Extended Component Definitions

This appendix contains the definitions for the extended requirements that are used in the PP, including those used in Appendices A and B.

Background and Scope

This Appendix provides a definition for all of the extended components introduced in this PP. These components are identified in the following table:

Functional Class	Functional Components
Cryptographic Support (FCS)	FCS_CKM_EXT Cryptographic Key Management
	FCS_HTTPS_EXT HTTPS Protocol
	FCS_IV_EXT Initialization Vector Generation
	FCS_RBG_EXT Random Bit Generation
	FCS_SRV_EXT Cryptographic Algorithm Services
	FCS_STG_EXT Cryptographic Key Storage
User Data Protection (FDP)	FDP_ACF_EXT Access Control Functions
	FDP_BCK_EXT Application Backup
	FDP_BLT_EXT Limitation of Bluetooth Device Access
	FDP_DAR_EXT Data-at-Rest Encryption
	FDP_IFC_EXT Information Flow Control Policy
	FDP_PBA_EXT Storage of Critical Biometric Parameters
	FDP_STG_EXT User Data Storage
	FDP_UPC_EXT Inter-TSF User Data Transfer Protection
Identification and Authentication (FIA)	FIA_AFL_EXT Authentication Failures
	FIA_BMG_EXT Biometric Authentication
	FIA_PMG_EXT Password Management
	FIA_TRT_EXT Authentication Throttling
	FIA_UAU_EXT User Authentication
	FIA_X509_EXT X.509 Validation of Certificates
Security Management (FMT)	FMT_MOF_EXT Management of Functions in TSF
	FMT_SMF_EXT Specification of Management Functions
Protection of the TSF (FPT)	FPT_AEX_EXT Anti-Exploitation Capabilities
	FPT_BBD_EXT Application Processor Mediation
	FPT_BLT_EXT Limitation Bluetooth Profile Support
	FPT_JTA_EXT JTAG Disablement
	FPT_KST_EXT Key Storage
	FPT_NOT_EXT Self-Test Notification
	FPT_TST_EXT TSF Self Test
	FPT_TUD_EXT TSF Updates

Functional Class	Functional Components
TOE Access (FTA)	FTA_SSL_EXT Session Locking and Termination
Trusted Path/Channels (FTP)	FTP_ITC_EXT Inter-TSF Trusted Channel

Extended Component Definitions

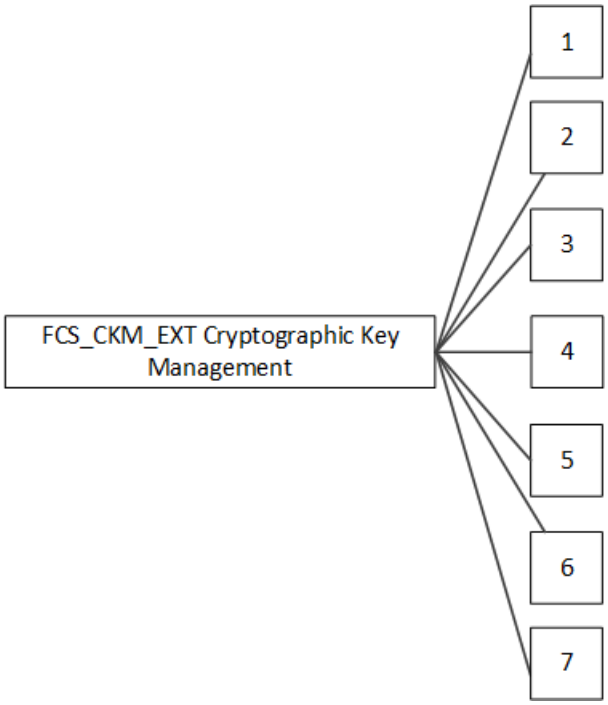
Class FCS: Cryptographic Support

FCS_CKM_EXT Cryptographic Key Management

Family Behavior

This family defines requirements for management of cryptographic keys that are not addressed by FCS_CKM in CC Part 2.

Component Leveling



FCS_CKM_EXT.1 Cryptographic Key Support, requires the TSF to implement a Root Encryption Key (REK).

FCS_CKM_EXT.2 Cryptographic Key Random Generation, requires the TSF to specify the mechanism it uses to generate Data Encryption Keys (DEKs).

FCS_CKM_EXT.3 Cryptographic Key Generation, requires the TSF to generate and manage the strength of Key Encryption Keys (KEKs).

FCS_CKM_EXT.4 Cryptographic Key Destruction, requires the TSF to be able to follow specified rules to destroy plaintext keying material and cryptographic keys when no longer needed.

FCS_CKM_EXT.5 TSF Wipe, requires the TSF to implement a cryptographic or other mechanism to make TSF data unreadable.

FCS_CKM_EXT.6 Salt Generation, requires the TSF to generate salts in a specified manner.

FCS_CKM_EXT.7 Cryptographic Key Support (REK), requires the TSF to prevent the reading or exporting of REKs.

Management: FCS_CKM_EXT.1

There are no management activities foreseen.

Audit: FCS_CKM_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Generation of a REK.

Management: FCS_CKM_EXT.2

There are no management activities foreseen.

Audit: FCS_CKM_EXT.2

There are no auditable events foreseen.

Management: FCS_CKM_EXT.3

There are no management activities foreseen.

Audit: FCS_CKM_EXT.3

There are no auditable events foreseen.

Management: FCS_CKM_EXT.4

There are no management activities foreseen.

Audit: FCS_CKM_EXT.4

There are no auditable events foreseen.

Management: FCS_CKM_EXT.5

The following actions could be considered for the management functions in FMT:

a) TSF wipe of protected data.
b) TSF wipe of enterprise data.

Audit: FCS_CKM_EXT.5

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Failure of the wipe.

Management: FCS_CKM_EXT.6

There are no management activities foreseen.

Audit: FCS_CKM_EXT.6

There are no auditable events foreseen.

Management: FCS_CKM_EXT.7

There are no management activities foreseen.

Audit: FCS_CKM_EXT.7

There are no auditable events foreseen.

FCS_CKM_EXT.1 Cryptographic Key Support

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.1 Random Bit Generation

FCS_CKM_EXT.1.1 The TSF shall support [**selection**: *immutable hardware*, *mutable hardware*] REK(s) with a [**selection**: *symmetric*, *asymmetric*] key of strength [**selection**: *112 bits*, *128 bits*, *192 bits*, *256 bits*].

FCS_CKM_EXT.1.2 Each REK shall be hardware-isolated from the OS on the TSF in runtime.

FCS_CKM_EXT.1.3 Each REK shall be generated by a RBG in accordance with FCS_RBG_EXT.1.

FCS_CKM_EXT.2 Cryptographic Key Random Generation

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.1 Random Bit Generation

FCS_CKM_EXT.2.1 All DEKs shall be [**selection**:

- *randomly generated*,
- *from the combination of a randomly generated DEK with another DEK or salt in a way that preserves the effective entropy of each factor by [**selection**: using an XOR operation, concatenating the keys and using a KDF (as described in SP 800-108), concatenating the keys and using a KDF (as described in SP 800-56C)]*

] with entropy corresponding to the security strength of AES key sizes of [**selection**: *128*, *256*] bits.

FCS_CKM_EXT.3 Cryptographic Key Generation

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic Key Generation

FCS_COP.1 Cryptographic Operation

FCS_RBG_EXT.1 Random Bit Generation

FCS_CKM_EXT.3.1 The TSF shall use **[selection:**

- *asymmetric KEKs of [**assignment**: security strength greater than or equal to 112 bits] security strength,*

- *symmetric KEKs of [**selection**: 128-bit, 256-bit] security strength corresponding to at least the security strength of the keys encrypted by the KEK*

].

FCS_CKM_EXT.3.2 The TSF shall generate all KEKs using one of the following methods:

- Derive the KEK from a Password Authentication Factor according to FCS_COP.1 and

[**selection**:

- *Generate the KEK using an RBG that meets this profile (as specified in FCS_RBG_EXT.1),*
- *Generate the KEK using a key generation scheme that meets this profile(as specified in FCS_CKM.1),*
- *Combine the KEK from other KEKs in a way that preserves the effective entropy of each factor by [**selection**: using an XOR operation, concatenating the keys and using a KDF (as described in SP800-108), concatenating the keys and using a KDF (as described in SP800-56C), encrypting one key with another]*

].

FCS_CKM_EXT.4 Cryptographic Key Destruction

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.1 Random Bit Generation

FCS_CKM_EXT.4.1 The TSF shall destroy cryptographic keys in accordance with the specified cryptographic key destruction methods:

- by clearing the KEK encrypting the target key
- in accordance with the following rules
  - For volatile memory, the destruction shall be executed by a single direct overwrite [**selection**: *consisting of a pseudo-random pattern using the TSF's RBG*, *consisting of zeroes*].
  - For non-volatile EEPROM, the destruction shall be executed by a single direct overwrite consisting of a pseudo random pattern using the TSF's RBG (as specified in FCS_RBG_EXT.1), followed by a read-verify.
  - For non-volatile flash memory, that is not wear-leveled, the destruction shall be executed [**selection**: *by a single direct overwrite consisting of zeros followed by a read-verify*, *by a block erase that erases the reference to memory that stores data as well as the data itself]*.
  - For non-volatile flash memory, that is wear-leveled, the destruction shall be executed [**selection**: *by a single direct overwrite consisting of zeros*, *by a block erase*].

- For non-volatile memory other than EEPROM and flash, the destruction shall be executed by a single direct overwrite with a random pattern that is changed before each write.

FCS_CKM_EXT.4.2 The TSF shall destroy all plaintext keying material and critical security parameters when no longer needed.

FCS_CKM_EXT.5 Cryptographic Key TSF Wipe

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.1 Random Bit Generation

FCS_CKM_EXT.5.1 The TSF shall wipe all protected data by [**assignment:** *wipe operation based on the type of memory in which the protected data resides*].

