Mapping Between

Protection Profile for Mobile Device Fundamentals, Version 3.3, 9 September 2022

and

NIST SP 800-53 Revision 5

Important Caveats

- **Product vs. System.** The Common Criteria is designed for the evaluation of products; the Risk Management Framework (NIST SP 800-37 Revision 2, DOD 8510.01) and associated control/control interpretations (NIST SP 800-53 Revision 5, CNSSI № 1253) are used for the assessment and authorization of mission systems. **Products cannot satisfy controls outside of the system context**. Products may support a system satisfying particular controls, but typically satisfaction also requires the implementation of operational procedures; further, given that systems are typically the product of integration of multiple products configured to meet mission requirements, an overall system assessment is required to determine if the control is satisfied in the overall system context.

- **Granularity of SFRs vs controls.** It is important to remember that the Security Functional Requirements (SFRs) and the Security and Privacy Controls (Controls) are at completely different levels of abstractions. SFRs can be very low level, specifying internal characteristics and behaviors of given functions. Even when broader, SFRs are restricted to a specific product. Controls, on the other hand, are very high level, specifying both technical behavior and processes for the system writ large, broadly across the large number of devices, components and products that make up the system and achieve the overall mission. A low-level SFR may contribute in some small way towards the satisfaction of a control, but it rarely satisfies the control in isolation and should not be interpreted as doing so. More often, the combination of SFRs that define the security functionality of a product may serve to support just a single control, and looking at the finer level of detail may not be as useful, such as the low-level details of protocol implementations. When looking at these mappings, it is important to remember the differences in levels of abstraction; in particular, it is important not to read more into an SFR to Control mapping than a contribution of some level of support.

- **SA-4(7).** Perhaps it is needless to say, but satisfaction of any NIAP PP supports system satisfaction of SA-4(7), which is the implementation of CNSSP № 11.

- **System context of supported controls.** For a conformant TOE to support these controls in the context of an information system, the selections and assignments completed in the TOE’s Security Target must be congruent with those made for the supported controls. For example, the TOE’s ability to generate audit records only supports AU-2 to the extent that the TOE’s audit records are included in the set of “organization-defined auditable events” assigned by that control. The security control assessor must compare the TOE’s functional claims to the behavior required for the system to determine the extent to which the applicable controls are supported.

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
Mandatory Requirements (presented alphabetically)				
FAU_GEN.1	**Audit Data Generation**	AU-2	**Event Logging**	A conformant TOE has the ability to generate audit records for various events. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
		AU-3	**Content of Audit Records**	A conformant TOE will ensure that audit records include date, type, outcome, and subject identity data. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
		AU-3(1)	**Content of Audit Records:** Additional Audit Information	A conformant TOE will generate audit information for some auditable events beyond what is mandated in AU-3. This may or may not be sufficient to satisfy this control based on the additional audit information required by the organization. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
		AU-12	**Audit Record Generation**	A conformant TOE has the ability to generate audit logs. The TOE

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
FAU_SAR.1	**Audit Review**	AU-6(7)	**Audit Record Review, Analysis, and Reporting:** Permitted Actions	A conformant TOE will allow designation of permitted actions to their respective roles.
		AU-7	**Audit Record Reduction and Report Generation**	A conformant TOE provides audit review mechanisms to administrators.
FAU_STG.1	**Audit Storage Protection**	AU-9	**Protection of Audit Information**	A conformant TOE has the ability to prevent unauthorized modification and deletion of audit records.
FAU_STG.4	**Prevention of Audit Data Loss**	AU-5	**Response to Audit Logging Process Failures**	A conformant TOE has the ability to react in a specific manner when the allocated audit storage space is full, which supports part (b) of the control.
FCS_CKM.1	**Cryptographic Key Generation**	SC-12	**Cryptographic Key Establishment and Management**	The ability of the TOE to generate symmetric and asymmetric keys satisfies the key generation portion of this control.
		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	A conformant TOE's ensures that generated asymmetric keys provide an appropriate level of security.
FCS_CKM.2/UNLOCKED	**Cryptographic Key Establishment**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports this control by providing a key establishment function.
		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	A conformant TOE supports the production of asymmetric keys by providing a key establishment function.

