Information system implements [*security safeguards*] to protect its memory from unauthorized code execution.	Assignment must be completed in a congruent fashion.
FPT_BLT_EXT.1	**Bluetooth Profile Limiting** Extended: Limitation of Bluetooth Profile Support • Product disables support for [assignment: list of Bluetooth profiles] Bluetooth profiles when they are not currently being used by an application on the Mobile Device, and shall require explicit user action to enable them.	AC-18	**Wireless Access** Organization… • Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access • Authorizes wireless access to the information system prior to allowing such connections.	This would fit in with supporting usage restrictions.
FPT_NOT_EXT.1	**Self-Test Event Notification** Event Notification • (1.2) Product [selection: logs, provides the administrator with] TSF-software integrity verification values. • (1.3) Product cryptographically signs all integrity verification values.	No changes from controls supported by base requirement.		
FPT_TUD_EXT.2	**Trusted Update** Trusted Update Verification • (2.5) Product by default only accepts mobile applications cryptographically signed by [acceptable certs] • (2.7) Product verifies software updates are a current or later versions	No changes from controls supported by base requirement.		
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	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.

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
			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.	