FCS_CKM_EXT.5.2 The TSF shall perform a power cycle on conclusion of the wipe procedure.

FCS_CKM_EXT.6 Cryptographic Key Salt Generation

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.1 Random Bit Generation

FCS_CKM_EXT.6.1 The TSF shall generate all salts using a RBG that meets FCS_RBG_EXT.1.

FCS_CKM_EXT.7 Cryptographic Key Support (REK)

Hierarchical to: No other components.

Dependencies: FCS_CKM_EXT.1 Cryptographic Key Support

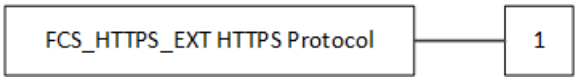
FCS_CKM_EXT.7.1 A REK shall not be able to be read from or exported from the hardware.

FCS_HTTPS_EXT HTTPS Protocol

Family Behavior

This family defines requirements for implementation of the HTTPS protocol.

Component Leveling



FCS_HTTPS_EXT.1 HTTPS Protocol, requires the TSF to implement the HTTPS protocol in accordance with the specified standard, using TLS, and notifying the application if invalid.

Management: FCS_HTTPS_EXT.1

The following actions could be considered for the management functions in FMT:

a) Configuring whether to allow/disallow establishment of a trusted channel if the peer/server certificate is deemed invalid.

Audit: FCS_HTTPS_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Failure of the certificate validity check.

FCS_HTTPS_EXT.1 HTTPS Protocol

Hierarchical to: No other components.

Dependencies: FIA_X509_EXT.1 X.509 Validation of Certificates

FMT_SMF.1 Specification of Management Functions

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as defined in [**assignment:** *specification that defines TLS implementation requirements*].

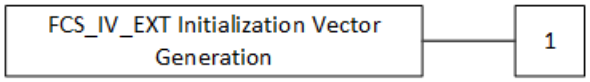
FCS_HTTPS_EXT.1.3 The TSF shall notify the application and [**selection**: *not establish the connection*, *request application authorization to establish the connection*, *no other action*] if the peer certificate is deemed invalid.

FCS_IV_EXT Initialization Vector Generation

Family Behavior

This family defines requirements for initialization vector generation in support of key generation.

Component Leveling



FCS_IV_EXT.1 Initialization Vector Generation, requires the TSF to generate IVs in accordance with a set of approved modes.

Management: FCS_IV_EXT.1

There are no management functions foreseen.

Audit: FCS_IV_EXT.1

There are no auditable events foreseen.

FCS_IV_EXT.1 Initialization Vector Generation

Hierarchical to: No other components.

Dependencies: No dependencies.

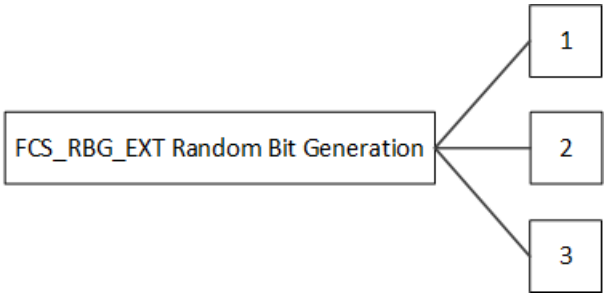
FCS_IV_EXT.1.1 The TSF shall generate IVs in accordance with Table 12: References and IV Requirements for NIST-approved Cipher Modes.

FCS_RBG_EXT Random Bit Generation

Family Behavior

This family defines requirements for the generation of random bits.

Component Leveling



FCS_RBG_EXT.1 Random Bit Generation, requires the TSF to generate random data with a certain amount of entropy and in accordance with applicable standards.

FCS_RBG_EXT.2 Random Bit Generator State Preservation, requires the TSF to save and restore the state of the RBG when powering off and starting up.

FCS_RBG_EXT.3 Support for Personalization String, requires the TSF to support a personalization string as a DRBG input parameter.

Management: FCS_RBG_EXT.1

There are no management functions foreseen.

Audit: FCS_RBG_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Failure of the randomization process.

Management: FCS_RBG_EXT.2

There are no management functions foreseen.

Audit: FCS_RBG_EXT.2

There are no auditable events foreseen.

Management: FCS_RBG_EXT.3

There are no management functions foreseen.

Audit: FCS_RBG_EXT.3

There are no auditable events foreseen.

FCS_RBG_EXT.1 Random Bit Generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with NIST Special Publication 800-90A using [**selection**: *Hash_DRBG*

(any), *HMAC_DRBG (any)*, *CTR_DRBG (AES)*].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from [**selection**: *a software-based noise source*, *TSF-hardware-based noise source*] with a minimum of [**selection**: *128 bits*, *256 bits*] of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.

FCS_RBG_EXT.1.3 The TSF shall be capable of providing output of the RBG to applications running on the TSF that request random bits.

FCS_RBG_EXT.2 Random Bit Generator State Preservation

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.1 Random Bit Generation

FCS_RBG_EXT.2.1 The TSF shall save the state of the deterministic RBG at power-off, and shall use this state as input to the deterministic RBG at startup.

FCS_RBG_EXT.3 Support for Personalization String

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.1 Random Bit Generation

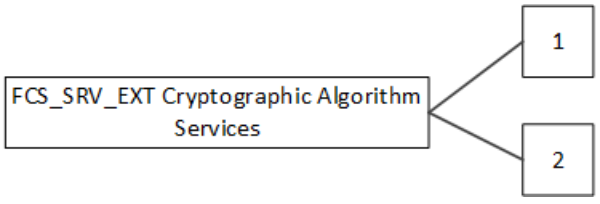
FCS_RBG_EXT.3.1 The TSF shall allow applications to add data to the deterministic RBG using the Personalization String as defined in SP 800-90A.

FCS_SRV_EXT Cryptographic Algorithm Services

Family Behavior

This family defines requirements for the ability of the TOE to make its cryptographic operations available to non-TSF components.

Component Leveling



FCS_SRV_EXT.1 Cryptographic Algorithm Services, requires the TSF to be able to perform specified mandatory and selected algorithms.

FCS_SRV_EXT.2 Cryptographic Key Storage Services, requires the TSF to be able to perform cryptographic operations.

Management: FCS_SRV_EXT.1

There are no management functions foreseen.

Audit: FCS_SRV_EXT.1

There are no auditable events foreseen.

Management: FCS_SRV_EXT.2

There are no management functions foreseen.

Audit: FCS_SRV_EXT.2

There are no auditable events foreseen.

FCS_SRV_EXT.1 Cryptographic Algorithm Services

Hierarchical to:	No other components.
Dependencies:	FCS_CKM.1 Cryptographic Key Generation
	FCS_COP.1 Cryptographic Operation
FCS_SRV_EXT.1.1	The TSF shall provide a mechanism for applications to request the TSF to perform the following cryptographic operations: [**assignment:** *cryptographic operations defined by the TSF in FCS_CKM.1 or FCS_COP.1*].

FCS_SRV_EXT.2 Cryptographic Key Storage Services

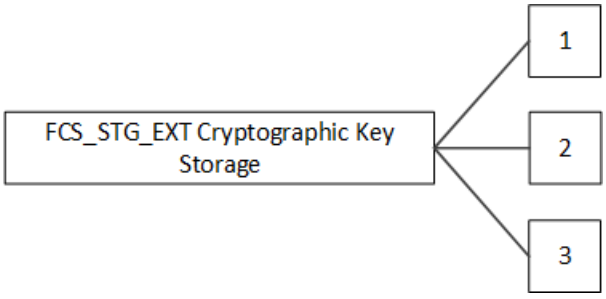
Hierarchical to:	No other components.
Dependencies:	FCS_COP.1 Cryptographic Operation
FCS_SRV_EXT.2.1	The TSF shall provide a mechanism for applications to request the TSF to perform the following cryptographic operations: [**assignment:** *cryptographic operations defined by the TSF in FCS_COP.1*] by keys stored in the secure key storage.

FCS_STG_EXT Cryptographic Key Storage

Family Behavior

This family defines requirements for the implementation of secure key storage with access control, confidentiality, and integrity protections.

Component Leveling



FCS_STG_EXT.1 Cryptographic Key Storage, requires the TSF to implement a secure key storage and defines the access restrictions to be enforced on this.

FCS_STG_EXT.2 Encrypted Cryptographic Key Storage, requires the TSF to implement confidentiality measures to protect the key storage.

FCS_STG_EXT.3 Integrity of Encrypted Key Storage, requires the TSF to implement integrity measures to protect the key storage.

Management: FCS_STG_EXT.1

The following actions could be considered for the management functions in FMT:

a) Importing keys/secrets into the secure key storage.
b) Destroying imported keys/secrets in the secure key storage.
c) Approving exceptions for shared use of keys/secrets by multiple applications.
d) Approving exceptions for destruction of keys/secrets by applications that did not import the key/secret

Audit: FCS_STG_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Import or destruction of key.
b) Exceptions to use and destruction rules.

Management: FCS_STG_EXT.2

There are no management functions foreseen.

Audit: FCS_STG_EXT.2

There are no auditable events foreseen.

Management: FCS_STG_EXT.3

There are no management functions foreseen.

Audit: FCS_STG_EXT.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Failure to verify integrity of stored key.

FCS_STG_EXT.1 Cryptographic Key Storage

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.1 Cryptographic Key Generation, or FDP_ITC.1 Import of User Data without Security Attributes, or FDP_ITC.2 Import of User Data with Security Attributes] FMT_SMR.1 Security Roles
FCS_STG_EXT.1.1	The TSF shall provide [**selection**: *mutable hardware*, *software-based*] secure key storage for asymmetric private keys and [**selection**: *symmetric keys*, *persistent secrets*, *no other keys*].
FCS_STG_EXT.1.2	The TSF shall be capable of importing keys/secrets into the secure key storage

upon request of [**selection**: *the user*, *the administrator*] and [**selection**: *applications running on the TSF*, *no other subjects*].

