PP-Module for SSL/TLS Inspection Proxy

Version: 1.0

2019-08-23

National Information Assurance Partnership

Revision History

Version	Date	Comment
V1.0	2019-08-23	Initial Release

Table of Contents

1 Introduction

1.1 Overview

The scope of this Protection Profile Module (PP-Module) is to describe the security functionality of SSL/TLS Inspection Proxy in terms of [CC] and to define functional and assurance requirements for such products. This PP-Module is intended for use by the following Base-PPs:

- collaborative Protection Profile for Network Devices (NDcPP), version 2.1

and can be used with the following modules:

- None.

This PP-Module is intended to specify the functionality of a network device that includes limited Certification Authority (CA) functionality to issue certificates for the purpose of providing network security services on the underlying plaintext. The device accomplishes this by terminating an intended TLS session between a monitored client and specified external servers. The device instead establishes a TLS session thread consisting of a TLS session between the device and the external server and a second TLS session between the device, acting as the external server, and the client. By replacing the end-to-end TLS session with two TLS sessions terminated at the TOE, the device is able to provide additional security services based on the decrypted plaintext.

A network device meeting this PP-Module may perform additional security services on the plaintext, provide the decrypted payload to external network devices to perform the security services, or do both. These additional security services, whether processed internally or externally, may be performed inline, or passively. If multiple security services are provided, some may be inline, while others are performed passively. This PP-Module does not cover the specific requirements associated with various additional services.

A TOE that conforms to a PP-Configuration containing this PP-Module may be a ‘Distributed TOE’ as defined in the NDcPP; however, the SSL/TLS Inspection Proxy functionality described in this PP-Module should be in a single TOE component. This PP-Module does not prohibit the TOE from implementing other security functionality in a distributed manner.

1.2 Terms

The following sections provide both Common Criteria and technology terms used in this PP-Module.

1.2.1 Common Criteria Terms

Term	Meaning
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration (PP-Configuration)	A comprehensive set of security requirements for a product type that consists of at least one PP and at least one PP-Module.

Term	Meaning
Protection Profile Module (PP-Module)	An implementation-independent set of security requirements for a specific subset of products described by a PP.
Security Assurance Requirement (SAR)	A requirement for how the TOE's proper implementation of the SFRs is verified by an evaluator.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
Target of Evaluation (TOE)	The product under evaluation.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.

1.2.2 Technology Terms

Term	Meaning
Attribute	A characterization of an entity (monitored client or the server requested by a monitored client) used in the TLS session establishment policy or the plaintext processing policy implemented by the TOE that describes the entity. Common attributes include IP address, name, and certificates associated to an entity.
Block operation	A high-level operation of the TLS session establishment policy implemented by the TOE that prevents TLS sessions between a monitored client and the server requested by the client.
Bypass operation	A high-level operation of the TLS session establishment policy implemented by the TOE that allows a TLS session between a monitored client and the server requested by the client. Alternatively, an operation of the plaintext processing policy implemented by the TOE to bypass certain inspection processing functional components for plaintext data flows established under the SSL/TLS session establishment policy.
Inspect operation	A high-level operation of the TLS session establishment policy implemented by the TOE that establishes a TLS session thread between a monitored client and a server requested by the monitored client in order to provide security services on the underlying plaintext application data.
Inspection processing functional components	A discrete set of security functions implemented within a single logical component, internal or external to the TOE that provides security services based on a plaintext data flow controlled by the TOE intended to protect a monitored client from defined security threats, or to enforce a defined policy regarding the servers allowed to be accessed by monitored clients.
Monitored Client	A TLS client that uses the TOE as an SSL/TLS Inspection Proxy. This device requires a trust anchor to be installed for the internal CA of the TOE, and makes SSL/TLS requests for services external to the enclave. This client makes SSL/TLS requests to a "requested server" through the TOE.

Term	Meaning
Requested Server	The target of an SSL/TLS request by a monitored client through the TOE. It is typically a service provider for clients using SSL/TLS. If mutual authentication is to be supported, this device requires a trust anchor to be installed for the internal CA of the TOE.
SSL/TLS	Secure Sockets Layer/Transport Layer Security (SSL/TLS): A set of security protocols defined by IETF RFCs to establish a secure point-to-point channel between a client and a server. The secure channel provides confidentiality, integrity and proof of origin to plaintext application data transferred between the client and server. SSL refers to early implementations of the SSL/TLS protocols that are deprecated. TLS refers to current versions of the SSL/TLS protocol.
TLS messages	Specific messages defined by TLS protocol standards. The TLS messages addressed in this PP-Module include TLS handshake messages: Client Hello, Server Hello, Server Certificate, Server Key Exchange, Client Key Exchange, Certificate Request, Client Certificate, Client Certificate Verify, Server Finished and Client Finished messages.
TLS session parameters	The parameters of a TLS session established by the TOE for protecting thru-traffic, minimally to include: the negotiated version, negotiated cipher suite, the size of any key exchange values sent or received in key exchange messages, the server certificate received, (a reference to) the server certificate sent, the client certificate received, (a reference to) the client certificate sent, and other negotiated values determined by the TLS handshake that are not fixed for all TLS sessions established.
TLS session thread	A connection negotiated by the TOE consisting of a TLS secure point-to-point channel between a monitored client and the TOE, a TLS secure point-to-point channel between the TOE and the requested server, and any traffic flow containing the underlying application plaintext decrypted from one of the SSL/TLS channels, that is transferred within or between inspection processing functional components controlled by the TOE.

1.3 Compliant Targets of Evaluation

The Target of Evaluation (TOE) may be a single device or a collection of devices that interact with each other to meet the requirements of this PP-Module. Other network devices can be used to supplement inspection of plaintext traffic made available by the TOE. Such external devices will be considered as part of the operational environment, unless they are used to meet the requirements of this PP-Module. Audit, web, or directory servers providing access to certificate validity information generated by the TOE, and intermediate or root certification authorities that issue certificates to the TOE's embedded certification authority are considered part of the operational environment and external to the TOE, but interfaces to these essential services which are required for operation of the TOE will be considered within the TOE boundary. Assurance activities to validate an interface include inspection and exercise of these interfaces using a specific instance of the service (audit server, web server, and external certification authority) implemented within the test environment.

