Extended Component Definitions

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

Background and Scope

This Appendix provides a definition for all 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_RBG_EXT Random Bit Generation
	FCS_STO_EXT Storage of Credentials
User Data Protection (FDP)	FDP_DAR_EXT Data-at-Rest Encryption
	FDP_DEC_EXT Access to Platform Resources
	FDP_NET_EXT Network Communications
Identification and Authentication (FIA)	FIA_X509_EXT X.509 Validation of Certificates
Security Management (FMT)	FMT_CFG_EXT Secure by Default Configuration
	FMT_MEC_EXT Supported Configuration Mechanism
Privacy (FPR)	FPR_ANO_EXT User Consent for Transmission of Personally Identifiable Information
Protection of the TSF (FPT)	FPT_AEX_EXT Anti-Exploitation Capabilities
	FPT_API_EXT Use of Supported Services and APIs
	FPT_IDV_EXT Software Identification and Versions
	FPT_LIB_EXT Use of Third Party Libraries
	FPT_TUD_EXT TSF Updates
Trusted Path/Channels (FTP)	FTP_DIT_EXT Protection of Data in Transit

Extended Component Definitions

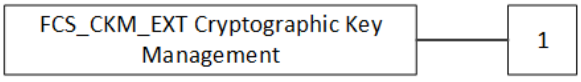
Class FCS: Cryptographic Support

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 Generation Services, requires the TSF to specify whether asymmetric key generation is implemented by the TSF, invoked from the operational environment, or not used by the TOE.

Management: FCS_CKM_EXT.1

There are no management functions foreseen.

Audit: FCS_CKM_EXT.1

There are no auditable events foreseen.

FCS_CKM_EXT.1 Cryptographic Key Generation Services

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_CKM_EXT.1.1 The application shall [**selection**:

- *generate no asymmetric cryptographic keys,*
- *invoke platform-provided functionality for asymmetric key generation*
- *implement asymmetric key generation*

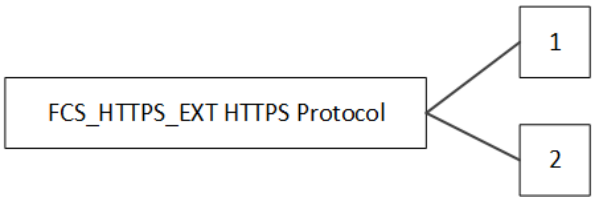
].

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, defines the capability of the TOE to implement HTTPS.

FCS_HTTPS_EXT.2 HTTPS Protocol with Mutual Authentication, defines HTTPS capabilities relating specifically to the case where the TOE acts as an HTTPS server that enforces mutual authentication.

Management: FCS_HTTPS_EXT.1

There are no management functions foreseen.

Audit: FCS_HTTPS_EXT.1

There are no auditable events foreseen.

Management: FCS_HTTPS_EXT.2

There are no management functions foreseen.

Audit: FCS_HTTPS_EXT.2

There are no auditable events foreseen.

FCS_HTTPS_EXT.1 HTTPS Protocol

Hierarchical to: No other components.

Dependencies: FIA_X509_EXT.1 X.509 Certificate Validation

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

FCS_HTTPS_EXT.1.2 The application shall implement HTTPS using TLS as defined in the TLS package.

FCS_HTTPS_EXT.1.3 The application shall [**assignment**: *take some action*] if the peer certificate is deemed invalid.

FCS_HTTPS_EXT.2 HTTPS Protocol with Mutual Authentication

Hierarchical to: No other components.

Dependencies: FCS_HTTPS_EXT.1 HTTPS Protocol

FIA_X509_EXT.1 X.509 Certificate Validation

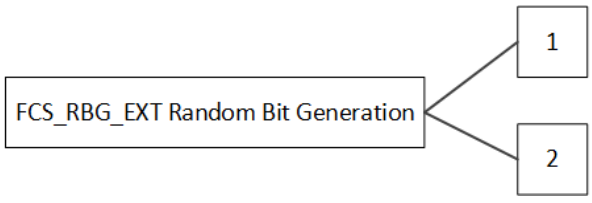
FCS_HTTPS_EXT.2.1 The application shall [**selection**: *not establish the connection, establish or not establish the connection based on an administrative or user setting]* if the peer certificate is deemed invalid.