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
FCS_CKM.2/LOCKED	**Cryptographic Key Establishment**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports this control by providing a key establishment function.
FCS_CKM_EXT.1	**Cryptographic Key Support**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE uses a REK to ensure secure key storage, satisfying the key storage portion of this control.
FCS_CKM_EXT.2	**Cryptographic Key Random Generation**	SC-12(2)	**Cryptographic Key Establishment and Management:** Symmetric Keys	A conformant TOE will support the production of symmetric keys by ensuring that sufficient entropy is made available to the key generation function when a (symmetric) DEK is generated.
FCS_CKM_EXT.3	**Cryptographic Key Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE provides a key generation function through some combination of password-based key derivation and other methods.
		SC-12(2) or SC-12(3)	**Cryptographic Key Establishment and Management:** Symmetric Keys -or- **Cryptographic Key Establishment and Management:** Asymmetric Keys	A conformant TOE may support either or both of these controls, depending on whether the TSF uses symmetric KEKs, asymmetric KEKs, or both.
FCS_CKM_EXT.4	**Key Destruction**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely destroy cryptographic keys.
FCS_CKM_EXT.5	**TSF Wipe**	AC-7(2)	**Unsuccessful Logon Attempts:** Purge or Wipe Mobile Device	The TOE supports the enforcement of this control by providing a wipe mechanism that can be invoked in response to excessive authentication failures. Note that the actual trigger for causing the wipe event in this

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
				situation is defined as FIA_AFL_EXT.1.
		MP-6	**Media Sanitization**	A conformant TOE supports this control by providing an interface to wipe TSF data.
		MP-6(8)	**Media Sanitization:** Remote Purging or Wiping of Information	This control is supported through the existence of a wipe mechanism that can be engaged remotely under certain conditions (i.e. if the mobile device is enrolled with an MDM). Note that implementation of this SFR means that the interface to perform the wipe operation exists; an environmental component must enforce the control through invoking it.
FCS_CKM_EXT.6	**Salt Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE generates salts in support of various key generation and establishment functions.
FCS_COP.1/CONDITION	**Cryptographic Operation**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform password-based key derivation using NSA-approved and FIPS-validated algorithms.
FCS_COP.1/ENCRYPT	**Cryptographic Operation**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform symmetric encryption and decryption using NSA-approved and FIPS-validated algorithms.
FCS_COP.1/HASH	**Cryptographic Operation**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform cryptographic hashing using NSA-approved and FIPS-validated algorithms.

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
FCS_COP.1/KEYHMAC	**Cryptographic Operation**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform keyed-hash message authentication using NSA-approved and FIPS-validated algorithms.
FCS_COP.1/SIGN	**Cryptographic Operation**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform cryptographic signing using NSA-approved and FIPS-validated algorithms.
FCS_HTTPS_EXT.1	**HTTPS Protocol**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting data in transit.
FCS_IV_EXT.1	**Initialization Vector Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to generate initialization vectors that ensure the secure operation of cryptographic functions.
FCS_RBG_EXT.1	**Random Bit Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE's use of an appropriate DRBG ensures that generated keys provide an appropriate level of security.
FCS_SRV_EXT.1	**Cryptographic Algorithm Services**	SC-13	**Cryptographic Protection**	A conformant TOE supports this control by providing an interface to the cryptographic services provided by the TSF, which can then be used for various cryptographic operations.
FCS_STG_EXT.1	**Cryptographic Key Storage**	AC-3(11)	**Access Enforcement:** Restrict Access to Specific Information Types	A conformant TOE restricts access to the key storage repository, which supports this control if such a repository is identified by the organization as requiring

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				restricted access.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely store cryptographic keys.
		SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE has the ability to securely store cryptographic keys.
FCS_STG_EXT.2	**Encrypted Cryptographic Key Storage**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE will use a key hierarchy to ensure the secure storage of cryptographic keys.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	A conformant TOE will use encryption to ensure the security of stored cryptographic data at rest.
		SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE has the ability to securely store cryptographic keys.
FCS_STG_EXT.3	**Integrity of Encrypted Key Storage**	SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE has the ability to securely store cryptographic keys.
		SI-7(6)	**Software, Firmware, and Information Integrity:** Cryptographic Protection	A conformant TOE uses cryptographic methods to ensure the integrity of stored data.
FDP_ACF_EXT.1	**Access Control for System Services**	AC-3	**Access Enforcement**	A conformant TOE can provide a mechanism/access policy to restrict access to system services and stored data by applications or groups of applications. This supports the control provided that the restrictions that can be enforced by the TSF are consistent with organizational policies as defined by AC-1.