FCS_STG_EXT.1.3 The TSF shall be capable of destroying keys/secrets in the secure key storage upon request of [**selection**: *the user*, *the administrator*].

FCS_STG_EXT.1.4 The TSF shall have the capability to allow only the application that imported the key/secret the use of the key/secret. Exceptions may only be explicitly authorized by [**selection**: *the user*, *the administrator*, *a common application developer*].

FCS_STG_EXT.1.5 The TSF shall allow only the application that imported the key/secret to request that the key/secret be destroyed. Exceptions may only be explicitly authorized by [**selection**: *the user*, *the administrator*, *a common application developer*].

FCS_STG_EXT.2 Encrypted Cryptographic Key Storage

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic Operation

FCS_STG_EXT.1 Cryptographic Key Storage

FCS_STG_EXT.2.1 The TSF shall encrypt all DEKs, KEKs, [**assignment**: *any long-term trusted channel key material*] and [**selection**: *all software-based key storage*, *no other keys*] by KEKs that are [**selection**:

- *1. Protected by the REK with [**selection**:*
  - *a. encryption by a REK,*
  - *b. encryption by a KEK chaining from a REK,*
  - *c. encryption by a KEK that is derived from a REK*

  ] ,
- *2. Protected by the REK and the password with [**selection**:*
  - *a. encryption by a* REK *and the password-derived* KEK*,*
  - *b. encryption by a* KEK *chaining to a* REK *and the password-derived or biometric-unlocked* KEK*,*
  - *c. encryption by a* KEK *that is derived from a* REK *and the password-derived or biometric-unlocked* KEK

  ]

].

FCS_STG_EXT.2.2 DEKs, KEKs, [**assignment**: *any long-term trusted channel key material*] and [**selection**: *all software-based key storage*, *no other keys*] shall be encrypted using one of the following methods: [**selection**:

- *using a SP800-56B key establishment scheme*,
- *using AES in the [**selection**: Key Wrap (KW) mode, Key Wrap with Padding (KWP) mode, GCM, CCM, CBC mode]*

].

FCS_STG_EXT.3 Integrity of Encrypted Key Storage

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic Operation

FCS_STG_EXT.2 Encrypted Cryptographic Key Storage

FCS_STG_EXT.3.1 The TSF shall protect the integrity of any encrypted DEKs and KEKs and [**selection**: *long-term trusted channel key material*, *all software-based key storage*, *no other keys*] by [**selection**:

- *[**selection**: GCM, CCM, Key Wrap, Key Wrap with Padding] cipher mode for encryption according to FCS_STG_EXT.2*,
- *a hash (FCS_COP.1/HASH) of the stored key that is encrypted by a key protected by FCS_STG_EXT.2*,
- *a keyed hash (FCS_COP.1/KEYHMAC) using a key protected by a key protected by FCS_STG_EXT.2*,
- *a digital signature of the stored key using an asymmetric key protected according to FCS_STG_EXT.2*,
- *an immediate application of the key for decrypting the protected data followed by a successful verification of the decrypted data with previously known information*

].

FCS_STG_EXT.3.2 The TSF shall verify the integrity of the [**selection**: *hash*, *digital signature*, *MAC*] of the stored key prior to use of the key.

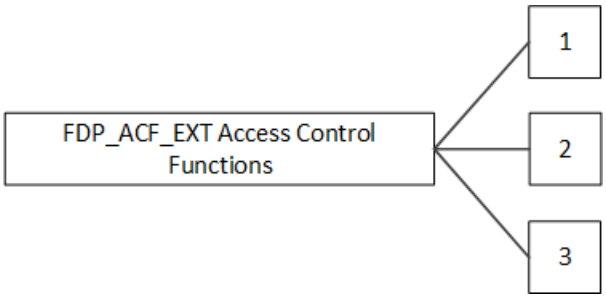
Class FDP: User Data Protection

FDP_ACF_EXT Access Control Functions

Family Behavior

This family defines the rules for access control functions that are not addressed by the FDP_ACF family in CC Part 2.

Component Leveling



FDP_ACF_EXT.1 Access Control for System Services, requires the TSF to be able to control access to its own services.

FDP_ACF_EXT.2 Access Control for System Resources, requires the TSF to be able to provide separate copies of system resources for different application groups.

FDP_ACF_EXT.3 Security Attribute Based Access Control, requires the TSF to enforce policies on applications that prohibit write and execute permissions from being granted simultaneously.

Management: FDP_ACF_EXT.1

The following actions could be considered for the management functions in FMT:

a) Placing applications into application groups based on enterprise configuration settings.
b) Enabling/disabling location services.
c) Enabling/disabling data signaling over externally-accessible hardware ports.

Audit: FDP_ACF_EXT.1

There are no auditable events foreseen.

Management: FDP_ACF_EXT.2

The following actions could be considered for the management functions in FMT:

a) Approve exceptions for sharing data between applications or groups of applications.

Audit: FDP_ACF_EXT.2

There are no auditable events foreseen.

Management: FDP_ACF_EXT.3

There are no management functions foreseen.

Audit: FDP_ACF_EXT.3

There are no auditable events foreseen.

FDP_ACF_EXT.1 Access Control for System Services

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security Roles

FDP_ACF_EXT.1.1 The TSF shall provide a mechanism to restrict the system services that are accessible to an application.

FDP_ACF_EXT.1.2 The TSF shall provide an access control policy that prevents [**selection**: *application*, *groups of applications*] from accessing [**selection**: *all*, *private*] data stored by other [**selection**: *application*, *groups of applications*]. Exceptions may only be explicitly authorized for such sharing by [**selection**: *the user*, *the administrator*, *a common application developer*, *no one*].

FDP_ACF_EXT.2 Access Control for System Resources

Hierarchical to: No other components.

Dependencies: FDP_ACF_EXT.1 Access Control for System Services

FMT_SMR.1 Security Roles

FDP_ACF_EXT.2.1 The TSF shall provide a separate [**assignment:** *system resources*] for each application group and only allow applications within that process group to access the resource. Exceptions may only be explicitly authorized for such sharing by [**selection**: *the user*, *the administrator*, *no one*].

FDP_ACF_EXT.3 Security Attribute Based Access Control

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_ACF_EXT.3.1 The TSF shall enforce an access control policy that prohibits an application from granting both write and execute permission to a file on the device except for [**selection**: *files stored in the application's private data folder*, *no exceptions*].

FDP_BCK_EXT Application Backup

Family Behavior

This family defines requirements for managing device backups.

Component Leveling

FDP_BCK_EXT.1 Application Backup, requires the TSF to be able to determine which data to include in backup operations.

Management: FDP_BCK_EXT.1

The following actions could be considered for the management functions in FMT:

a) Enable/disable backup of certain applications to a local or remote system.

Audit: FDP_BCK_EXT.1

There are no auditable events foreseen.

FDP_BCK_EXT.1 Application Backup

Hierarchical to: No other components.

Dependencies: No dependencies.

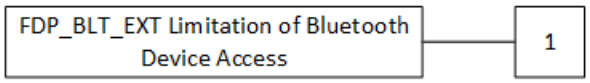
FDP_BCK_EXT.1.1 The TSF shall provide a mechanism for applications to mark [**selection**: *all application data*, *selected application data*] to be excluded from device backups.

FDP_BLT_EXT Limitation of Bluetooth Device Access

Family Behavior

This family defines requirements for managing Bluetooth devices.

Component Leveling



FDP_BLT_EXT.1 Limitation of Bluetooth Device Access, requires the TSF to manage which applications communicate with Bluetooth devices.

Management: FDP_BLT_EXT.1

There are no management functions foreseen.

Audit: FDP_BLT_EXT.1

There are no auditable events foreseen.

FDP_BLT_EXT Limitation of Bluetooth Device Access

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_BLT_EXT.1.1 The TSF shall limit the applications that may communicate with a particular paired Bluetooth device.

FDP_DAR_EXT Data-at-Rest Encryption

Family Behavior

This family defines requirements for implementation of data-at-rest protection.

Component Leveling

FDP_DAR_EXT.1 Protected Data Encryption, requires the TSF to be able to protect all data with a chosen method of encryption.

FDP_DAR_EXT.2 Sensitive Data Encryption, requires the TSF to be able to label, encrypt, store, and decrypt sensitive data and keys.

Management: FDP_DAR_EXT.1

The following actions could be considered for the management functions in FMT:

a) Enabling data-at-rest protection.
b) Enabling removable media's data-at-rest protection.

Audit: FDP_DAR_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Failure to encrypt/decrypt data.

Management: FDP_DAR_EXT.2

There are no management functions foreseen.

Audit: FDP_DAR_EXT.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Failure to encrypt/decrypt data.

FDP_DAR_EXT.1 Protected Data Encryption

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic Operation

FDP_DAR_EXT.1.1 Encryption shall cover all protected data.

FDP_DAR_EXT.1.2 Encryption shall be performed using DEKs with AES in the [**selection**: *XTS*, *CBC*, *GCM*] mode with key size [**selection**: *128*, *256*] bits.

FDP_DAR_EXT.2 Sensitive Data Encryption

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic Operation

FCS_CKM.2 Cryptographic Key Establishment

FCS_STG_EXT.2 Encrypted Cryptographic Key Storage

FDP_DAR_EXT.2.1 The TSF shall provide a mechanism for applications to mark data and keys as sensitive.

FDP_DAR_EXT.2.2 The TSF shall use an asymmetric key scheme to encrypt and store sensitive data received while the product is locked.

FDP_DAR_EXT.2.3 The TSF shall encrypt any stored symmetric key and any stored private key of the asymmetric key(s) used for the protection of sensitive data according to FCS_STG_EXT.2.

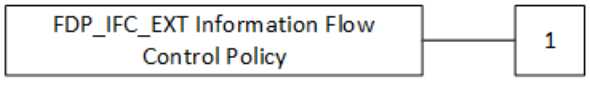
FDP_DAR_EXT.2.4 The TSF shall decrypt the sensitive data that was received while in the locked state upon transitioning to the unlocked state using the asymmetric key scheme and shall re-encrypt that sensitive data using the symmetric key scheme.