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 Services, requires the TSF to specify whether random bit generation is implemented by the TSF, invoked from the operational environment, or not used by the TOE.

FCS_RBG_EXT.2 Random Bit Generation from Application, specifies the mechanism by which the TSF generates random bits.

Management: FCS_RBG_EXT.1

There are no management functions foreseen.

Audit: FCS_RBG_EXT.1

There are no auditable events foreseen.

Management: FCS_RBG_EXT.2

There are no management functions foreseen.

Audit: FCS_RBG_EXT.2

There are no auditable events foreseen.

FCS_RBG_EXT.1 Random Bit Generation Services

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RBG_EXT.1.1 The application shall [selection:

- *use no DRBG functionality,*
- *invoke platform-provided DRBG functionality,*
- *implement DRBG functionality*

] for its cryptographic operations.

FCS_RBG_EXT.2 Random Bit Generator State Preservation

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic Operation

FCS_RBG_EXT.1 Random Bit Generation Services

FCS_RBG_EXT.2.1 The application shall perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using [**selection**: *Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)*]

FCS_RBG_EXT.2.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from a platform-based DRBG and [**selection**:

- *a software-based noise source,*
- *a hardware-based noise source,*
- *no other noise source*

] with a minimum of [**selection**:

- *128 bits,*
- *256 bits*

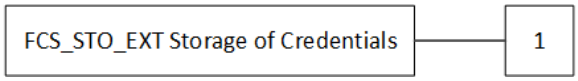
] of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.

FCS_STO_EXT Storage of Credentials

Family Behavior

This family defines requirements for the secure storage of credential data.

Component Leveling



FCS_STO_EXT.1 Storage of Credentials, requires the application to define how to store credentials to non-volatile memory.

Management: FCS_ STO_EXT.1

There are no management functions foreseen.

Audit: FCS_ STO_EXT.1

There are no auditable events foreseen.

FCS_STO_EXT.1 Storage of Credentials

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_STO_EXT.1.1 The application shall [**selection**:

- *not store any credentials,*
- *invoke the functionality provided by the platform to securely store [**assignment**: list of credentials],*
- *implement functionality to securely store [**assignment**: list of credentials] according to [**assignment**: cryptographic mechanism]*

] to non-volatile memory.

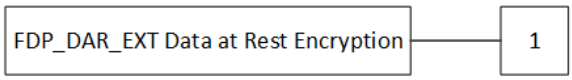
Class FDP: User Data Protection

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 Encryption of Sensitive Application Data, requires the application to be able to protect all data with a chosen method of encryption.

Management: FDP_DAR_EXT.1

There are no management functions foreseen.

Audit: FDP_DAR_EXT.1

There are no auditable events foreseen.

FDP_DAR_EXT.1 Encryption of Sensitive Application Data

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_DAR_EXT.1.1 The application shall [**selection**:

- *leverage platform-provided functionality to encrypt sensitive data,*
- *implement functionality to encrypt sensitive data as defined in the PP-Module for File Encryption,*
- *protect sensitive data in accordance with FCS_STO_EXT.1,*
- *not store any sensitive data*

] in non-volatile memory

FDP_DEC_EXT Access to Platform Resources

Family Behavior

This family defines requirements for accessing platform resources.

Component Leveling

FDP_DEC_EXT.1 Access to Platform Resources, requires the application to restrict access to hardware sources and sensitive information repositories.

Management: FDP_DEC_EXT.1

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

a) enable/disable the transmission of any information describing the system's hardware, software, or configuration.

Audit: FDP_DEC_EXT.1

There are no auditable events foreseen.

FDP_DEC_EXT.1 Access to Platform Resources

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_DEC_EXT.1.1 The application shall restrict its access to [***assignment****: system hardware resources*].

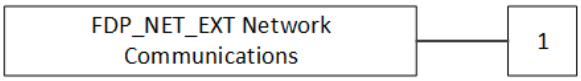
FDP_DEC_EXT.1.2 The application shall restrict its access to [**assignment:** *sensitive information repositories*].