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
		AC-3(12)	**Access Enforcement:** Assert and Enforce Application Access	A conformant TOE supports an access control policy to limit the system services that applications can access.
		AC-6	**Least Privilege**	A conformant TOE supports this control by providing the ability to restrict system services and data to its applications to the minimum set required for their use.
FDP_DAR_EXT.1	**Protected Data Encryption**	AC-19(5)	**Access Control for Mobile Devices:** Full Device or Container-based Encryption	The device storage is encrypted using a DEK.
		SC-28	**Protection of Information at Rest**	A conformant TOE provides a method to protect information at rest.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	The specific method used by the TOE to protect information at rest is encrypted storage.
FDP_DAR_EXT.2	**Sensitive Data Encryption**	AC-3	**Access Enforcement**	A conformant TOE supports this control by providing a mechanism to mark certain data as sensitive. Note however that this support relies on this behavior being part of the organization's access control policies as defined by AC-1.
		AC-3(11)	**Access Enforcement:** Restrict Access to Specific Information Types	A conformant TOE supports this control by providing a mechanism to encrypt sensitive data when the TOE is in its locked state. Sensitive data may include specific repositories and their contents, so the control is satisfied to the extent that these are listed as repositories that the organization protects.
		SC-12	**Cryptographic**	A conformant TOE can

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
			Key Establishment and Management	use this functionality in order to meet organizational requirements for secure key storage. Specifically, cryptographic storage (as defined by FCS_STG_EXT.2) is the method by which stored key data is protected.
		SC-28	**Protection of Information at Rest**	The TOE supports this control by providing a method to define the specific information at rest that should be protected.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	The TOE supports this control by providing a cryptographic mechanism that can be used to protect sensitive data.
FDP_IFC_EXT.1	**Subset Information Flow Control**	AC-17(2)	**Remote Access:** Protection of Confidentiality and Integrity Using Encryption	The SFR allows a conformant TOE to implement secure remote access using a VPN.
		SC-7(7)	**Boundary Protection:** Split Tunneling for Remote Devices	A conformant TOE prevents split tunneling by requiring all traffic to flow through the VPN client.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE supports this control by securing data in transit.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TSF's method of securing data in transit is through the use of an IPsec VPN.
FDP_STG_EXT.1	**User Data Storage**	AC-3(11)	**Access Enforcement:** Restrict Access to Specific Information Types	A conformant TOE restricts access to the trust anchor database, which supports this control if such a repository is identified by the organization as requiring restricted access.
		SC-12	**Cryptographic Key Establishment**	A conformant TOE supports this control by securing the contents of

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
			and Management	the Trust Anchor Database, which contains private key data.
FDP_UPC_EXT.1/APPS	**Inter-TSF User Data Transfer Protection (Applications)**	AC-4(21)	**Information Flow Enforcement:** Physical or Logical Separation of Information Flows	A conformant TOE allows information flows to be separated based on the protocols and/or radios used by different applications on the device.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE will support this control by providing a protected communication channel between mobile applications and remote trusted IT products.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The protected communications implemented by the TOE use cryptographic methods to secure data in transit.
		SC-11	**Trusted Path**	A conformant TOE supports this control by providing a trusted path from the user of the device to remote trusted IT products through user-facing applications.
FIA_AFL_EXT.1	**Authentication Failure Handling**	AC-7	**Unsuccessful Logon Attempts**	A conformant TOE has the ability to detect when a defined number of unsuccessful authentication attempts occur and take some action based on this.
		AC-7(2)	**Unsuccessful Logon Attempts:** Purge or Wipe Mobile Device	A conformant TOE has the ability to wipe all protected data once the defined number of unsuccessful authentication attempts has been reached.
FIA_PMG_EXT.1	**Password Management**	IA-5(1)	**Authenticator Management:** Password-Based Authentication	A conformant TOE will have the ability to enforce some minimum password complexity requirements, although they are not identical to