This PP-Module includes some functionality typical of firewalls. In particular, a device meeting this PP-Module is configurable so that it can block or process TLS traffic between monitored clients and requested servers. It's important to note that the device may support TLS connections for remote administration;

these TLS connections are distinct from those between the monitored clients and requested servers, and must meet different requirements. In the case of an SSL/TLS inspection proxy, the primary processing is to inspect the TLS traffic. A TOE also has the capability of passing the TLS handshake messages intact to allow end-to-end TLS encrypted traffic between monitored clients and specific servers without providing additional services (bypass the inspection) on decrypted traffic. The decision to drop, process, or bypass traffic is based on IP addresses and ports, as well as on the content of TLS handshake messages, including the certificate of the server, and other characteristics of the traffic that might be available. A device can also determine which additional security services, especially those provided by external network devices, are applied to a particular session based on the plaintext exposed, such as HTTP headers including uniform resource locators (URLs), user passwords, or other sensitive information.

This PP-Module does not require facilitating inspection of mutually authenticated TLS sessions. It does not address the management of clients required to support inspection, nor requirements to avoid monitored clients from discovering the existence of such inspection. Processing to support Certificate Pinning is included as an optional requirement since establishing an inspection point prevents the monitored clients from doing so themselves. Similarly, management of the TOE's certificate trust store is required, since monitored clients cannot block traffic from sites using certificates issued by compromised CA certificates after the traffic is inspected.

1.3.1 TOE Boundary

An SSL/TLS Inspection Proxy (STIP) is one or more network devices that uses CA functionality to replace an end-to-end TLS session with a TLS session between the STIP and a monitored client and another TLS session between the STIP and the TLS endpoint requested by the monitored client (the requested server). Additional functionality within the same network component as STIP functionality, or via external network devices, can be used to perform network security services, such as performing intrusion detection or providing reputation services on the plaintext traffic made available by the TOE. This functionality, while enabled by the TOE is out of scope. However, protecting and separating traffic flows of plaintext to or between discrete functional components performing such network security services is required and considered within the TOE. If the TOE provides an external interface to plaintext traffic for additional network security services, the entirety of all external processing will be considered a single functional component – the TOE is not responsible for controlling the flow of traffic among external systems.

All functionality described by the SFRs are within the TOE boundary, as is the ability for the TSF to establish secure remote connections with trusted entities in the Operational Environment (OE).

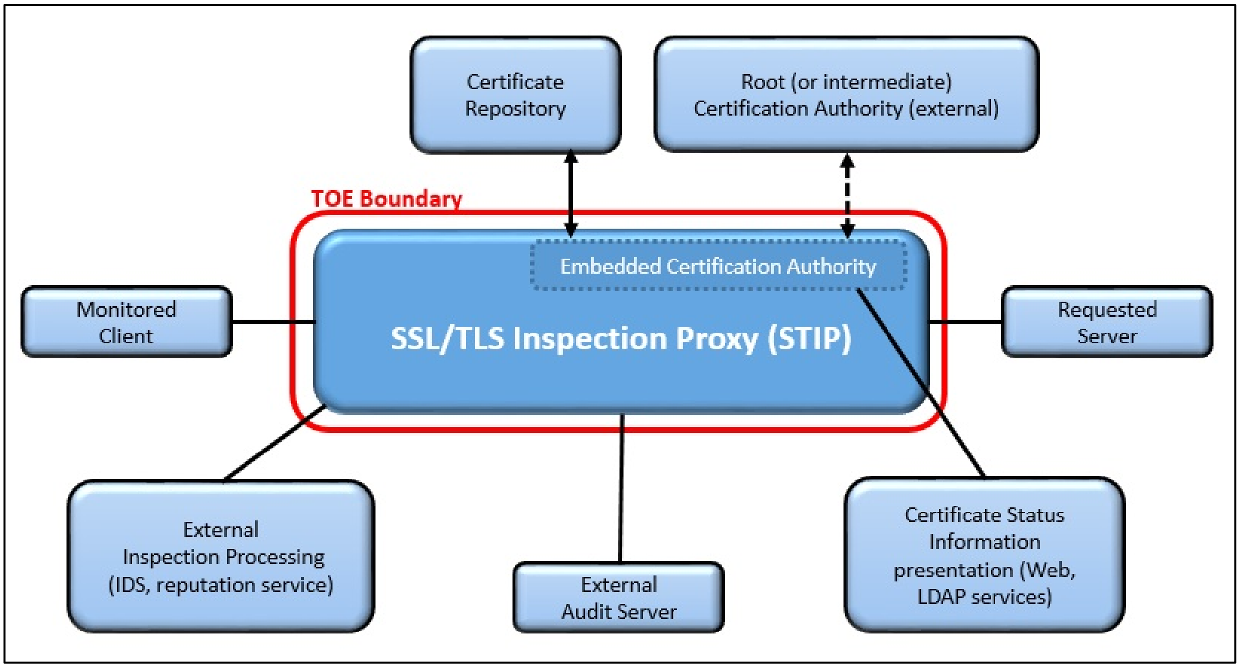

Certificate Repository
Root (or intermediate) Certification Authority (external)
TOE Boundary
Embedded Certification Authority
SSL/TLS Inspection Proxy (STIP)
Monitored Client
Requested Server
External Inspection Processing (IDS, reputation service)
External Audit Server
Certificate Status Information presentation (Web, LDAP services)

Figure 1 – TLS Inspection Infrastructure

As can be seen from this figure, the TOE sits between a monitored client and requested server in order to intercept TLS traffic between them. For connections subject to inspection, the TOE will replace the end-to-end TLS session between the monitored client and requested server and establish a TLS session thread in order to forward the plaintext application traffic to one or more inspection processing functional components in the operational environment for inspection. The TSF provides an embedded CA that is used to reconstruct the TLS channel and pass it to its intended destination in an encrypted format. The embedded CA provides certificates it issues to an (external) certificate repository and provides certificate status information to an (internal or external) certificate status presentation mechanism.

1.4 Use Cases

Requirements in this PP-Module are designed to address the security problem in the following use cases. The description of these use cases provide instructions for how the TOE and its OE should be made to support the functionality required by this PP-Module.

TLS Forward Proxy with inspection:

Inspection Operation

The TOE intercepts traffic authorized for inspection from monitored clients requesting a server-only authenticated TLS session with a requested server. The TOE initiates a TLS session with the requested server and validates the requested server’s certificate as legitimately issued by a trusted element of its trust store. The TOE authenticates the server on behalf of the client and generates a certificate that indicates the TOE is an authorized proxy for the requested server. The certificate is issued by the TOE’s embedded CA, which is trusted by the monitored client. The TOE establishes a valid TLS session with the monitored client using the issued certificate. Any TLS traffic between the monitored client and the requested server is decrypted by the TOE and assigned to a unique TLS session thread that is routed to one or more inspection processes, and encrypted into the respective TLS sessions.