FDP_IFC_EXT Information Flow Control Policy

Family Behavior

This family defines requirements for handling of information flows that are not addressed by FDP_IFC in CC Part 2.

Component Leveling



FDP_IFC_EXT.1 Subset Information Flow Control, requires the TSF to be able to support the use of an IPsec VPN to protect data in transit.

Management: FDP_IFC_EXT.1

The following actions could be considered for the management functions in FMT:

a) Enabling/disabling VPN protection.
b) Enabling/disabling Always On VPN protection.

Audit: FDP_IFC_EXT.1

There are no auditable events foreseen.

FDP_IFC_EXT.1 Subset Information Flow Control

Hierarchical to: No other components.

Dependencies: FTP_ITC_EXT.1 Trusted Channel Communication

FDP_IFC_EXT.1.1 The TSF shall [**selection**:

- *provide an interface which allows a VPN client to protect all IP traffic using IPsec*,
- *provide a VPN client which can protect all IP traffic using IPsec*

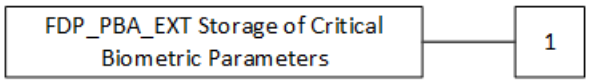
] with the exception of IP traffic required to establish the VPN connection.

FDP_PBA_EXT Storage of Critical Biometric Parameters

Family Behavior

This family defines requirements for protecting authentication templates.

Component Leveling



FDP_PBA_EXT.1 Storage of Critical Biometric Parameters, requires the TSF to protect authentication templates with a chosen method.

Management: FDP_PBA_EXT.1

There are no management functions foreseen.

Audit: FDP_PBA_EXT.1

There are no auditable events foreseen.

FDP_PBA_EXT.1 Storage of Critical Biometric Parameters

Hierarchical to: No other components.

Dependencies: FIA_UAU.5 Multiple Authentication Mechanisms

FDP_PBA_EXT.1.1 The TSF shall protect the authentication template [**selection**: *using a PIN as an*

*additional factor, using a password as an additional factor, [**assignment**: other circumstances]*].

FDP_STG_EXT User Data Storage

Family Behavior

This family defines requirements for managing data storage.

Component Leveling

FDP_STG_EXT.1 User Data Storage, requires the TSF to protect the Trust Anchor Database.

Management: FDP_STG_EXT.1

The following actions could be considered for the management functions in FMT:

a) Importing X.509v3 certificates into the Trust Anchor Database.
b) Removing imported X.509v3 certificates from the Trust Anchor Database.
c) Approving import and removal by applications of X.509v3 certificates in the Trust Anchor Database.

Audit: FDP_STG_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Addition or removal of certificate from Trust Anchor Database.

FDP_STG_EXT.1 User Data Storage

Hierarchical to: No other components.

Dependencies: No dependencies.

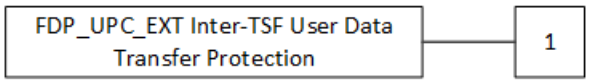
FDP_STG_EXT.1.1 The TSF shall provide protected storage for the Trust Anchor Database.

FDP_UPC_EXT Inter-TSF User Data Transfer Protection

Family Behavior

This family defines requirements for managing trusted channel protocols.

Component Leveling



FDP_UPC_EXT.1 Inter-TSF User Data Transfer Protection, requires the TSF to be able to protect communication channels between products using a chosen secure method.

Management: FDP_UPC_EXT.1

Audit: FDP_UPC_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Application initiation of trusted channel.

FDP_UPC_EXT.1 Inter-TSF User Data Transfer Protection

Hierarchical to: No other components.

Dependencies: FTP_ITC_EXT.1 Trusted Channel Communication

FDP_UPC_EXT.1.1 The TSF shall provide a means for non-TSF applications executing on the TOE to use [***assignment****: data transfer 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 its end points, protects channel data from disclosure, and detects modification of the channel data.

FDP_UPC_EXT.1.2 The TSF shall permit the non-TSF applications to initiate communication via the trusted channel.

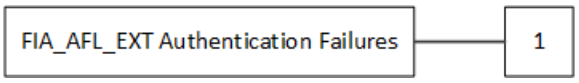
Class FIA: Identification and Authentication

FIA_AFL_EXT Authentication Failures

Family Behavior

This family defines requirements for authentication failure handling that are not addressed by the FIA_AFL family in CC Part 2.

Component Leveling



FIA_AFL_EXT.1 Authentication Failure Handling, requires the TSF be able to manage unsuccessful authentication attempts and limit the number of attempts for each method.

Management: FIA_AFL_EXT.1

The following actions could be considered for the management functions in FMT:

a) Configuration of authentication failure limit.

Audit: FIA_AFL_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Excess of authentication failure limit.

FIA_AFL_EXT.1 Authentication Failure Handling

Hierarchical to: No other components.

Dependencies: FCS_CKM_EXT.5 TSF Wipe

FIA_UAU.1 Timing of Authentication

FIA_AFL_EXT.1.1 The TSF shall consider password and [**assignment**: *other authentication mechanisms*] as critical authentication mechanisms.

FIA_AFL_EXT.1.2 The TSF shall detect when a configurable positive integer within [**assignment**: *range of acceptable values for each authentication mechanism*] of [**selection**: *unique*, *non-unique*] unsuccessful authentication attempts occur related to last successful authentication for each authentication mechanism.

FIA_AFL_EXT.1.3 The TSF shall maintain the number of unsuccessful authentication attempts that have occurred upon power off.

FIA_AFL_EXT.1.4 When the defined number of unsuccessful authentication attempts has exceeded the maximum allowed for a given authentication mechanism, all future authentication attempts will be limited to other available authentication mechanisms, unless the given mechanism is designated as a critical authentication mechanism.

FIA_AFL_EXT.1.5 When the defined number of unsuccessful authentication attempts for the last available authentication mechanism or single critical authentication mechanism has been surpassed, the TSF shall perform a wipe of all protected data.

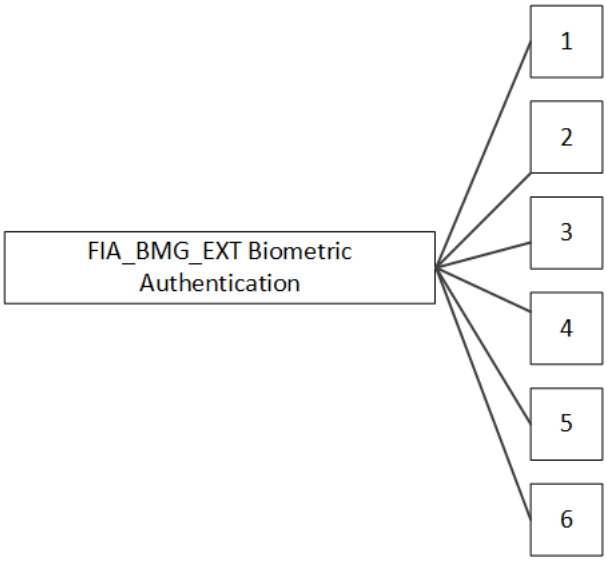
FIA_AFL_EXT.1.6 The TSF shall increment the number of unsuccessful authentication attempts prior to notifying the user that the authentication was unsuccessful.

FIA_BMG_EXT Biometric Authentication

Family Behavior

This family defines requirements for biometric authentication and the handling of data used to support this function.

Component Leveling



FIA_BMG_EXT.1 Accuracy of Biometric Authentication, requires the TSF to reject false positive and false negative biometric authentication attempts to a specified degree of precision.

FIA_BMG_EXT.2 Biometric Enrollment, requires the TSF to enforce quality metrics on enrolled biometric data.

FIA_BMG_EXT.3 Biometric Verification, requires the TSF to enforce quality metrics on biometric data used for authentication.

FIA_BMG_EXT.4 Biometric Templates, requires the TSF to enforce quality metrics on biometric templates.

FIA_BMG_EXT.5 Handling Unusual Biometric Templates, requires the TSF to handle biometric templates properly when they contain unusual data properties.

FIA_BMG_EXT.6 Spoof Detections for Biometrics, requires the TSF to apply spoof detection on biometric authentication attempts.

Management: FIA_BMG_EXT.1

There are no management functions foreseen.

Audit: FIA_BMG_EXT.1

There are no auditable events foreseen.

Management: FIA_BMG_EXT.2

There are no management functions foreseen.

Audit: FIA_BMG_EXT.2

There are no auditable events foreseen.

Management: FIA_BMG_EXT.3

There are no management functions foreseen.

Audit: FIA_BMG_EXT.3

There are no auditable events foreseen.

Management: FIA_BMG_EXT.4

The following actions could be considered for the management functions in FMT:

a) Revoking biometric template.

Audit: FIA_BMG_EXT.4

There are no auditable events foreseen.

Management: FIA_BMG_EXT.5

The following actions could be considered for the management functions in FMT:

b) Revoking biometric template.

Audit: FIA_BMG_EXT.5

There are no auditable events foreseen.

Management: FIA_BMG_EXT.6

There are no management functions foreseen.

Audit: FIA_BMG_EXT.6

There are no auditable events foreseen.

FIA_BMG_EXT.1 Accuracy of Biometric Authentication

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of Authentication

FIA_BMG_EXT.1.1 The one-attempt BAF False Accept Rate (FAR) for [**assignment**: *biometric modality selected in FIA_UAU.5.1*] shall not exceed [**assignment**: *claimed FAR no greater than 1:100*] with a one-attempt BAF False Reject Rate (FRR) not to exceed 1 in [**assignment**: *claimed FRR no greater than 1:10*].

FIA_BMG_EXT.1.2 The overall System Authentication False Accept Rate (SAFAR) shall be no greater than 1 in [**assignment**: *a SAFAR no greater than 1:500*] within a 1% margin.

FIA_BMG_EXT.2 Biometric Enrollment

Hierarchical to: No other components.