FDP_NET_EXT Network Communications

Family Behavior

This family defines requirements for the TOE's use of network connectivity.

Component Leveling



FDP_NET_EXT.1 Network Communications, identifies the purpose for each network interface used by the TOE and how that interface is invoked.

Management: FDP_NET_EXT.1

There are no management functions foreseen.

Audit: FDP_NET_EXT.1

There are no auditable events foreseen.

FDP_NET_EXT.1 Network Communications

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_NET_EXT.1.1 The application shall restrict network communication to [**selection**:

- *no network communication,*
- *user-initiated communication for [**assignment**: list of functions for which the user can initiate network communication],*
- *respond to [**assignment**: list of remotely initiated communication],*
- *[**assignment**: list of application-initiated network communication]*

].

Class FIA: Identification and Authentication

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 Certificate Validation, specifies the rules the TSF must follow to determine if an X.509 certificate is valid.

FIA_X509_EXT.2 X.509 Certificate Authentication, defines the TOE's usage of X.509 certificates and how it reacts to certificates that cannot be validated.

Management: FIA_X509_EXT.1

There are no management functions foreseen.

Audit: FIA_X509_EXT.1

There are no auditable events foreseen.

Management: FIA_X509_EXT.2

There are no management functions foreseen.

Audit: FIA_X509_EXT.2

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

a) configuration of TSF behavior in the event that certificate revocation status cannot be verified.

FIA_X509_EXT.1 X.509 Certificate Validation

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_X509_EXT.1.1 The application shall [**selection**: *invoked platform-provided functionality, implement functionality*] to validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.

- The application 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 application shall validate that any CA certificate includes caSigning purpose in the key usage field.
- The application shall validate the revocation status of the certificate using [**selection**: *OCSP as specified in RFC 6960, CRL as specified in RFC 5280 Section 6.3, CRL as specified in RFC 8603, 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 application 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 EKU field.
    - 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.
    - S/MIME certificates presented for email encryption and signature shall have the Email Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) 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.
    - 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.

FIA_X509_EXT.1.2 The application shall treat a certificate as a CA certificate only 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 Certificate Validation

[FTP_ITC.1 Inter-TSF Trusted Channel, or

FTP_TRP.1 Trusted Path]

FIA_X509_EXT.2.1 The application shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [**assignment:** *trusted channel or trusted path communications protocol*].

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

Class FMT: Security Management

FMT_CFG_EXT Secure by Default Configuration

Family Behavior

This family defines requirements for authorization to manage the behavior of the application.

Component Leveling

FMT_CFG_EXT.1 Secure by Default Configuration, requires the application to define how to set new credentials and protect the application from modification by unprivileged users.

Management: FMT_CFG_EXT.1

There are no management functions foreseen.

Audit: FMT_CFG_EXT.1

There are no auditable events foreseen.

FMT_CFG_EXT.1 Secure by Default Configuration

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_CFG_EXT.1.1 The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials.

FMT_CFG_EXT.1.2 The application shall be configured by default with file permissions which protect the application binaries and data files from modification by normal unprivileged users.

FMT_MEC_EXT Supported Configuration Mechanism

Family Behavior

This family defines requirements for the TOE's use of mechanisms for the storage of configuration data.

Component Leveling

FMT_MEC_EXT.1 Supported Configuration Mechanism, requires the application to store configuration data either through the use of an appropriate environmental mechanism or through its own file encryption capability.

Management: FMT_MEC_EXT.1

There are no management functions foreseen.

Audit: FMT_MEC_EXT.1

There are no auditable events foreseen.

FMT_MEC_EXT.1 Supported Configuration Mechanism

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_MEC_EXT.1.1 The application shall [**selection**:

- *invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.*
- *Implement functionality to encrypt and store configuration options as defined by FDP_PRT_EXT.1 in the PP-Module for File Encryption*].

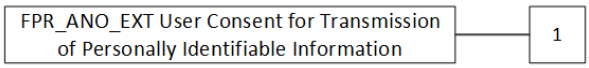
Class FPR: Privacy

FPR_ANO_EXT User Consent for Transmission of Personally Identifiable Information

Family Behavior

This family defines requirements for anonymity that are not covered by the Part 2 family FPR_ANO.