TLS Bypass Operation

The TOE determines that TLS traffic between a monitored client and a requested server is not to be decrypted for inspection, and routes the TLS handshake messages without modification.

TLS Blocking Operation

The TOE determines that a TLS session between a monitored client and a requested server is not authorized, and then performs a blocking operation that refuses to pass the attempted TLS traffic. In addition to dropping and logging of incoming TLS messages, an error response to the client may be provided. The blocking operation may be invoked during the initial TLS handshake, or during the processing of decrypted traffic obtained as part of an inspection operation. In the latter case, a transition from inspection operation to blocking operation includes termination of the TLS session thread.

Exception Processing

The TOE supports allowances for inspection of TLS sessions using outdated TLS versions, cipher suites, or key exchange values, and for servers using invalid certificates. These are managed such that monitored clients, requested servers, or (optionally) specific client-server pairs can be associated with allowed TLS versions, cipher suites, and key exchange values.

This PP-Module permits the inspection of mutually-authenticated TLS sessions between monitored clients and requested servers via exception processing. However, as a best practice, it is recommended instead that this behavior be handled as part of the TLS Inspection Bypass and/or TLS Session Blocking functionality. If the TOE provides inspection processing for mutually authenticated traffic, the ST must claim these optional SFRs.

This PP-Module does not specify routing policies for non-TLS traffic and exception processing should not be used to address functionality otherwise included in the collaborative Protection Profile for Stateful Traffic Filter Firewalls.

2 Conformance Claims

Conformance Statement

This PP-Module has a conformance type of Exact Conformance, inherited from its Base-PP, the NDcPP version 2.1.

CC Conformance Claims

This PP-Module is conformant to Parts 2 (extended) and 3 (conformant) of the Common Criteria Version 3.1, Revision 5 [CC].

PP Claims

This PP-Module does not claim conformance to any Protection Profile.

Package Claims

This PP-Module does not claim conformance to any packages.

3 Security Problem Description

The TLS Inspection Proxy is a network device that embeds limited CA functionality to support the replacement of end-to-end TLS sessions with TLS session threads, making the underlying plaintext available to additional network security functionality. As such, it exposes data within the TOE boundary, and to external processes, which would normally be encrypted. It manages a CA signing key that is trusted by the monitored clients to issue TLS server certificates representing the requested servers for which inspection is authorized.

The security problem is described in terms of the threats that the TOE is expected to address, assumptions about its operational environment, and any organizational security policies the TOE is expected to enforce. Note that as a PP-Module of the NDcPP, all threats, assumptions, and OSPs defined in the Base-PP will also apply to the TOE unless otherwise specified.

The Security Functional Requirements (SFRs) defined in this PP-Module will mitigate the threats that are defined in the PP-Module but will also mitigate some Base-PP threats in more comprehensive detail due to the specific capabilities provided by the TOE.

3.1 Threats

T.UNTRUSTED_COMMUNICATION

Untrusted intermediate systems have access to provide unauthorized communications to the TOE, or to manipulate authorized TLS messages in an attempt to compromise the TOE, the monitored clients, or the requested servers. Within this PP-Module, the focus is on an adversary that controls or exploits a requested server that may attempt to cause the device to inappropriately bypass inspection.

Use of weak cryptography can allow adversary access to plaintext intended by the monitored clients to be encrypted. Such access could disclose user passwords that facilitate additional activities against users of monitored clients. Within this PP-Module, the focus is on the use of weak cryptography and adversary attempts to degrade the cryptographic operations within the TLS protocol.

External network security devices may communicate with the TOE to apply security services to the exposed plaintext. An adversary may attempt to gain access the plaintext via misrouting of traffic or manipulate the traffic in such a way as to cause unauthorized exposure, denial of service, or corruption of the underlying plaintext.

(O.PROTECTED_COMMUNICATIONS)

T.AUDIT

Certificates issued by the device are trusted by monitored clients, and are required for analysis if traffic processed by the device causes the client to fail or become compromised. Unknown activity related to the issuance and use of certificates can allow an adversary to mask client exploits through or via the TOE, especially if the device fails before the incident can be understood. Unknown activity associated to routing configurations, communications with the TOE, as well as the decision to bypass inspection of traffic can allow an adversary to mask attempts to access monitored clients.

(O.AUDIT_LOSS_RESPONSE, O.AUDIT_PROTECTION, O.SYSTEM_MONITORING, OE.AUDIT, OE.CERT_REPOSITORY, OE.CERT_REPOSITORY_SEARCH)

T.UNAUTHORIZED_USERS

In addition to managing administrative credentials, authorized users may have role restrictions to limit their access to the device's certification authority functionality. In addition to the threat of disclosure or modification of authorized user credentials to users without authorized access to the device, a user with limited access might attempt to extend their access by gaining access to other user's credentials.

(O.TOE_ADMINISTRATION)

T.CREDENTIALS

In addition to device credentials used in protected communications, the device maintains a trusted certification authority signing key. Any disclosure or unauthorized manipulation of the signing key can result in unintended certificates, signed executable, or signed data that would be trusted by monitored clients. Any modification of the signing key can result in denial of service to inspection capabilities, or to the monitored clients.

(O.CERTIFICATES, O.PERSISTENT_KEY_PROTECTION, OE.CERT_REPOSITORY)

T.SERVICES

Manipulation of the device can result in issued certificates being used for unauthorized purposes or abuse of inspection services. An authorized user (AU) (or adversary able to gain access to AU credentials) can access or misuse device services, or disclose sensitive or security critical data.

(O.CERTIFICATES, O.PROTECTED_COMMUNICATIONS, O.TOE_ADMINISTRATION)

T.DEVICE_FAILURE

Failure of the certification authority component can result in unauthorized or improperly constrained certificates, or the inability to properly manage the validity of issued certificates. Failure of routing traffic to inspection processing (internal or external) can result in unauthorized disclosure or modification of traffic, or denial of service to monitored clients.

(O.CERTIFICATES, O.INTEGRITY_PROTECTION, O.PERSISTENT_KEY_PROTECTION, O.RECOVERY)

T.UNAUTHORIZED_DISCLOSURE

In addition to general threats to network devices, the TOE controls access to sensitive data that is intended by the monitored client to be encrypted.

(O.PROTECTED_COMMUNICATIONS, O.TOE_ADMINISTRATION)

T.INAPPROPRIATE_ACCESS

Decryption services applied to traffic between monitored clients and unintended servers can violate privacy laws, or disclose unauthorized traffic to inspection processes. Certification authority signature applied to unauthorized data could facilitate adversary exploits of monitored clients.