Dependencies: FIA_BMG_EXT.4 Biometric Templates

FIA_BMG_EXT.2.1 The TSF shall only use biometric samples of sufficient quality for enrollment. Sample data shall have [**assignment**: *quality metrics corresponding to each biometric modality*].

FIA_BMG_EXT.3 Biometric Verification

Hierarchical to: No other components.

Dependencies: FIA_BMG_EXT.4 Biometric Templates

FIA_BMG_EXT.3.1 The TSF shall only use biometric samples of sufficient quality for verification. As such, sample data shall have [**assignment**: *quality metrics corresponding to each biometric modality*].

FIA_BMG_EXT.4 Biometric Templates

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_BMG_EXT.4.1 The TSF shall only generate and use enrollment templates and/or authentication templates of sufficient quality for any subsequent authentication functions.

FIA_BMG_EXT.5 Handling Unusual Biometric Templates

Hierarchical to: No other components.

Dependencies: FIA_BMG_EXT.4 Biometric Templates

FIA_BMG_EXT.5.1 The matching algorithm shall handle properly formatted enrollment templates and/or authentication templates, especially those with unusual data properties, appropriately. If such templates contain incorrect syntax, are of low quality, or contain enrollment data considered unrealistic for a given modality, then they shall be rejected by the matching algorithm and an error code shall be reported.

FIA_BMG_EXT.6 Spoof Detections for Biometrics

Hierarchical to: No other components.

Dependencies: FIA_BMG_EXT.1 Accuracy of Biometric Authentication

FIA_UAU.5 Multiple Authentication Mechanisms

FIA_BMG_EXT.6.1 The TSF shall perform Presentation Attack Detection testing up to the attack potential of [**selection**: *basic*, *intermediate*, *advanced*] attacks, for each biometric modalities selected in FIA_UAU.5.1 on each enrollment and authentication attempt, rejecting detected spoofs. When an authentication attempt fails due to PAD testing, the TSF shall not indicate to the user the reason for failure to authenticate.

FIA_PMG_EXT Password Management

Family Behavior

This family defines requirements for managing password criteria.

Component Leveling

FIA_PMG_EXT.1 Password Management, requires the TSF to control the criteria for passwords.

Management: FIA_PMG_EXT.1

The following actions could be considered for the management functions in FMT:

a) Configuring password policy.

Audit: FIA_PMG_EXT.1

There are no auditable events foreseen.

FIA_PMG_EXT.1 Password Management

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of Authentication

FIA_PMG_EXT.1.1 The TSF shall support the following for the Password Authentication Factor:

1. Passwords shall be able to be composed of any combination of [**selection**: *upper and lower case letters*, *[**assignment**: a character set of*

at least 52 characters]], numbers, and special characters: [**selection**: *"!", "@", "#", "$", "%", "^", "&", "*", "(", ")", [**assignment**: other characters]*];

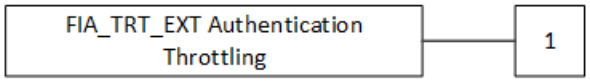
2. Password length up to [**assignment**: *an integer greater than or equal to 14*] characters shall be supported.

FIA_TRT_EXT Authentication Throttling

Family Behavior

This family defines requirements for prevention of brute-force authentication attempts.

Component Leveling



FIA_TRT_EXT.1 Authentication Throttling, requires the TSF to limit authentication attempts by number of attempts in a set amount of time.

Management: FIA_TRT_EXT.1

There are no management functions foreseen.

Audit: FIA_TRT_EXT.1

There are no auditable events foreseen.

FIA_TRT_EXT.1 Authentication Throttling

Hierarchical to: No other components.

Dependencies: FIA_UAU.5 Multiple Authentication Mechanisms

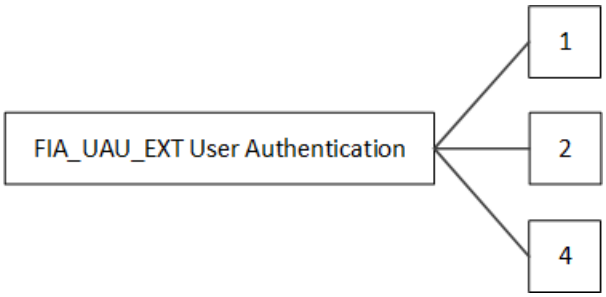
FIA_TRT_EXT.1.1 The TSF shall limit automated user authentication attempts by [**selection**: *preventing authentication via an external port*, *enforcing a delay between incorrect authentication attempts*] for all authentication mechanisms selected in FIA_UAU.5.1. The minimum delay shall be such that no more than 10 attempts can be attempted per 500 milliseconds.

FIA_UAU_EXT User Authentication

Family Behavior

This family defines requirements for user authentication that are not addressed by FIA_UAU in CC Part 2.

Component Leveling



FIA_UAU_EXT.1 Authentication for Cryptographic Operation, requires the TSF enforce data-at-rest protection until successful authentication has occurred.

FIA_UAU_EXT.2 Timing of Authentication, requires the TSF to prevent a subject's use of TOE until the user is authenticated.

FIA_UAU_EXT.4 Secondary User Authentication, requires the TSF to enforce the use of a secondary authentication factor to access certain user data.

Management: FIA_UAU_EXT.1

There are no management functions foreseen.

Audit: FIA_UAU_EXT.1

There are no auditable events foreseen.

Management: FIA_UAU_EXT.2

The following actions could be considered for the management functions in FMT:

a) Enabling/disabling display TSF notifications while in the locked state.
b) Enabling/disabling bypass of local user authentication.

Audit: FIA_UAU_EXT.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Action performed before authentication.

Management: FIA_UAU_EXT.4

There are no management functions foreseen.

Audit: FIA_UAU_EXT.4

There are no auditable events foreseen.

FIA_UAU_EXT.1 Authentication for Cryptographic Operation

Hierarchical to: No other components.

Dependencies: FDP_DAR_EXT.1 Protected Data Encryption

FDP_DAR_EXT.2 Sensitive Data Encryption

FIA_UAU_EXT.1.1 The TSF shall require the user to present the Password Authentication Factor prior to decryption of protected data and encrypted DEKs, KEKs and [**selection:** *long-term trusted channel key material, all software-based key storage, no other keys*] at startup.

FIA_UAU_EXT.2 Timing of Authentication

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU_EXT.2.1 The TSF shall allow [**selection**: *[**assignment**: list of actions]*, *no actions*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU_EXT.2.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU_EXT.4 Secondary User Authentication

Hierarchical to: No other components.

Dependencies: FDP_ACF_EXT.2 Access Control for System Resources

FIA_UAU.5 Multiple Authentication Mechanisms

FIA_UAU_EXT.4.1 The TSF shall provide a secondary authentication mechanism for accessing Enterprise applications and resources. The secondary authentication mechanism shall control access to the Enterprise application and shared resources and shall be incorporated into the encryption of protected and sensitive data belonging to Enterprise applications and shared resources.

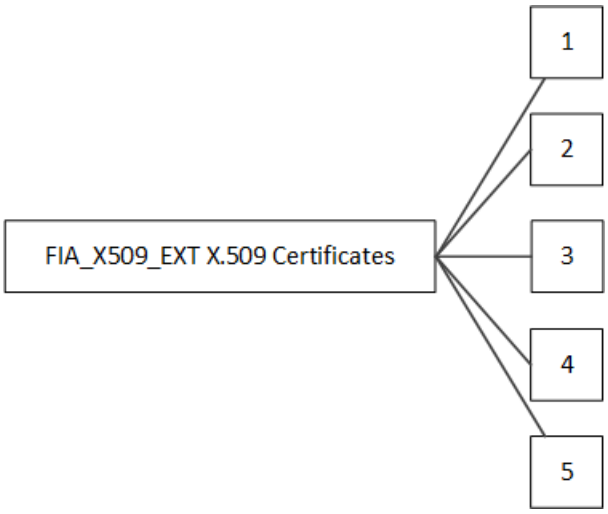
FIA_UAU_EXT.4.2 The TSF shall require the user to present the secondary authentication factor prior to decryption of Enterprise application data and Enterprise shared resource data.

FIA_X509_EXT X.509 Certificates

Family Behavior

This family defines requirements for the management and use of X.509 certificates.

Component Leveling



FIA_X509_EXT.1 X.509 Validation of Certificates, specifies the rules the TSF must follow to determine if a particular X.509 certificate is valid.

FIA_X509_EXT.2 X.509 Certificate Authentication, defines the TSF's usage of X.509 certificates and how it reacts to certificates with undetermined revocation status.

FIA_X509_EXT.3 Request Validation of Certificates, requires the TSF to make a certificate validation service available to environmental components.

FIA_X509_EXT.4 X.509 Certificate Enrollment, requires the TSF to implement Enrollment over Secure Transport (EST) as a mechanism to obtain X.509 certificates.

FIA_X509_EXT.5 X.509 Certificate Requests, requires the TSF to generate X.509 certificate requests and validate the responses.

Management: FIA_X509_EXT.1

There are no management activities foreseen.

Audit: FIA_X509_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Failure to validate X.509v3 certificate.

Management: FIA_X509_EXT.2

The following actions could be considered for the management functions in FMT:

a) Configuring whether to allow/disallow establishment of a trusted channel if the TSF cannot establish a connection to determine the validity of a certificate.

Audit: FIA_X509_EXT.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Failure to establish connection to determine revocation status.

Management: FIA_X509_EXT.3

There are no management activities foreseen.

Audit: FIA_X509_EXT.3

There are no auditable events foreseen.

Management: FIA_X509_EXT.4

There are no management activities foreseen.

Audit: FIA_X509_EXT.4

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Generation of Certificate Enrollment Request.
b) Success or failure of enrollment.
c) Update of EST Trust Anchor Database

Management: FIA_X509_EXT.5

There are no management activities foreseen.

Audit: FIA_X509_EXT.5

There are no auditable events foreseen.