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
				CNSS or DoD requirements or to those specified in part (f) and (h) of this control.
FIA_TRT_EXT.1	**Authentication Throttling**	AC-7	**Unsuccessful Logon Attempts**	A conformant TOE supports this control by enforcing a delay between unsuccessful authentication attempts.
FIA_UAU.5	**Multiple Authentication Mechanisms**	IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE will require user identification and authentication before permitting access to the mobile device.
		IA-2(1)	**Identification and Authentication (Organizational Users):** Multi-Factor Authentication to Privileged Accounts	A conformant TOE may provide multi-factor authentication in order to access the mobile device.
		IA-2(2)	**Identification and Authentication (Organizational Users):** Multi-Factor Authentication to Non-Privileged Accounts	A conformant TOE may provide multi-factor authentication in order to access the mobile device.
		IA-5(12)	**Authenticator Management:** Biometric Authentication Performance	A conformant TOE may offer biometric verification as a form of authentication.
FIA_UAU.6/CREDENTIAL	**Re-Authenticating (Credential Change)**	IA-11	**Re-Authentication**	A conformant TOE supports this control by requiring re-authentication upon change of any authentication factor. Note that this control is only supported to the extent that this behavior represents an ‘organization-defined’ situation for it to occur.
FIA_UAU.6/LOCKED	**Re-Authenticating**	AC-11	**Device Lock**	A compliant TOE

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
	TSF Lock)			supports this control by requiring user re-authentication following a TSF initiated lock or user initiated lock condition.
FIA_UAU.7	**Protected Authentication Feedback**	IA-6	**Authentication Feedback**	The TOE is required to provide obscured feedback to the user while authentication is in progress.
FIA_UAU_EXT.1	**Authentication for Cryptographic Operation**	SC-28	**Protection of Information at Rest**	A compliant TOE supports this control by protecting information at rest until the device user is authenticated.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	A compliant TOE supports this control by enforcing cryptographic protection of information at rest.
FIA_UAU_EXT.2	**Timing of Authentication**	AC-14	**Permitted Actions Without Identification of Authentication**	A conformant TOE will define a list of actions that are permitted prior to authentication.
FIA_X509_EXT.1	**X.509 Validation of Certificates**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE has the ability to validate certificate path and status.
		SC-23(5)	**Session Authenticity:** Allowed Certificate Authorities	A conformant TOE supports this control because the SFR requires the certificate path to terminate with a certificate in the trust anchor database. This means that the TSF has the capability to reject a certificate based on its issuer not being trusted. This allows the TOE to conform to an organizational policy to accept only those certificates that are signed by a trusted issuer, as long as those issuers are designated in the system as trust anchors.
FIA_X509_EXT.2	**X509 Certificate Authentication**	AC-18(1)	**Wireless Access:** Authentication	A conformant TOE supports the

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
			and Encryption	authentication portion of this control by requiring X.509 authentication for remote trusted communications.
		CM-14	**Signed Components**	**(selection-dependent)** A conformant TOE may support this control by requiring the use of X.509 certificates for update integrity verification, depending on selections made.
		IA-3 -or- IA-9	**Device Identification and Authentication** **-or-** **Service Identification and Authentication**	A conformant TOE supports one of these controls by using X.509 certificates to authenticate remote entities with which the TSF attempts to connect to via a trusted protocol. Which control is supported depends on whether the presented certificate represents a device or a service running on a particular device (e.g. in a case where a single device has different certificates used for different services).
		IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	**(selection-dependent)** A conformant TOE may support this control if the TSF uses X.509 authentication for a trusted channel that requires client authentication, such as mutually-authenticated TLS.
		SI-7(15)	**Software, Firmware, and Information Integrity:** Code Authentication	**(selection-dependent)** A conformant TOE may use X.509 certificates to authenticate software updates to the TOE, depending on selections made.
FIA_X509_EXT.3	**Request Validation of Certificates**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE supports this control in part by providing an interface to perform