(O.RESIDUAL_INFORMATION_CLEARING, O.TOE_ADMINISTRATION, OE.RESIDUAL_INFORMATION)

3.2 Assumptions

This section describes modifications to the assumptions made in the NDcPP as they apply to SSL/TLS inspection devices in particular. These assumptions are inherited from the NDcPP with additions specified in **bold** and deletions specified in ~~strikethrough~~. Assumptions from the Base-PP not listed here apply as stated. There are no assumptions that are unique to the functionality described in this PP-Module. An SSL/TLS inspection device is not expected to provide assurance in any of the areas addressed by the modified assumptions, and as a result, requirements are not included to mitigate the threats associated.

A.LIMITED_FUNCTIONALITY

> **An SSL/TLS inspection proxy** device is assumed to provide networking functionality, **issue and manage certificates, encrypt and decrypt SSL/TLS traffic, and perform security services on the SSL/TLS traffic and its decrypted payload** as its core functions and not provide other functionality or services that could be deemed as general-purpose computing. For example, the device should not provide a computing platform for general purpose applications.

~~A.NO_THROUGH_TRAFFIC_PROTECTION~~

> *Rationale: An SSL/TLS inspection proxy device exposes the underlying plaintext of SSL/TLS encrypted traffic and must protect this data as it transits the device.*

A.TRUSTED_ADMINISTRATOR

> The Security Administrator**s** for the **SSL/TLS inspection proxy** device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords and credentials have sufficient strength and entropy.~~ and to lack malicious intent when administering the device~~. ~~The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.~~
>
> *Rationale: An SSL/TLS inspection proxy includes signing credentials that are trusted by monitored clients, and can have security impact beyond the device if not properly managed. At a minimum, integrity of the audit record of administrator actions and of critical functionality is required to hold administrators of the SSL/TLS device accountable for their actions, and to be able to recover from any errors or malicious activity that may impact monitored clients. Note that this might not require additional privileged roles for managing the SSL/TLS inspection proxy device if the audit mechanism and local audit records cannot be modified.*

A.RESIDUAL_INFORMATION

> The security administrator **invokes available features of the SSL/TLS inspection proxy device to** ensure that there is no unauthorized access possible for sensitive residual information **(e.g., decrypted SSL/TLS payload, ephemeral keys), when equipment is discarded or removed from its operational environment, and that persistent secret and private keys** (e.g. cryptographic keys, keying material, PINs, passwords etc.) **are permanently destroyed** on **SSL/TLS** inspection proxy equipment.

Rationale: Any exposure of the SSL/TLS inspection device's persistent secret and private keys can seriously impact the security of the monitored clients.

3.3 Organizational Security Policies

This section describes the organizational security policies the TOE may be expected to satisfy. P.ACCESS_BANNER is inherited from the NDcPP, with additions specified in **bold** that pertain to modifications to the policy required as a result of the functionality described in this PP-Module. P.AUTHORIZATION_TO_INSPECT is required as a result of the functionality required by the PP-Module that can inspect TLS traffic that a client might otherwise assume is encrypted. This policy does not conflict with policies (or functionality) described by the Base-PP.

P.ACCESS_BANNER

The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE. **The TOE may be required to additionally provide a consent to monitor notice for users whose traffic is inspected by the device, if the monitored client might not provide such a banner.**

(O.DISPLAY_BANNER)

P.AUTHORIZATION_TO_INSPECT

The authority to inspect client traffic may be limited by law, regulation, or policies based on the monitored client, requested server, or nature of the traffic.

(O.DISPLAY_BANNER, O.PROTECTED_COMMUNICATIONS, O.TOE_ADMINISTRATION)

4 Security Objectives

4.1 Security Objectives for the TOE

Security objectives for the TOE are listed here. Note that TOE objectives are satisfied by SFRs defined in this PP-Module as well as those in the NDcPP, as indicated.

O.AUDIT_LOSS_RESPONSE

The TOE will respond to possible loss of audit records when an audit trail cannot be written to by restricting auditable events.

Addressed by: FAU_STG.4

O.AUDIT_PROTECTION

The TOE will protect audit records against unauthorized access, modification, or deletion to ensure accountability of user actions.

Addressed by: FAU_SAR.1 (optional), FAU_STG.1 (NDcPP)

O.CERTIFICATES

The TSF must ensure that certificates, certificate revocation lists, and certificate status information are valid.

Addressed by: FDP_CER_EXT.1, FDP_CER_EXT.2, FDP_CER_EXT.3, FDP_CER_EXT.4 (selection-based), FDP_CER_EXT.5 (selection-based), FDP_CRL_EXT.1 (selection-based), FDP_CSI_EXT.1 (selection-based), FDP_CSI_EXT.2 (selection-based), FDP_CSIR_EXT.1, FDP_OCSP_EXT.1 (selection-based), FDP_OCSPS_EXT.1 (selection-based), FDP_PIN_EXT.1 (optional), FIA_ENR_EXT.1, FIA_ESTC_EXT.1 (selection-based), FIA_ESTC_EXT.2 (objective), FIA_X509_EXT.1/STIP, FIA_X509_EXT.2 (NDcPP), FIA_X509_EXT.3 (NDcPP, selection-based)

O.DISPLAY_BANNER

The TOE will display an advisory warning regarding use of the TOE.

Addressed by: FTA_TAB.1 (NDcPP), FTA_TAB.1/TLS (selection-based)

O.INTEGRITY_PROTECTION

The TOE will provide appropriate integrity protection for TSF data and software and any user data stored by the TOE.

Addressed by: FPT_FLS.1, FPT_TST_EXT.1 (NDcPP)

O.PERSISTENT_KEY_PROTECTION

The TOE will provide appropriate confidentiality and access protection to persistent keys and security critical parameters stored by the TOE.

Addressed by: FCS_STG_EXT.1, FDP_STG_EXT.1, FPT_KST_EXT.1, FPT_KST_EXT.2

O.PROTECTED_COMMUNICATIONS

The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities. The TOE will protect data assets when they are being transmitted to and from the TOE, including through intervening untrusted components.

Addressed by: FCS_CKM.4 (NDcPP), FCS_CKM_EXT.5 (selection-based), FCS_COP.1/STIP, FCS_TLSC_EXT.1 (NDcPP), FCS_TTTC_EXT.1, FCS_TTTC_EXT.3 (selection-based), FCS_TTTC_EXT.4 (selection-based), FCS_TTTC_EXT.5, FCS_TLSS_EXT.1 (NDcPP), FCS_TTTS_EXT.1, FCS_TTTS_EXT.3 (selection-based), FCS_TTTS_EXT.4 (selection-based), FDP_PPP_EXT.1, FDP_PRC_EXT.1, FDP_STIP_EXT.1, FDP_STIP_EXT.2 (selection-based), FDP_TEP_EXT.1, FTP_ITC.1 (NDcPP)

O.RECOVERY

The TOE will have the ability to store and recover to a previous state at the direction of the administrator (e.g., provide support for archival and recovery capabilities).