FIA_X509_EXT.1 X.509 Validation of Certificates

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic Operation

FIA_X509_EXT.1.1 The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a certificate in the Trust Anchor Database.
- The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension, that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met.
- The TSF shall validate that any CA certificate includes caSigning purpose in the key usage field
- The TSF shall validate the revocation status of the certificate using [**selection**: *OCSP as specified in RFC 6960*, *CRL as specified in RFC 5759*, *an OCSP TLS Status Request Extension (OCSP stapling) as specified in RFC 6066*, *OCSP TLS Multi-Certificate Status Request Extension (i.e., OCSP Multi-Stapling) as specified in RFC 6961*].
- The TSF shall validate the extendedKeyUsage field according to the following rules:

- Certificates used for trusted updates and executable code integrity verification shall have the Code Signing Purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
- Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
- Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the EKU field. [conditional]
- Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the EKU field.
- OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the EKU field. [conditional]

FIA_X509_EXT.1.2 The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509_EXT.2 X.509 Certificate Authentication

Hierarchical to: No other components.

Dependencies: FIA_X509_EXT.1 X.509 Validation of Certificates

FTP_ITC_EXT.1 Trusted Channel Communication

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication [**assignment:** *trusted channel protocols*] and [**selection**: *code signing for system software updates*, *code signing for mobile applications*, *code signing for integrity verification*, *[**assignment**: other uses]*, *no additional uses*].

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the revocation status of a certificate, the TSF shall [**selection**: *allow the administrator to choose whether to accept the certificate in these cases*, *allow the user to choose whether to accept the certificate in these cases*, *accept the certificate*, *not accept the certificate*].

FIA_X509_EXT.3 Request Validation of Certificates

Hierarchical to: No other components.

Dependencies: FIA_X509_EXT.1 X.509 Validation of Certificates

FIA_X509_EXT.3.1 The TSF shall provide a certificate validation service to applications.

FIA_X509_EXT.3.2 The TSF shall respond to the requesting application with the success or failure of the validation.

FIA_X509_EXT.4 X.509 Certificate Enrollment

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic Key Generation

FIA_X509_EXT.1 X.509 Validation of Certificates

FIA_X509_EXT.4.1 The TSF shall use 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 Section 4.2.

FIA_X509_EXT.4.2 The TSF shall be capable of authenticating EST requests using an existing certificate and corresponding private key as specified by RFC 7030 Section 3.3.2.

FIA_X509_EXT.4.3 The TSF shall be capable of authenticating EST requests using HTTP Basic Authentication with a username and password as specified by RFC 7030 Section 3.2.3.

FIA_X509_EXT.4.4 The TSF shall perform authentication of the EST server using an Explicit Trust Anchor following the rules described in RFC 7030, section 3.6.1.

FIA_X509_EXT.4.5 The TSF shall be capable of requesting server-provided private keys as specified in RFC 7030 Section 4.4.

FIA_X509_EXT.4.6 The TSF shall be capable of updating its EST-specific Trust Anchor Database using the "Root CA Key Update" process described in RFC 7030 Section 4.1.3.

FIA_X509_EXT.4.7 The TSF shall generate 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*].

FIA_X509_EXT.4.8 The TSF shall validate the chain of certificates from the Root CA certificate in the Trust Anchor Database to the EST Server CA certificate upon receiving a CA Certificates Response.

FIA_X509_EXT.5 X.509 Certificate Requests

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic Key Generation

FIA_X509_EXT.1 X.509 Validation of Certificates

FIA_X509_EXT.5.1 The TSF shall generate 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*].

FIA_X509_EXT.5.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

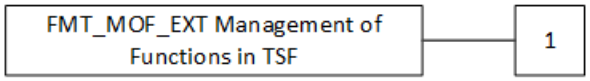
Class FMT: Security Management

FMT_MOF_EXT Management of Functions in TSF

Family Behavior

This family defines requirements for authorization to manage the behavior of the TSF that are not addressed by FMT_MOF in CC Part 2.

Component Leveling



FMT_MOF_EXT.1 Management of Security Functions Behavior, requires the TSF to apply restrictions to access its management functions to the authorized roles.

Management: FMT_MOF_EXT.1

The following actions could be considered for the management functions in FMT:

a) Managing the group of roles that can interact with the functions in the TSF.

Audit: FMT_MOF_EXT.1

There are no auditable events foreseen.

FMT_MOF_EXT.1 Management of Security Functions Behavior

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_MOF_EXT.1.1 The TSF shall restrict the ability to perform the functions [**assignment:** *list of management functions*] to the user.

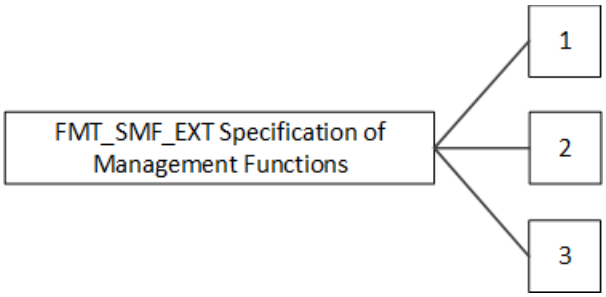
FMT_MOF_EXT.1.2 The TSF shall restrict the ability to perform the functions [**assignment:** *list of management functions*] to the administrator when the device is enrolled and according to the administrator-configured policy.

FMT_SMF_EXT Specification of Management Functions

Family Behavior

This family defines requirements for security-relevant management functions that are not addressed by FMT_SMF in CC Part 2.

Component Leveling



FMT_SMF_EXT.1 Specification of Management Functions, requires the TSF to define the management functions that it implements.

FMT_SMF_EXT.2 Specification of Remediation Actions, requires the TSF to automatically perform specific management functions in response to a specific event.

FMT_SMF_EXT.3 Current Administrator, requires the TSF to provide users with a list of administrators and their specified functions.

Management: FMT_SMF_EXT.1

There are no management activities foreseen.

Audit: FMT_SMF_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Initiation of policy update.
b) Change of setting.
c) Initiation of software update.
d) Initiation of application installation or update.

Management: FMT_SMF_EXT.2

The following actions could be considered for the management functions in FMT:

a) Configuration of the functions that are performed in response to unenrollment event.

Audit: FMT_SMF_EXT.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Initiation of unenrollment.
b) Completion of unenrollment.

Management: FMT_SMF_EXT.3

There are no management functions foreseen.

Audit: FMT_SMF_EXT.3

There are no auditable events foreseen.

FMT_SMF_EXT.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF_EXT.1.1 The TSF shall be capable of performing [**assignment:** *list of management functions*].

FMT_SMF_EXT.2 Specification of Remediation Actions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF_EXT.2.1 The TSF shall offer [**assignment:** *remediation functions*] upon un-enrollment and [**selection**: *[**assignment**: other administrator-configured triggers]*, *no other triggers*].

FMT_SMF_EXT.3 Current Administrator

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security Roles

FMT_SMF_EXT.3.1 The TSF shall provide a mechanism that allows users to view a list of currently authorized administrators and the management functions that each administrator is authorized to perform.

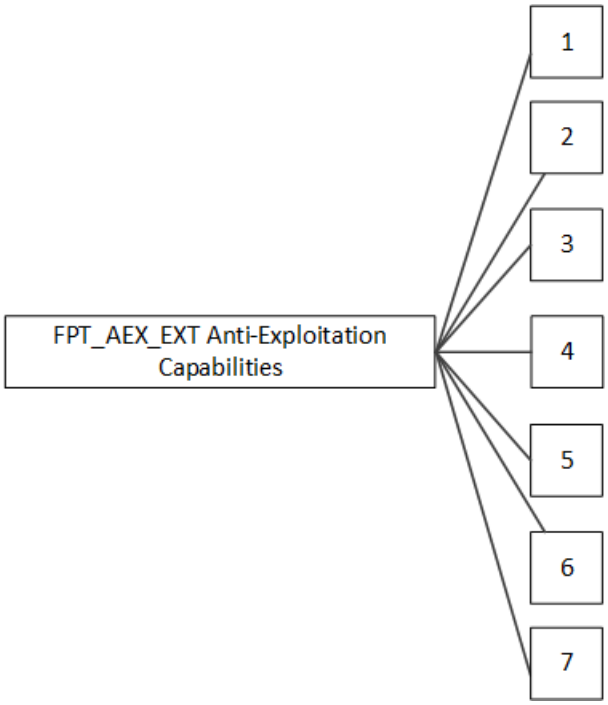
Class FPT: Protection of the TSF

FPT_AEX_EXT Anti-Exploitation Capabilities

Family Behavior

This family defines requirements for protecting against common types of software exploitation techniques.

Component Leveling



FPT_AEX_EXT.1 Application Address Space Layout Randomization, requires the TSF to support address space layout randomization (ASLR)

FPT_AEX_EXT.2 Memory Page Permissions, requires the TSF to enforce access permissions on physical memory.

FPT_AEX_EXT.3 Stack Overflow Protection, requires the TSF to implement stack overflow protection.

FPT_AEX_EXT.4 Domain Isolation, requires the TSF to protect itself from untrusted subjects and enforce address space isolation.

FPT_AEX_EXT.5 Kernel Address Space Layout Randomization, requires the TSF to provide ASLR to the kernel.

FPT_AEX_EXT.6 Write or Execute Memory Page Permissions, requires the TSF to prevent physical memory from being both writable and executable.

FPT_AEX_EXT.7 Heap Overflow Protection, requires the TSF to support heap-based buffer overflow protection.

Management: FPT_AEX_EXT.1

There are no management functions foreseen.

Audit: FPT_AEX_EXT.1

There are no auditable events foreseen.

Management: FPT_AEX_EXT.2

There are no management functions foreseen.

Audit: FPT_AEX_EXT.2

There are no auditable events foreseen.

Management: FPT_AEX_EXT.3

There are no management functions foreseen.

Audit: FPT_AEX_EXT.3

There are no auditable events foreseen.

Management: FPT_AEX_EXT.4

There are no management functions foreseen.