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
				certificate validation.
FMT_MOF_EXT.1	**Management of Security Functions Behavior**	AC-3	**Access Enforcement**	A conformant TOE supports this control by providing access control restrictions to various functions. Note that the extent of support depends on the extent to which this behavior is captured in the organizational access control policies defined by AC-1.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE supports this control by providing different role-based levels of management functionality to users, administrators, and MDM.
		AC-6	**Least Privilege**	A conformant TOE supports the concept of least privilege by limiting device management functions to only the roles that are needed to perform them.
		AC-6(1)	**Least Privilege:** Authorize Access to Security Functions	A conformant TOE will enforce access restrictions such that users are not granted excessive administrative privileges to manage the TSF.
		AC-6(10)	**Least Privilege:** Prohibit Non-Privileged Users from Executing Privileged Functions	A conformant TOE supports this control by defining some management functionality as privileged such that ordinary users cannot perform these functions.
FMT_SMF.1	**Specification of Management Functions**	AC-2(5)	**Account Management:** Inactivity Logout	If optional functionality for configuration of screen lock and/or remote connection inactivity timeout is selected, a conformant TOE has the ability to enforce inactivity logout mechanisms.

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
		AC-14	**Permitted Actions without Identification or Authentication**	The ability of a conformant TOE to configure the unauthenticated services that are available to it allows for the implementation of an access control policy.
		AC-17	**Remote Access**	If optional functionality for configuration of a remote management server is selected, a conformant TOE has the ability to implement remote access in accordance with an organizational policy.
		AU-4	**Audit Log Storage Capacity**	If optional functionality for configuration of audit storage capacity is selected, a conformant TOE will have the ability to satisfy this control.
		AU-4(1)	**Audit Log Storage Capacity:** Transfer to Alternate Storage	If optional functionality for configuration of remote audit/logging server is selected, a conformant TOE has the ability to offload audit data to alternate storage.
		AU-9(4)	**Protection of Audit Information:** Access by Subset of Privileged Users	This will allow a conformant TOE to assign responsibilities for management of the audit data.
		AU-12	**Audit Record Generation**	If optional functionality for configuration of audit rules is selected, a conformant TOE satisfies the control related to the ability to select the events audited by the system.
		CM-6	**Configuration Settings**	A conformant TOE may satisfy one or more optional capabilities defined in this SFR. In general, a conformant TOE will satisfy this control to the extent that

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				the TOE provides a method to configure its behavior in accordance with STIGs or other organizational requirements. Specific additional controls may be supported depending on the functionality claimed by the TOE; the security control assessor must review what has been selected in the Security Target and determine what additional support is provided, if any.
		CM-11	**User-Installed Software**	A conformant TOE will provide the ability to enforce restrictions on the software that users can install on the mobile device.
		IA-4	**Identifier Management**	If the optional management function for directory server configuration is selected, a conformant TOE has the ability to support identifier management through connection to a centralized directory server.
		IA-5	**Authenticator Management**	If management functions for the composition of user/administrator passwords are selected, a conformant TOE has mechanisms used to ensure strength of secrets for passwords.
		SC-7	**Boundary Protection**	If optional management functionality for enabling/disabling use of external interfaces is selected, a conformant TOE has the ability to ensure that connectivity to it occurs only through managed and monitored interfaces.
		SC-7(14)	**Boundary**	If optional management

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
			Protection: Protect Against Unauthorized Physical Connections	functionality for the ability to enable/disable use of USB ports is selected, a conformant TOE has the ability to restrict physical access to the information system.
FMT_SMF_EXT.2	**Specification of Remediation Actions**	MP-6(8)	**Media Sanitization:** Remote Purging or Wiping of Information	A conformant TOE supports this control by providing the ability to perform a wipe of enterprise data upon un-enrollment of the mobile device.
FPT_AEX_EXT.1	**Application Address Space Layout Randomization**	SI-16	**Memory Protection**	A conformant TOE will provide ASLR and for the base address of any user-space memory to consist of at least 8 unpredictable bits that addresses the control's broader requirement for memory protection.
FPT_AEX_EXT.2	**Memory Page Permissions**	SI-16	**Memory Protection**	A conformant TOE will have the ability to enforce read, write and execute permissions on every page of physical memory that addresses the control's broader requirement for memory protection.
FPT_AEX_EXT.3	**Stack Overflow Protection**	SI-16	**Memory Protection**	A conformant TOE has the ability to prevent unauthorized code execution.
FPT_AEX_EXT.4	**Domain Isolation**	SC-39	**Process Isolation**	The TOE's enforced isolation of address spaces between applications is addressed by this control. The isolation of address spaces also serves to protect processes against modification by other processes.
		SC-3	**Security Function Isolation**	A conformant TOE has the ability to isolate non-security from security functions in order to prevent any tampering or unauthorized access.