Addressed by: FPT_FLS.1, FCS_CKM_EXT.5 (selection-based), FPT_RCV.1

O.RESIDUAL_INFORMATION_CLEARING

The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.

Addressed by: FDP_RIP.1

O.SYSTEM_MONITORING

The TOE will provide the ability to generate audit data and send that data to an external IT entity. The TOE will record in audit records: date and time of action and the entity responsible for the action. The TOE will provide the ability to store and review certificate information.

Addressed by: FAU_GEN.1 (NDcPP), FAU_GCR_EXT.1, FAU_SCR_EXT.1 (selection-based), FAU_SAR.3 (optional), FAU_STG_EXT.1 (NDcPP)

O.TOE_ADMINISTRATION

The TOE will provide mechanisms to ensure that only privileged users are able to log in and configure the TOE, and provide protections for logged-in users. The TOE will ensure that administrative responsibilities are separated across different roles in order to mitigate the impact of improper administrative activities or unauthorized administrative access.

Addressed by: FMT_MOF.1, FMT_SMF.1 (NDcPP), FMT_SMR.2 (NDcPP)

4.2 Security Objectives for the Operational Environment

This section describes modifications to the security objectives for the operational environment made in the NDcPP as they apply to SSL/TLS inspection devices in particular. These assumptions are inherited from the NDcPP with additions specified in **bold** and deletions specified in ~~strikethrough~~.

Note that this PP-Module allows the ST author in some cases to select if the TSF or OE is invoked to perform some function. There are objectives for the OE that correspond to those SFRs, covering the case where the ST author selects the item pertaining to the OE being invoked to perform the function. If the TOE performs all such functions (that is, the OE-related selection is not chosen), then the corresponding objective for the OE will need to be removed by the ST author.

~~OE.NO_THRU_TRAFFIC_PROTECTION~~

Rationale: An SSL/TLS inspection proxy device exposes the underlying plaintext of SSL/TLS encrypted traffic and must protect this data as it transits the device. Therefore, this specific type of network device will provide through traffic protection so this objective does not apply.

OE.RESIDUAL_INFORMATION

The security administrator ensures there is no unauthorized access possible for sensitive residual information (e.g. **decrypted SSL/TLS payload**, ephemeral keys, PINs, passwords, etc.) **and that persistent secret and private keys are permanently destroyed** on networking equipment when the equipment is discarded or removed from its operational environment.

Rationale: Any exposure of the SSL/TLS inspection device's persistent secret and private keys can seriously impact the security of the monitored clients. Therefore, the objective for the environment to destroy residual information is applied to this data.

OE.AUDIT

The operational environment includes an audit server with adequate storage to retain the audit record, and the audit server provides adequate availability, integrity, and access control to the audit record to support operational requirements. Administration of the audit server is separate from that of the SSL/TLS inspection proxy, and can support all required role separations.

Rationale: Each certificate issued by the SSL/TLS inspection device is trusted by monitored clients for the validity period asserted in the certificate. Inappropriate issuance or use of certificates issued by the SSL/TLS inspection device may require the circumstances of the issuance to be investigated, and appropriate actions (e.g., certificate revocation, administrative actions, etc.) to be taken.

OE.CERT_REPOSITORY

The OE provides a certificate repository for storage of certificates (and optionally CRLs) issued by the TSF.

Rationale: Each certificate issued by the SSL/TLS inspection device is trusted by monitored clients for the validity period asserted in the certificate. Inappropriate issuance of certificates, especially certificates with code-signing or which can act as subordinate CAs to issue additional certificates, or inappropriate use of certificates issued by the SSL/TLS inspection device to conduct unauthorized inspection, or to gain access to protected resources may require the circumstances of the issuance to be investigated, and appropriate actions (e.g., certificate revocation, administrative actions, etc.) to be taken.

OE.CERT_REPOSITORY_SEARCH

The OE provides the ability to search a certificate repository for specific certificate fields in certificates issued by the TSF and return the certificate and an identifier for the certificate that can

be used to search the audit trail for events related to that certificate and for unauthorized or improperly constrained certificates.

Rationale: Each certificate issued by the SSL/TLS inspection device is trusted by monitored clients for the validity period asserted in the certificate. Inappropriate issuance or use of certificates issued by the SSL/TLS inspection device may require the circumstances of the issuance to be investigated, and appropriate actions (e.g., certificate revocation, administrative actions, etc.) to be taken.

4.3 Security Objectives Rationale

This section describes how the threats, assumptions, and organizational security policies map to the security objectives. All mappings and rationale are included in the table below.

Threat, Assumption, or Policy	Security Objectives	Rationale
T.UNTRUSTED_COMMUNICATION	O.PROTECTED_COMMUNICATIONS	Data traversing the TOE is subject to authenticity and integrity verification.
T.AUDIT	O.AUDIT_LOSS_RESPONSE	The TOE provides mechanisms to deal with audit trails being unavailable.
	O.AUDIT_PROTECTION	Audit records are protected from modification, deletion, and unauthorized access.
	O.SYSTEM_MONITORING	Audit records contain the information necessary to determine cause for concerns.
	OE.AUDIT	Storage within an external audit server provides increased record capacity.
	OE.CERT_REPOSITORY	The certificate repository provides a comprehensive set of certificates generated by the TOE that can be searched.
	OE.CERT_REPOSITORY_SEARCH	Ability to search the audit trail for certificate related events provides confidence in certificate validity and proper use.
T.UNAUTHORIZED_USERS	O.TOE_ADMINISTRATION	Use of role separation and authentication mechanisms ensure that only authorized users can access the TOE.
T.CREDENTIALS	O.CERTIFICATES	The TOE tracks certificates, certificate revocation lists, and certificate status information used by the TSF.