Audit: FPT_AEX_EXT.4

There are no auditable events foreseen.

Management: FPT_AEX_EXT.5

There are no management functions foreseen.

Audit: FPT_AEX_EXT.5

There are no auditable events foreseen.

Management: FPT_AEX_EXT.6

There are no management functions foreseen.

Audit: FPT_AEX_EXT.6

There are no auditable events foreseen.

Management: FPT_AEX_EXT.7

There are no management functions foreseen.

Audit: FPT_AEX_EXT.7

There are no auditable events foreseen.

FPT_AEX_EXT.1 Application Address Space Layout Randomization

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.1 Random Bit Generation

FPT_AEX_EXT.1.1 The TSF shall provide address space layout randomization ASLR to applications.

FPT_AEX_EXT.1.2 The base address of any user-space memory mapping will consist of at least 8 unpredictable bits.

FPT_AEX_EXT.2 Memory Page Permissions

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_AEX_EXT.2.1 The TSF shall be able to enforce read, write, and execute permissions on every page of physical memory.

FPT_AEX_EXT.3 Stack Overflow Protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_AEX_EXT.3.1 TSF processes that execute in a non-privileged execution domain on the application processor shall implement stack-based buffer overflow protection.

FPT_AEX_EXT.4 Domain Isolation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_AEX_EXT.4.1 The TSF shall protect itself from modification by untrusted subjects.

FPT_AEX_EXT.4.2 The TSF shall enforce isolation of address space between applications.

FPT_AEX_EXT.5 Kernel Address Space Layout Randomization

Hierarchical to: No other components.

Dependencies: FCS_RBG_EXT.1 Random Bit Generation

FPT_AEX_EXT.5.1 The TSF shall provide address space layout randomization (ASLR) to the kernel.

FPT_AEX_EXT.5.2 The base address of any kernel-space memory mapping will consist of [**assignment**: *number greater than or equal to 4*] unpredictable bits.

FPT_AEX_EXT.6 Write or Execute Memory Page Permissions

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_AEX_EXT.6.1 The TSF shall prevent write and execute permissions from being simultaneously granted to any page of physical memory [**selection**: *with no exceptions*, *[**assignment**: specific exceptions]*].

FPT_AEX_EXT.7 Heap Overflow Protection

Hierarchical to: No other components.

Dependencies: No dependencies.

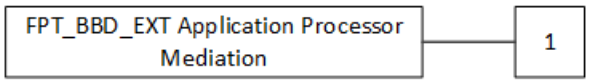
FPT_AEX_EXT.7.1 The TSF shall include heap-based buffer overflow protections in the runtime environment it provides to processes that execute on the application processor.

FPT_BBD_EXT Application Processor Mediation

Family Behavior

This family defines requirements for separation of baseband and application processor execution.

Component Leveling



FPT_BBD_EXT.1 Application Processor Mediation, requires the TSF to enforce separation between baseband and application processor execution except through application processor mechanisms.

Management: FPT_BBD_EXT.1

There are no management functions foreseen.

Audit: FPT_BBD_EXT.1

There are no auditable events foreseen.

FPT_BBD_EXT.1 Application Processor Mediation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_BBD_EXT.1.1 The TSF shall prevent code executing on any baseband processor (BP) from accessing application processor (AP) resources except when mediated by the AP.

FPT_BLT_EXT Limitation of Bluetooth Profile Support

Family Behavior

This family defines requirements for limiting Bluetooth capabilities without user action.

Component Leveling

FPT_BLT_EXT.1 Limitation of Bluetooth Profile Support, requires the TSF to maintain a disabled by default posture for Bluetooth profiles.

Management: FPT_BLT_EXT.1

There are no management functions foreseen.

Audit: FPT_BLT_EXT.1

There are no auditable events foreseen.

FPT_BLT_EXT.1 Limitation of Bluetooth Profile Support

Hierarchical to: No other components.

Dependencies: No dependencies.

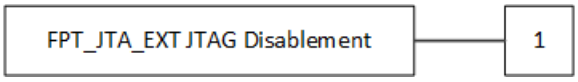
FPT_BLT_EXT.1.1 The TSF shall disable support for [**assignment**: *list of Bluetooth profiles*] Bluetooth profiles when they are not currently being used by an application on the Mobile Device, and shall require explicit user action to enable them.

FPT_JTA_EXT JTAG Disablement

Family Behavior

This family defines requirements for JTAG interface access limitations.

Component Leveling



FPT_JTA_EXT.1 JTAG Disablement, requires the TSF to specify the mechanism used to restrict access to its JTAG interface.

Management: FPT_JTA_EXT.1

There are no management functions foreseen.

Audit: FPT_JTA_EXT.1

There are no auditable events foreseen.

FPT_JTA_EXT.1 JTAG Disablement

Hierarchical to: No other components.

Dependencies: No dependencies.

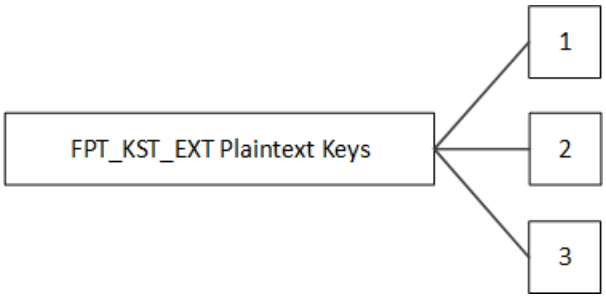
FPT_JTA_EXT.1.1 The TSF shall [**selection**: *disable access through hardware*, *control access by a signing key*] to JTAG.

FPT_KST_EXT Plaintext Keys

Family Behavior

This family defines requirements for protecting plaintext keys.

Component Leveling



FPT_KST_EXT.1 Key Storage, requires the TSF to avoid storage of plaintext keys in readable memory.

FPT_KST_EXT.2 No Key Transmission, requires the TSF to prevent transmitting plaintext key material to the operational environment.

FPT_KST_EXT.3 No Plaintext Key Export, requires the TSF to prevent the export of plaintext keys.

Management: FPT_KST_EXT.1

There are no management functions foreseen.

Audit: FPT_KST_EXT.1

There are no auditable events foreseen.

Management: FPT_KST_EXT.2

There are no management functions foreseen.

Audit: FPT_KST_EXT.2

There are no auditable events foreseen.

Management: FPT_KST_EXT.3

There are no management functions foreseen.

Audit: FPT_KST_EXT.3

There are no auditable events foreseen.

FPT_KST_EXT.1 Key Storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_KST_EXT.1.1 The TSF shall not store any plaintext key material in readable non-volatile memory.

FPT_KST_EXT.2 No Key Transmission

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_KST_EXT.2.1 The TSF shall not transmit any plaintext key material outside the security boundary of the TOE.

FPT_KST_EXT.3 No Plaintext Key Export

Hierarchical to: No other components.

Dependencies: No dependencies.

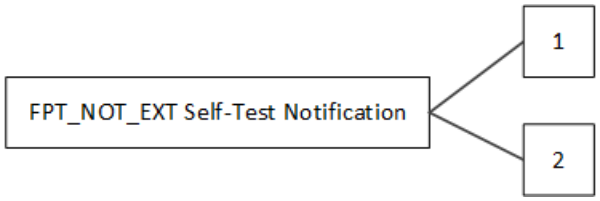
FPT_KST_EXT.3.1 The TSF shall ensure it is not possible for the TOE user(s) to export plaintext keys.

FPT_NOT_EXT Self-Test Notification

Family Behavior

This family defines requirements for generation of notifications in response to completed self-tests.

Component Leveling



FPT_NOT_EXT.1 Self-Test Notification, requires the TSF to become non-operational when certain failures occur.

FPT_NOT_EXT.2 Software Integrity Verification, requires the TSF to generate and sign software integrity verification values.

Management: FPT_NOT_EXT.1

There are no management functions foreseen.

Audit: FPT_NOT_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Measurement of TSF software.

Management: FPT_NOT_EXT.2

The following actions could be considered for the management functions in FMT:

a) Retrieval of TSF software integrity verification values.

Audit: FPT_NOT_EXT.2

There are no auditable events foreseen.

FPT_NOT_EXT.1 Self-Test Notification

Hierarchical to: No other components.

Dependencies: FPT_TST_EXT.1 TSF Cryptographic Functionality Testing

FPT_TST_EXT.2 TSF Integrity Checking

FPT_NOT_EXT.1.1 The TSF shall transition to non-operational mode and [**selection**: *log failures in the audit record*, *notify the administrator*, *[**assignment**: other actions]*, *no other actions*] when the following types of failures occur:

- failures of the self-test(s)
- TSF software integrity verification failures
- [**selection**: *no other failures*, *[**assignment**: other failures]*]

FPT_NOT_EXT.2 Software Integrity Verification

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic Operation

FPT_NOT_EXT.2.1 The TSF shall [**selection**: *audit*, *provide the administrator with*] TSF-software integrity verification values.

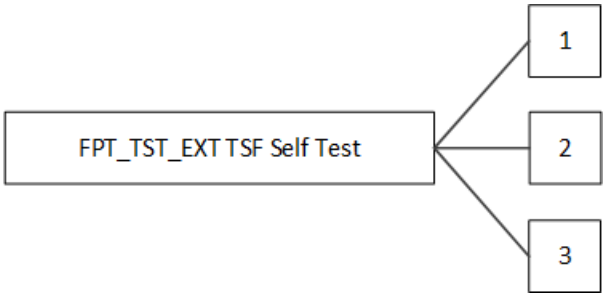
FPT_NOT_EXT.2.2 The TSF shall cryptographically sign all integrity verification values.

FPT_TST_EXT TSF Self Test

Family Behavior

This family defines requirements for execution of self-tests that are not addressed by FPT_TST in CC Part 2.

Component Leveling



FPT_TST_EXT.1 TSF Cryptographic Functionality Testing, requires the TSF to run self-test at start-up to verify correct operation.