Component Leveling



FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information, requires the TSF to transmit personally identifiable information only with explicit approval.

Management: FPR_ANO_EXT.1

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

a) enable/disable the transmission of any PII.

Audit: FPR_ANO_EXT.1

There are no auditable events foreseen.

FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information

Hierarchical to: No other components.

Dependencies: No dependencies.

FPR_ANO_EXT.1.1 The application shall [**selection**:

- *not transmit PII over a network,*
- *require user approval before executing [**assignment**: list of functions that transmit PII over a network]*

] .

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 Anti-Exploitation Capabilities, requires the application to implement functionality that protects against common software exploits.

Management: FPT_AEX_EXT.1

There are no management functions foreseen.

Audit: FPT_AEX_EXT.1

There are no auditable events foreseen.

FPT_AEX_EXT.1 Anti-Exploitation Capabilities

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_AEX_EXT.1.1 The application shall not request to map memory at an explicit address except for [**assignment**: *list of explicit exceptions*].

FPT_AEX_EXT.1.2 The application shall [**selection**:

- *not allocate any memory region with both write and execute permissions,*
- *allocate memory regions with write and execute permissions for only [**assignment**: list of functions performing just-in-time compilation]*

].

FPT_AEX_EXT.1.3 The application shall be compatible with security features provided by the platform vendor.

FPT_AEX_EXT.1.4 The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.

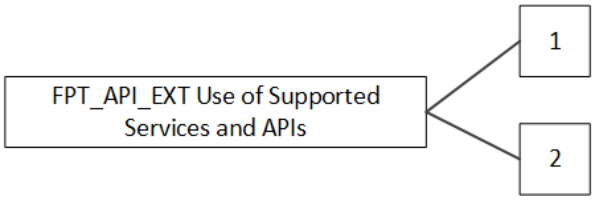
FPT_AEX_EXT.1.5 The application shall be built with stack-based buffer overflow protection enabled.

FPT_API_EXT Use of Supported Services and APIs

Family Behavior

This family defines requirements for specifying the environmental APIs used by the TOE.

Component Leveling



FPT_API_EXT.1 Use of Supported Services and APIs, requires the application to use only documented platform APIs.

FPT_API_EXT.2 Use of Supported Services and APIs, requires the application implement media parsing in a specified manner.

Management: FPT_API_EXT.1

There are no management functions foreseen.

Audit: FPT_API_EXT.1

There are no auditable events foreseen.

Management: FPT_API_EXT.2

There are no management functions foreseen.

Audit: FPT_API_EXT.2

There are no auditable events foreseen.

FPT_API_EXT.1 Use of Supported Services and APIs

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_API_EXT.1.1 The application shall use only documented platform APIs.

FPT_API_EXT.2 Use of Supported Services and APIs

Hierarchical to: No other components.

Dependencies: No dependencies.

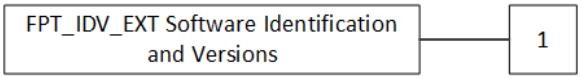
FPT_API_EXT.2.1 The application [**selection**: *shall use platform-provided libraries, does not implement functionality*] for parsing [**assignment**: *list of formats parsed that are included in the IANA MIME media types*].

FPT_IDV_EXT Software Identification and Versions

Family Behavior

This family defines requirements for how to use versioning.

Component Leveling



FPT_IDV_EXT.1 Software Identification and Versions, requires the TSF to specify the versioning mechanism used.

Management: FPT_IDV_EXT.1

There are no management functions foreseen.

Audit: FPT_IDV_EXT.1

There are no auditable events foreseen.

FPT_IDV_EXT.1 Software Identification and Versions

Hierarchical to: No other components.

Dependencies: No dependencies.

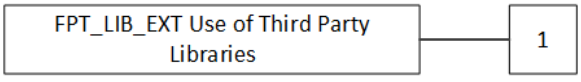
FPT_IDV_EXT.1.1 The application shall be versioned with [**selection**: *SWID tags that comply with minimum requirements from ISO/IEC 19770-2:2015, [**assignment**: other version information]*].