	O.PERSISTENT_KEY_PROTECTION	Keys stored on the TOE are protected from unauthorized use and disclosure.
	OE.CERT_REPOSITORY	A certificate repository for all certificates issued by the TOE is provided, making verification straightforward.
T.SERVICES	O.CERTIFICATES	The TOE verifies certificates, certificate revocation lists, and certificate status information prior to any use.
	O.PROTECTED_COMMUNICATIONS	Data traversing the TOE is subject to authenticity, confidentiality, and integrity verification.
	O.TOE_ADMINISTRATION	Use of role separation and authentication mechanisms mitigates the risk of misuse and improper disclosure.
T.DEVICE_FAILURE	O.CERTIFICATES	The TOE verifies certificates, certificate revocation lists, and certificate status information is valid.
	O.INTEGRITY_PROTECTION	Software, TSF, and user data are protected via integrity mechanisms.
	O.PERSISTENT_KEY_PROTECTION	Keys stored on the TOE are protected from unauthorized use and disclosure.
	O.RECOVERY	Administrators have the ability to restore the TOE to a previous (known-good) state.
T.UNAUTHORIZED_DISCLOSURE	O.PROTECTED_COMMUNICATIONS	Data traversing the TOE is subject to authenticity, confidentiality, and integrity verification.
	O.TOE_ADMINISTRATION	Use of role separation and authentication mechanisms mitigates the risk of misuse and ensures the device is properly managed.
T.INAPPROPRIATE_ACCESS	O.RESIDUAL_INFORMATION_CLEARING	The TOE’s lack of residual data retention ensures that unauthorized access to information is not possible.
	O.TOE_ADMINISTRATION	Use of role separation and authentication mechanisms mitigates the risk of misuse and improper disclosure.

	OE.RESIDUAL_INFORMATION	Sensitive information residing within the operational environment, such as keys and decrypted data, are unavailable.
A.LIMITED_FUNCTIONALITY	OE.NO_GENERAL_PURPOSE (Base-PP)	The lack of general purpose computing functionality satisfies this assumption.
A.RESIDUAL_INFORMATION	OE.RESIDUAL_INFORMATION	Sensitive information residing within the operational environment, such as keys and decrypted data, are unavailable.
A.TRUSTED_ADMINISTRATOR	O.TOE_ADMINISTRATION	Use of role separation and authentication mechanisms ensure the device is properly managed, which satisfies the assumption.
P.ACCESS_BANNER	O.DISPLAY_BANNER	The TSF provides an advisory warning regarding use of the TOE.
P.AUTHORIZATION_TO_INSPECT	O.DISPLAY_BANNER	The TOEs advisory warning includes consent to monitor.
	O.PROTECTED_COMMUNICATIONS	The TSF ensures that data traversing the TOE boundary is protected, alleviating concerns about inspection.
	O.TOE_ADMINISTRATION	Administrator roles provide separation of activities and ensure inspection is authorized and performed properly.

Table 1 – Security Objectives Rationale

5 Security Requirements

This chapter describes the security requirements which have to be fulfilled by the TOE. Those requirements comprise functional components from Part 2 and assurance components from Part 3 of [CC]. The following notations are used:

- **Refinement** operation (denoted by **bold text**) is used to add details to a requirement, and thus further restricts a requirement.
- **Selection** (denoted by *italicized text):* is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operation (denoted by *italicized text*) is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- **Iteration** operation is identified with a slash followed by a description of the purpose of the SFR (e.g. "FCS_COP.1/STIP").

5.1 NDcPP Security Functional Requirements Direction

This PP-Module extends the NDcPP (referred to as the Base-PP). The STIP is expected to meet the combination of the security functions described in this PP-Module and the Base-PP.

The requirements from the NDcPP apply in the usual way when used as a Base-PP for this PP-Module. Selection-based requirements are included if the ST author includes an applicable selection from the Base-PP. Optional requirements can be included or excluded as directed by the Base-PP. Distributed TOEs as defined in the NDcPP are allowed, and are constructed according to rules outlined in that document.

The following sections describe the modifications and operations the ST author must make to the SFRs defined in the Base-PP in addition to what is mandated by section 5.3.

5.1.1 Applicable Modified SFRs

The SFRs listed in this section are defined in the Base-PP and relevant to the secure operation of the STIP. SFRs in this section include those that require certain selections, are refined, and that may require additional application notes in order to ensure that the functionality provided by the network device is consistent with the functionality required by the TOE so it conforms to this PP-Module.

FAU_GEN.1 Audit Data Generation

There are additional auditable events that serve to extend the FAU_GEN.1 SFR found in the Base-PP. As such, the following events should be combined with those of the Base-PP in the context of a conforming ST. Note that Table 2 contains auditable events for all SFRs defined in the PP-Module, even those that are optional, selection-based, or objective. The ST does not need to include auditable events for any SFRs that are not claimed by the TOE.

SFR	Auditable Event	Additional Audit Record Contents
FAU_GCR_EXT.1	None	None
FAU_SCR_EXT.1 (selection-based)	None	None

SFR	Auditable Event	Additional Audit Record Contents
FAU_SAR.1 (optional)	None	None
FAU_SAR.3 (optional)	None	None
FAU_STG.4	None	None
FCS_CKM_EXT.5 (selection-based)	None	None
FCS_STG_EXT.1	None	None
FCS_TTTC_EXT.1	Establishment of TLS session	TLS session parameters
FCS_TTTC_EXT.3 (selection-based)	Mutual authentication authorized	[*selection: client certificate value, [assignment: client certificate object identifier]*]
	Mutual authentication not authorized	None
FCS_TTTC_EXT.4 (selection-based)	None	None
FCS_TTTC_EXT.5	None	None
FCS_TTTS_EXT.1	Establishment of TLS session	TLS session parameters
FCS_TTTS_EXT.3 (selection-based)	Mutual authentication required and valid client certificate received	Client certificate
	Mutual authentication not used (all other cases):	None
FCS_TTTS_EXT.4 (selection-based)	None	None
FDP_CER_EXT.1	None	None
FDP_CER_EXT.2	Linking of issued certificate to validated certificate	Success: [*selection: Issued Certificate value, issued certificate object identifier*], [*selection: validated Certificate, validated certificate object identifier*] Failure: Reason for failure
FDP_CER_EXT.3	Certificate generation	Success: [*selection: Certificate value, certificate object identifier*]
FDP_CER_EXT.4 (selection-based)	None	None
FDP_CER_EXT.5 (selection-based)	Certificate generation	Success: [*selection: Certificate value, certificate object identifier*]
FDP_CRL_EXT.1	Failure to generate CRL	None