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
FPT_JTA_EXT.1	**JTAG Disablement**	SI-16	**Memory Protection**	A conformant TOE supports this control by preventing unauthorized access to system memory through a JTAG interface.
FPT_KST_EXT.1	**Key Storage**	AC-3(11)	**Access Enforcement:** Restrict Access to Specific Information Types	A conformant TOE stores key data in such a way that it is never placed in readable persistent storage as plaintext. This supports the control by ensuring that key data is always stored in a location where access to it can be restricted.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the key storage portion of this control by ensuring that cryptographic key data is not stored insecurely.
		SC-28	**Protection of Information at Rest**	A conformant TOE can support this control if the organization defines key data as information at rest that is subject to protection.
FPT_KST_EXT.2	**No Key Transmission**	IA-5	**Authenticator Management**	A conformant TOE supports part (g) of this control by ensuring that any secret key data that may be used as part of an authenticator is not transmitted outside the TOE boundary.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the key storage portion of this control by ensuring that cryptographic key data is not transmitted outside the TOE boundary.
FPT_KST_EXT.3	**No Plaintext Key Export**	IA-5	**Authenticator Management**	A conformant TOE supports part (g) of this control by ensuring that any secret key data that may be used as part of an authenticator is not exported from the TOE.
		SC-12	**Cryptographic Key**	A conformant TOE supports the key storage

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
			Establishment and Management	portion of this control by ensuring that cryptographic key data is not exported from the TOE.
FPT_NOT_EXT.1	**Self-Test Notification**	SI-6	**Security and Privacy Function Verification**	A conformant TOE may support part (c) of this control if the SFR selection includes notifying the administrator of a self-test failure. By transitioning to a non-operational mode. The TSF also satisfies part (d) of this control through implementation of a failure response.
		SI-7(8)	**Software, Firmware, and Information Integrity:** Auditing Capability for Significant Events	**(selection-dependent)** A conformant TOE may have the ability to audit failed integrity tests depending on the selections made in this SFR. Note that the SFR applies to all self-test failures in general, but only those related to integrity apply to this control.
		SC-24	**Fail in Known State**	**(selection-dependent)** A conformant TOE will transition into the locked state upon the detection of a self-test failure and potentially other failures depending on the selections made in this SFR.
FPT_STM.1	**Reliable Time Stamps**	AU-8	**Time Stamps**	A conformant can generate and use time stamps addresses the actions defined in this control.
		SC-45	**System time Synchronization**	A conformant TOE can synchronize the TOE's internal clock with an NTP server or carrier network clock.
FPT_TST_EXT.1	**TSF Cryptographic Functionality**	SI-6	**Security and Privacy Function Verification**	A conformant TOE has the ability to verify the correct operation of its

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
	Testing			cryptographic functionality.
FPT_TST_EXT.2/PREKERNEL	**TSF Integrity Checking (Pre-Kernel)**	SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE has the ability to verify the integrity of the TOE's software components that can be considered a subset of the actions available for selection and assignment in the SFR.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	A conformant TOE has the ability to verify the integrity of the boot chain prior to execution.
		SI-7(6)	**Software, Firmware, and Information Integrity:** Cryptographic Protection	A conformant TOE has the ability to implement cryptographic mechanisms to detect unauthorized change.
		SI-7(9)	**Software, Firmware, and Information Integrity:** Verify Boot Process	A conformant TOE has the ability to verify the integrity of the boot process.
FPT_TUD_EXT.1	**TSF Version Query**	CM-8	**System Component Inventory**	A conformant TOE supports this control to the extent that it unambiguously identify itself and any installed applications, which can be used as inputs when defining a component inventory.
FPT_TUD_EXT.2	**TSF Update Verification**	CM-14	**Signed Components**	A conformant TOE has the ability to require that third-party applications running on it use signed updates.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	A conformant TOE has the ability to verify the integrity of updates to itself.
FPT_TUD_EXT.3	**Application Signing**	CM-14	Signed Components	A conformant TOE will ensure that updates are not installed unless a valid code signing certificate is provided.
		SI-7(15)	**Software,**	A conformant TOE will