FPT_LIB_EXT TSF Use of Third Party Libraries

Family Behavior

This family defines requirements for identification of any third-party libraries used by the TOE.

Component Leveling



FPT_LIB_EXT TSF Use of Third Party Libraries, requires the TOE to identify the third party libraries that it uses.

Management: FPT_LIB_EXT.1

There are no management functions foreseen.

Audit: FPT_LIB_EXT.1

There are no auditable events foreseen.

FPT_LIB_EXT.1 TSF Use of Third Party Libraries

Hierarchical to: No other components.

Dependencies: No dependencies.

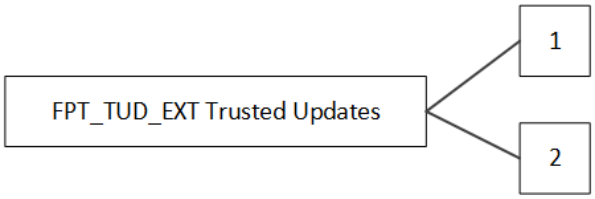
FPT_LIB_EXT.1.1 The application shall be packaged with only [**assignment**: *list of third-party libraries*].

FPT_TUD_EXT Trusted Updates

Family Behavior

This family defines requirements for applying updates to the TOE.

Component Leveling



FPT_TUD_EXT.1 Integrity for Installation and Update, requires the TSF to specify how updates to it are acquired and verified.

FPT_TUD_EXT.2 Integrity for Installation and Update, requires TOE updates to be packaged in a certain manner.

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

There are no management functions foreseen.

Audit: FPT_TUD_EXT.2

There are no auditable events foreseen.

FPT_TUD_EXT.1 Integrity for Installation and Update

Hierarchical to: No other components.

Dependencies: FPT_IDV_EXT.1 Software Identification and Versions

FPT_TUD_EXT.1.1 The application shall [**selection**: *provide the ability, leverage the platform*] to check for updates and patches to the application software.

FPT_TUD_EXT.1.2 The application shall [**selection**: *provide the ability, leverage the platform*] to query the current version of the application software.

FPT_TUD_EXT.1.3 The application shall not download, modify, replace or update its own binary code.

FPT_TUD_EXT.1.4 Application updates shall be digitally signed such that the application platform can cryptographically verify them prior to installation.

FPT_TUD_EXT.1.5 The application is distributed [**selection**: *with the platform OS, as an additional software package to the platform OS*].

FPT_TUD_EXT.2 TSF Integrity for Installation and Update

Hierarchical to: No other components.

Dependencies: FPT_TUD_EXT.1 Integrity for Installation and Update

FPT_TUD_EXT.2.1 The application shall be distributed using the format of the platform-supported package manager.

FPT_TUD_EXT.2.2 The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events.

FPT_TUD_EXT.2.3 The application installation package shall be digitally signed such that its platform can cryptographically verify them prior to installation.

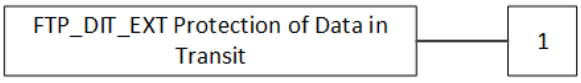
Class FTP: Trusted Path/Channels

FTP_DIT_EXT Protection of Data in Transit

Family Behavior

This family defines requirements for protecting data in transit.

Component Leveling



FTP_DIT_EXT.1 Protection of Data in Transit, requires the TSF to specify what data is transmitted outside the TOE over a trusted channel, what protocol is used for data transmission, and whether the TSF implements this protocol or invokes an environmental interface to do so.

Management: FTP_DIT_EXT.1

There are no management functions foreseen.

Audit: FTP_DIT_EXT.1

There are no auditable events foreseen.

FTP_DIT_EXT.1 Protection of Data in Transit

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_DIT_EXT.1 The application shall [**selection**:

- *not transmit any [**selection**: data, sensitive data],*
- *encrypt all transmitted [**selection**: sensitive data, data] with [**assignment**: trusted protocol],*
- *invoke platform-provided functionality to encrypt all transmitted sensitive data with [**assignment**: trusted protocol],*
- *invoke platform-provided functionality to encrypt all transmitted data with [**assignment**: trusted protocol]*

] between itself and another trusted IT product.