SFR	**Auditable Event**	**Additional Audit Record Contents**
(selection-based)		
FDP_CSI_EXT.1 (selection-based)	None	None
FDP_CSI_EXT.2 (selection-based)	None	None
FDP_CSIR_EXT.1	None	None
FDP_OCSP_EXT.1 (selection-based)	Failure to generate certificate status information	None
FDP_OCSPS_EXT.1 (selection-based)	Failure to include certificate status information in TLS handshake message	None
FDP_PIN_EXT.1 (optional)	None	None
FDP_PPP_EXT.1	Configuration changes to the plaintext processing policy	None
FDP_PRC_EXT.1	Plaintext routed to inspection processing functional component	TLS Session Thread identifier, [*assignment: processing element identifier*]
FDP_RIP.1	None	None
FDP_STG_EXT.1	None	None
FDP_STIP_EXT.1	Establishment of a TLS inspection session thread	[*assignment: TLS session thread attributes*], [*assignment: client attributes*], and [*assignment: server attributes*] associated to the thread.
	Establishment of an encrypted TLS data flow	[*assignment: encrypted TLS data flow attributes*]
	Bypass operation invoked	TLS Session Thread identifier, identifier(s) of processing element(s) bypassed, reason for bypass (rule invoking)
	Block operation invoked	TLS Session Thread identifier, blocking reason (rule invoking)
FDP_STIP_EXT.2 (selection-based)	None	None
FDP_TEP_EXT.1	Mutual authentication authorized	[*assignment: client attributes obtained from the validated client certificate*]
FIA_ENR_EXT.1	None	None
FIA_ESTC_EXT.1	EST requests	None

SFR	Auditable Event	Additional Audit Record Contents
(selection-based)		
FIA_ESTC_EXT.2 (objective)	None	None
FIA_X509_EXT.1/STIP	None	None
FMT_MOF.1	None	None
FPT_FLS.1	Invocation of failures under this requirement	Indication that the TSF has failed with the type of failure that occurred
FPT_KST_EXT.1	None	None
FPT_KST_EXT.2	All attempts to use the TOE's embedded CA's private signing key, and [*selection, assignment [other secret and private keys], no other*]	Identifier of user or process that attempted access
FPT_RCV.1	The fact that a failure or service discontinuity occurred	None
	Resumption of the regular operation	TSF failure types that are available on recovery
FTA_TAB.1/TLS (selection-based)	None	None

Table 2 – FAU_GEN.1 Audit Event and Details

FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy all cryptographic keys **and critical security parameters, when no longer required** in accordance with the specified cryptographic key destruction method [*assignment:*

- *For plaintext keys in volatile storage, the destruction shall be executed by a [selection:*
  - o *Single overwrite consisting of [selection:*
    - ▪ *a pseudo-random pattern using the TSF's RBG,*
    - ▪ *zeroes,*
    - ▪ *ones,*
    - ▪ *a new value of the key,*
    - ▪ *[assignment: a static or dynamic value that does not contain any CSP]]*
  - o *destruction of reference to the key directly followed by a request for garbage collection];*
- *For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [selection:*
  - o *Logically addresses the storage location of the key and performs a [selection: single, [assignment: number of passes]-pass] overwrite consisting of [selection:*

  - *a pseudo-random pattern using the TSF's RBG,*
  - *zeroes,*
  - *ones,*
  - *a new value of the key,*
  - *[assignment: a static or dynamic value that does not contain any CSP];*
- *Instructs a part of the TSF to destroy the abstraction that represents the key]*]

that meets the following: [*no standard*].

Application Note: *This SFR is refined from its definition in the Base-PP through the inclusion of security critical parameters and clarifies when destruction is required; a STIP device includes persistent keys, including the embedded CA's signing private key that should not be destroyed until they are no longer needed. Security critical parameters includes security related information (e.g., secret and private cryptographic keys, authentication data such as passwords and PINs) appearing in plaintext or otherwise unprotected form and whose disclosure or modification can compromise the security of a CA or the security of the information protected by the CA or the security of the information protected by the CA.*

FIA_X509_EXT.1/Rev X.509 Certificate Validation

Application Note: *There is no change to the text of this SFR or its Evaluation Activities in this PP-Module. However, this PP-Module requires TLS connections (to perform the STIP functions) and certificates associated with those connections. For scoping purposes, it's important to note that for certificates associated with the TLS connections between the TOE and monitored clients/requested servers, the ST author should use FIA_X509_EXT.1/STIP. This requirement from the Base-PP (and the /ITT iteration, if appropriate) should be used for certificates associated other functions.*

FIA_X509_EXT.2 X.509 Certificate Authentication

Since the use of X.509 certificates is required for this technology type, this selection-based SFR as defined in the NDcPP is considered to be mandatory for any TOE whose conformance claim includes this PP-Module. Unlike the FIA_X509_EXT.1 component, this component will apply to all certificates. Additionally, the SFR is refined as follows:

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for **TLS**, [*selection: DTLS, HTTPS, IPsec, SSH, **no other protocols***] and [*selection: code signing for system software updates, 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 **[selection: Security Administrator, CA Operations Staff]** to choose whether **[selection: to accept the***

certificate, to associate the failed connection event per FDP_TEP_EXT.1.5] *in these cases, accept the certificate, not accept the certificate*].

Application Note: *"TLS" is moved outside the selection in the first element, since the TOE must implement TLS to accomplish the STIP functionality. The application notes for the first element from the Base-PP also apply.*

It is worth noting that since this SFR applies to all uses of certificates in the TOE, it may be the case that the actions taken in response to a failure to be able to determine revocation status (which is specified in the 2nd element) is handled differently for different connections. If this is the case, the ST author must make it clear which actions are associated with which connections so that the correct evaluation of the functionality can be performed.

The second element has three modifications from that in the Base-PP. First, the word "validity" is replaced with "revocation status" for clarity. This is consistent with what is in the application note in the NDcPP, and using "revocation status" more directly indicates what is required.

Second, the general notion of "administrator" is replaced with the more refined roles defined in this PP-Module; the ST author should make the appropriate selection.

Finally, a selection is added that allows ST author flexibility in addressing the issue of failure to connect to check revocation status in the specific case that the certificates being checked are associated with either a monitored client or a requested server. This selection ("to associate the failed connection event per FDP_TEP_EXT.1.5"), when chosen, indicates that selected administrative role is able to specify a STIP operation (block, bypass, inspect) to be taken in the event that the revocation status can't be checked. The requirement that the TOE be able to perform this operation when such an event occurs is specified in FDP_TEP_EXT.1.5.