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
			Firmware, and Information Integrity: Code Authentication	ensure that updates are not installed unless a valid code signing certificate is provided.
FTA_SSL_EXT.1	**TSF- and User-Initiated Locked State**	AC-11	**Device Lock**	A conformant TOE has the ability to initiate a device lock after a defined period of time or upon user request
		AC-11(1)	**Device Lock:** Pattern-Hiding Displays	A conformant TOE has the ability obfuscate the display when in the locked state.
FTA_TAB.1	**Default TOE Access Banners**	AC-8	**System Use Notification**	The TOE displays an advisory warning to the user prior to authentication.
		PL-4	**Rules of Behavior**	The TOE displays an advisory warning to the user prior to authentication to identify the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy.
FTP_ITC_EXT.1	**Trusted Channel Communication**	IA-3	**Device Identification and Authentication**	A conformant TOE supports this control by providing 802.1X as a method of device authentication over a WLAN.
		IA-3(1)	**Device Identification and Authentication**: Cryptographic Bidirectional Authentication	The use of EAP-TLS as part of establishing WLAN communications allows a conformant TOE to support this control by providing cryptographic bidirectional authentication for wireless devices.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality**	The use of the cryptographic protocols

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
			and Integrity: Cryptographic Protection	specified in the SFR ensures the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
Optional Requirements (presented alphabetically)				
FIA_UAU_EXT.4	**Secondary User Authentication**	IA-2(1)	**Identification and Authentication (Organizational Users)**: Multi-Factor Authentication to Privileged Accounts	A conformant TOE has the ability to implement access control policies that prohibit access to Enterprise resources until a secondary authentication factor is provided by the user.
		IA-2(2)	**Identification and Authentication (Organizational Users):** Multi-Factor Authentication to Non-Privileged Accounts	A conformant TOE has the ability to implement access control policies that prohibit access to Enterprise resources until a secondary authentication factor is provided by the user.
Objective Requirements (presented alphabetically)				
FAU_SEL.1	**Selective Audit**	AU-12	**Audit Record Generation**	A conformant TOE has the ability to support part (b) of this control by providing a mechanism to determine the set of auditable events that result in the generation of audit records.
FCS_RBG_EXT.2	**Random Bit Generator State Preservation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the key generation function of this control through its handling of random bit generation.
FCS_RBG_EXT.3	**Support for Personalization String**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE's preservation of its DRBG state between power cycles provides assurance of availability for random bit generation services.
FCS_SRV_EXT.2	**Cryptographic Key Storage Services**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform encryption and decryption as well as

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
				cryptographic hashing and cryptographic signature services using NSA-approved and FIPS-validated algorithms.
FDP_ACF_EXT.3	**Security Attribute Based Access Control**	AC-3	**Access Enforcement**	A conformant TOE supports this control by preventing simultaneous write and execute permissions except in specific cases. This supports the control provided that enforcement of these restrictions is consistent with organizational policies as defined by AC-1.
FDP_BCK_EXT.1	**Application Backup**	N/A	N/A	While NIST SP 800-53 includes controls for the backup of information system data, there is no security control for the ability to deliberately exclude items from the backup function.
FDP_BLT_EXT.1	**Limitation of Bluetooth Device Access**	AC-3	**Access Enforcement**	A conformant TOE can enforce access control on the Bluetooth interface by limiting its use to certain applications only. This supports the control provided that enforcement of these restrictions is consistent with organizational policies as defined by AC-1.
		AC-18	**Wireless Access**	A conformant TOE requires a service to be authorized before it can communicate with a paired Bluetooth device.
		IA-9	**Service Identification and Authentication**	A conformant TOE supports identification of services by limiting the services that can invoke the Bluetooth interface.
FIA_X509_EXT.4	**X509 Certificate Enrollment**	AC-18(1)	**Wireless Access:** Authentication and Encryption	A conformant TOE supports the authentication portion of