FPT_TST_EXT.2 TSF Integrity Checking, requires the TSF to verify integrity or executable code.

FPT_TST_EXT.3 TSF Integrity Testing, requires the TSF to prevent code execution if deemed invalid.

Management: FPT_TST_EXT.1

There are no management functions foreseen.

Audit: FPT_TST_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Initiation of self-test.

b) Failure of self-test.

Management: FPT_TST_EXT.2

There are no management functions foreseen.

Audit: FPT_TST_EXT.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Start-up of TOE.
b) Detected integrity violation.

Management: FPT_TST_EXT.3

Audit: FPT_TST_EXT.3

There are no auditable events foreseen.

FPT_TST_EXT.1 TSF Cryptographic Functionality Testing

Hierarchical to:	No other components.
Dependencies:	FCS_COP.1 Cryptographic Operation
FPT_TST_EXT.1.1	The TSF shall run a suite of self-tests during initial start-up (on power on) to demonstrate the correct operation of all cryptographic functionality.

FPT_TST_EXT.2 TSF Integrity Checking

Hierarchical to:	No other components.
Dependencies:	FCS_COP.1 Cryptographic Operation
FPT_TST_EXT.2.1	The TSF shall verify the integrity of [**assignment**: *TSF data*] stored in mutable media prior to its execution through the use of [**assignment**: *cryptographic or immutable hardware mechanism*].

FPT_TST_EXT.3 TSF Integrity Testing

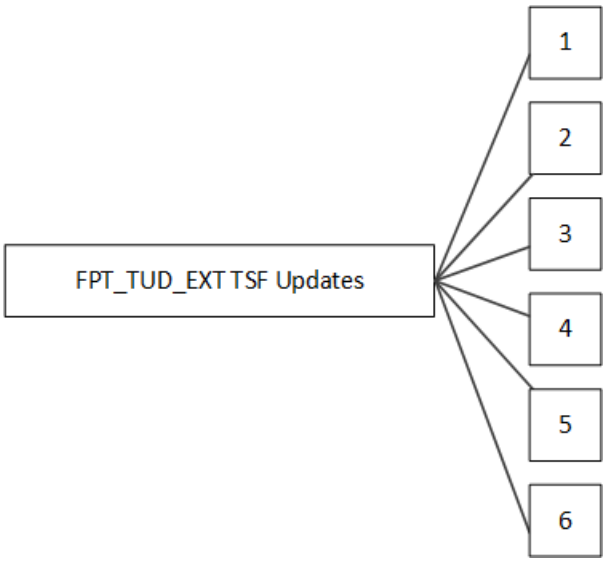
Hierarchical to:	No other components.
Dependencies:	FPT_TST_EXT.2 TSF Integrity Checking
	FIA_X509_EXT.1 X.509 Validation of Certificates
	FIA_X509_EXT.2 X.509 Certificate Authentication
FPT_TST_EXT.3.1	The TSF shall not execute code if the code signing certificate is deemed invalid.

FPT_TUD_EXT TSF Updates

Family Behavior

This family defines requirements for trusted updates.

Component Leveling



FPT_TUD_EXT.1 TSF Version Query, requires the TSF to provide authorized users the ability to query specified versions.

FPT_TUD_EXT.2 TSF Update Verification, requires the TSF to ensure that system software updates are digitally signed prior to installation.

FPT_TUD_EXT.3 Application Signing, requires the TSF to ensure that application software updates are digitally signed prior to installation.

FPT_TUD_EXT.4 Trusted Update Verification, requires the TSF to enforce validity of system software's code signing certificate prior to installation.

FPT_TUD_EXT.5 Application Verification, requires the TSF to enforce validity of application software's code signing certificate prior to installation.

FPT_TUD_EXT.6 Trusted Update Verification, requires the TSF to prevent the intentional rollback of software updates.

Management: FPT_TUD_EXT.1

There are no management functions foreseen.

Audit: FPT_TUD_EXT.1

There are no auditable events foreseen.

Management: FPT_TUD_EXT.2

The following actions could be considered for the management functions in FMT:

a) Updating of system software.

Audit: FPT_TUD_EXT.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Success or failure of signature verification for applications.

Management: FPT_TUD_EXT.3

Audit: FPT_TUD_EXT.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Success or failure of signature verification for applications.

Management: FPT_TUD_EXT.4

There are no management functions foreseen.

Audit: FPT_TUD_EXT.4

There are no auditable events foreseen.

Management: FPT_TUD_EXT.5

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Configure certificate or public key used to validate digital signature on applications.

Audit: FPT_TUD_EXT.5

There are no auditable events foreseen.

Management: FPT_TUD_EXT.6

There are no management functions foreseen.

Audit: FPT_TUD_EXT.6

There are no auditable events foreseen.

FPT_TUD_EXT.1 TSF Version Query

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TUD_EXT.1.1	The TSF shall provide authorized users the ability to query the current version of the TOE firmware/software.
FPT_TUD_EXT.1.2	The TSF shall provide authorized users the ability to query the current version of the hardware model of the device.
FPT_TUD_EXT.1.3	The TSF shall provide authorized users the ability to query the current version of installed mobile applications.

FPT_TUD_EXT.2 TSF Update Verification

Hierarchical to:	No other components.

Dependencies: FCS_COP.1 Cryptographic Operation

FPT_TUD_EXT.2.1 The TSF shall verify software updates to the Application Processor system software and [**selection**: *[**assignment**: other processor system software]*, *no other processor system software*] using a digital signature verified by the manufacturer trusted key prior to installing those updates.

FPT_TUD_EXT.2.2 The TSF shall [**selection**: *never update*, *update only by verified software*] the TSF boot integrity [**selection**: *key*, *hash*].

FPT_TUD_EXT.2.3 The TSF shall verify that the digital signature verification key used for TSF updates [**selection**: *is validated to a public key in the Trust Anchor Database*, *matches an immutable hardware public key*].

FPT_TUD_EXT.3 Application Signing

Hierarchical to: No other components.

Dependencies: FIA_X509_EXT.1 X.509 Validation of Certificates

FIA_X509_EXT.2 X.509 Certificate Authentication

FPT_TUD_EXT.3.1 The TSF shall verify mobile application software using a digital signature mechanism prior to installation.

FPT_TUD_EXT.4 Trusted Update Verification

Hierarchical to: No other components.

Dependencies: FIA_X509_EXT.1 X.509 Validation of Certificates

FIA_X509_EXT.2 X.509 Certificate Authentication

FPT_TUD_EXT.4.1 The TSF shall not install code if the code signing certificate is deemed invalid.

FPT_TUD_EXT.5 Application Verification

Hierarchical to: No other components.

Dependencies: FIA_X509_EXT.1 X.509 Validation of Certificates

FIA_X509_EXT.2 X.509 Certificate Authentication

FPT_TUD_EXT.5.1 The TSF shall by default only install mobile applications cryptographically verified by [**selection**: *a built-in X.509v3 certificate*, *a configured X.509v3 certificate*].

FPT_TUD_EXT.6 Trusted Update Verification

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TUD_EXT.6.1 The TSF shall verify that software updates to the TSF are a current or later version than the current version of the TSF.

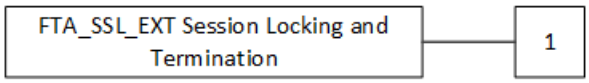
Class FTA: TOE Access

FTA_SSL_EXT Session Locking and Termination

Family Behavior

This family defines requirements for session locking capabilities that are not addressed by FTA_SSL in CC Part 2.

Component Leveling



FTA_SSL_EXT.1 TSF- and User-initiated Locked State, requires the TSF to manage the transition to a locked state and what operations can be performed.

Management: FTA_SSL_EXT.1

The following actions could be considered for the management functions in FMT:

a) Configuring session locking policy.
b) Transitioning to the locked state.

Audit: FTA_SSL_EXT.1

There are no auditable events foreseen.

FTA_SSL_EXT.1 TSF- and User-initiated Locked State

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL_EXT.1.1 The TSF shall transition to a locked state after a time interval of inactivity.

FTA_SSL_EXT.1.2 The TSF shall transition to a locked state after initiation by either the user or the administrator.

FTA_SSL_EXT.1.3 The TSF shall, upon transitioning to the locked state, perform the following operations:

a. clearing or overwriting display devices, obscuring the previous contents;
b. [**assignment**: *other actions performed upon transitioning to the locked state*].

Class FTP: Trusted Path/Channels

FTP_ITC_EXT Inter-TSF Trusted Channel

Family Behavior

This family defines requirements for trusted channels that are not addressed by FTP_ITC in CC Part 2 because they apply specifically to channels required by a mobile device.

Component Leveling

FTP_ITC_EXT.1 Trusted Channel Communication, requires the TSF to manage the communication channel between itself and other trusted products.

Management: FTP_ITC_EXT.1

The following actions could be considered for the management functions in FMT:

a) Configuring the actions that require trusted channel, if applicable.
b) Enabling/disabling communications protocols where the TSF acts as a server.

Audit: FTP_ITC_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Initiation and termination of trusted channel.

FTP_ITC_EXT.1 Trusted Channel Communication

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC_EXT.1.1 The TSF shall use

- 802.11-2012 in accordance with [**assignment:** *requirements or standards defining implementation of this protocol*],
- 802.1X in accordance with [**assignment:** *requirements or standards defining implementation of this protocol*],
- EAP-TLS in accordance with [**assignment:** *requirements or standards defining implementation of this protocol*],
- mutually authenticated TLS as defined in [**assignment:** *requirements or standards defining implementation of this protocol*]

and [**assignment:** *other protocols*]

] protocols to provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels, provides assured identification of its end points, protects channel data from disclosure, and detects modification of the channel data.

FTP_ITC_EXT.1.2 The TSF shall permit the TSF to initiate communication via the trusted channel.

FTP_ITC_EXT.1.3 The TSF shall initiate communication via the trusted channel for wireless access point connections, administrative communication, configured enterprise connections, and [**selection**: *OTA updates*, *no other connections*].