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
				this control by supporting enrollment of certificates that are subsequently used for authentication.
		IA-5	**Authenticator Management**	A conformant TOE has the ability to request certificate enrollment which serves as initial authenticator content, satisfying part (b) of this control.
		IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE will validate certificate responses, satisfying part (a) of this control.
FIA_X509_EXT.5	**X509 Certificate Requests**	IA-5	**Authenticator Management**	A conformant TOE has the ability to generate certificate request messages that can be used to establish initial authenticator content, satisfying part (b) of this control.
		IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE will validate certificate responses, satisfying part (a) of this control.
FMT_SMF_EXT.3	**Current Administrator**	AC-6(7)	**Least Privilege:** Review of User Privileges	A conformant TOE will provide the ability to enumerate the administrators of the TOE and the privileges assigned to them.
FPT_AEX_EXT.5	**Kernel Address Space Layout Randomization**	SI-16	**Memory Protection**	A conformant TOE will provide ASLR and for the base address of any user-space memory to consist of at least 8 unpredictable bits that addresses the control's broader requirement for memory protection.
FPT_AEX_EXT.6	**Write or Execute Memory Page Permissions**	SI-16	**Memory Protection**	A conformant TOE will have the ability to enforce read, write and execute permissions on every page of physical memory that addresses the control's broader requirement for memory protection.

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
FPT_AEX_EXT.7	**Heap Overflow Protection**	N/A	N/A	There is no control that specifically relates to buffer overflow.
FPT_BBD_EXT.1	**Application Processor Mediation**	SC-3(1)	**Security Function Isolation:** Hardware Separation	A conformant TOE will separate baseband processor code from accessing application processor resources.
FPT_BLT_EXT.1	**Limitation of Bluetooth Profile Support**	IA-3	**Device Identification and Authentication**	A conformant TOE supports this control by providing a method to limit the devices that are permitted to be authenticated over the Bluetooth interface.
FPT_NOT_EXT.2	**Software Integrity Verification**	IA-3(4)	**Device Identification and Authentication:** Device Attestation	A conformant TOE will provide software integrity verification values as a method of device attestation.
FPT_TST_EXT.2/ POSTKERNEL	**TSF Integrity Checking (Post-Kernel)**	SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE has the ability to verify the integrity of the TOE's software components that can be considered a subset of the actions available for selection and assignment in the SFR.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	A conformant TOE has the ability to verify the integrity of executable code prior to execution.
		SI-7(6)	**Software, Firmware, and Information Integrity:** Cryptographic Protection	A conformant TOE has the ability to implement cryptographic mechanisms to detect unauthorized change.
FPT_TUD_EXT.5	**Application Verification**	CM-14	**Signed Components**	A conformant TOE will require an X.509v3 certificate in order to permit the installation of mobile applications.
FPT_TUD_EXT.6	**Trusted Update Verification**	N/A	**N/A**	While NIST SP 800-53 includes controls for software updates, there is no security control to ensure that a current or later version is installed

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				other than the current version.
Implementation-Based Requirements (presented alphabetically)				
FDP_UPC_EXT.1/BLUETOOTH	**Inter-TSF User Data Transfer Protection (Bluetooth)**	AC-18	**Wireless Access**	A conformant TOE has the ability to communicate with a paired Bluetooth device. The extent to which this functionality satisfies the control is based on the extent to which the supported Bluetooth functionality aligns with organizational policies for wireless access.
Selection-Based Requirements (presented alphabetically)				
FCS_CKM_EXT.7	**Cryptographic Key Support (REK)**	SC-12	**Cryptographic Key Establishment and Management**	If consistent with organizational requirements, a conformant TOE supports the key management portion of this control through ensuring appropriate measures for the generation and storage of its REK.
FDP_ACF_EXT.2	**Access Control for System Resources**	AC-3(11)	**Access Enforcement:** Restrict Access to Specific Information Types	A conformant TOE supports this control by enforcing access control against system repositories. The control is supported to the extent that these repositories align with those specified by the organization as requiring access control.
FPT_TST_EXT.3	**TSF Integrity Testing**	CM-14	**Signed Components**	A conformant TOE will ensure that code is not executed unless a valid code signing certificate is provided.
		SI-7(15)	**Software, Firmware, and Information Integrity:** Code Authentication	A conformant TOE will ensure that code is not executed unless a valid code signing certificate is provided.
FPT_TUD_EXT.4	**Trusted Update Verification**	CM-14	**Signed Components**	A conformant TOE will require an X.509v3 certificate in order to permit the installation of

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				mobile applications.