FIA_X.509_EXT.3 X.509 Certificate Requests

There is no change to the text of this SFR or its Evaluation Activities in this PP-Module. However, this is currently listed as an optional SFR in the Base-PP. For a TOE that claims this PP-Module, this SFR is moved to selection-based because certificate enrollment can be performed either through PKCS#10 (covered by this SFR) or through Enrollment over Secure Transport (EST) (covered by the selection-based SFR FIA_ESTC_EXT.1 in this PP-Module). The ST author claims this SFR if "PKCS#10" is selected in FIA_ENR_EXT.1.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

- *Ability to administer the TOE locally and remotely,*
- *Ability to configure the access banner,*

- *Ability to update the TOE, and to verify the updates using [selection: digital signature, hash comparison] capability prior to installing those updates,*
- *Ability to configure the authentication failure parameters for FIA_AFL.1,*
- ***Ability to manage user accounts,***
- ***Ability to manage remote audit mechanism,***
- ***Ability to perform on-demand integrity tests,***
- ***Ability to_import and remove X.509v3 certificates into/from the Trust Anchor Database,***
- ***Ability to configure identifying information for the TOE's embedded CA,***
- ***Ability to configure a maximum certificate validity duration,***
- ***Ability to manage inspection policy,***
- ***Ability to configure inspection processing [assignment: details beyond those covered by "inspection policy"],***
- [*selection:*
  - *Ability to start and stop services,*
  - *Ability to configure* ***local*** *audit behavior,*
  - *Ability to modify the behavior of the transmission of audit data to an external IT entity, the handling of audit data, the audit functionality when Local Audit Storage Space is full,*
  - *Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1,*
  - *Ability to manage the cryptographic keys;*
  - *Ability to configure the cryptographic functionality,*
  - *Ability to configure thresholds for SSH rekeying,*
  - *Ability to configure the lifetime for IPsec SAs,*
  - *Ability to configure the interaction between TOE components,*
  - *Ability to enable or disable automatic checking for updates or automatic updates,*
  - *Ability to re-enable an Administrator account,*
  - *Ability to set the time which is used for time-stamps,*
  - *Ability to configure NTP,*
  - *Ability to configure the reference identifier for the peer,*
  - *Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors,*
  - *Ability to import X.509v3 certificates to the TOE's trust store,*
  - ***Ability to configure and manage certificate profiles,***
  - ***Ability to revoke issued certificates,***
  - ***Ability to configure certificate status services,***
  - ***Ability to configure automated process used to approve the revocation of a certificate or information about the revocation of a certificate,***
  - ***Ability to clear a cache of valid issued certificates,***
  - ***Ability to configure rules for automated issuance of certificates,***

- ***Ability to modify the CRL configuration,***
- ***Ability to modify the OCSP configuration,***
- ***Ability to import private keys,***
- ***Ability to configure the TOE's behavior on validating certificates whose revocation status cannot be determined,***
- ***Ability to configure the TOE's behavior when non-supported critical extensions occur in a requested server certificate,***
- ***Ability to generate and export PKCS#10 messages,***
- ***Ability to generate and export EST messages and accept and process EST responses,***
- ***Ability to configure TLS error responses for monitored clients,***
- ***Ability to configure notification and consent message for monitored clients,***
- ***Ability to configure rules for displaying a notification and consent message for acknowledgement prior to TLS inspection processing.***
- ***Ability to search the certificate repository,***
- *No other capabilities]*

].

Application Note: *This PP-Module defines additional management functions that are required or optional for the TOE. The Base-PP SFR has been refined to include these functions as mandatory or selection-based.*

FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles: [

- *Security Administrator, [selection:*
- ***Auditor,***
- ***CA Operations Staff,***
- ***Account Manager,***
- ***No other roles****]*].

Application Note: *As is the case in the Base-PP, the TOE does not need its roles to have the same names as those defined in this SFR. It is expected that the Security Target will define the administrative roles and privileges defined by the TSF and map them to the roles listed in this* PP-Module.

If "ability to manage local audit storage behavior" is selected in FMT_SMF.1, the 'Auditor' role must be selected here; role separation is required for audit storage functionality.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions [

- *All roles shall be able to administer the TOE locally,*
- *All roles shall be able to administer the TOE remotely,*
- ***[selection:***

- ***No identity is authorized to assume both an Account Manager role and any of the other roles in FMT_SMR.2.1,***
- ***No identity is authorized to assume both an Auditor role and any of the other roles in FMT_SMR.2.1,***
- ***No other conditions]***]

are satisfied.

Application Note: *This PP-Module refines the SFR defined in the Base-PP to include additional administrative roles. As defined in FMT_MOF.1, the TSF is expected to provide different privileges to the given roles.*

If the TSF supports an Auditor and/or Account Manager role, it is expected that the relevant selections above will be made. It is the intent of this PP-Module that if either or both of these roles are provided, their critical functionality is isolated from any other roles (see FMT_MOF.1).

5.2 TOE Security Functional Requirements

The following requirements specify the STIP functionality to be met by the TOE in addition to the requirements specified in the Base-PP.

5.2.1 Security Audit (FAU)

FAU_GCR_EXT.1 Generation of Certificate Repository

FAU_GCR_EXT.1.1 The TSF shall [*selection: store, invoke the Operational Environment to store*] certificates issued by the TSF.

Application Note: *While there is a requirement that a certificate repository exists and the TOE stores all certificates it generates in that repository, the repository can physically be within the TOE or in the OE. If the repository is provided by the TOE, then the first item in the first selection is chosen. If the storage is provided by the OE, then the second item in the first selection is chosen. It should be noted that the physical implementation of the certificate repository is left to the vendor; for instance, it can be a standalone store, or incorporated within the audit trail.*

FAU_STG.4 Prevention of Audit Data Loss

FAU_STG.4.1 The TSF shall [*prevent audited events, except those taken by the* ***[assignment: Security Administrator, Auditor]***] and [*assignment: other actions to be taken in case of audit storage failure*] if the audit trail **cannot be written to**.

Application Note: *This requirement applies to the TOE regardless of whether the audit trail is stored within the TOE boundary or on an external system in the Operational Environment. If the audit trail is stored locally, then the requirement applies when the audit trail cannot be written to when it is full. If the audit trail (in whole or in part) is stored on a system external to the TOE, then the requirement applies when the connection between the TOE and the external audit server becomes* *disconnected and the audit trail cannot be written to. In the case where the audit trail is external to the TOE and cannot be written to because it is full (and the TOE has some way of detecting that), then the requirement applies in that case as well. In all cases, the ST author is expected to describe (in the TSS) how the TSF is made aware of any such failures and how it behaves in response.*

5.2.2 Cryptographic Support (FCS)

FCS_COP.1/STIP Cryptographic Operation (Data Encryption/Decryption in Support of STIP)

FCS_COP.1.1/STIP The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithms [*AES in CCM and CCM-8 mode and [selection: TDES used in CBC mode with 3 distinct keys in its key set, no other algorithms]*] and cryptographic key sizes **[*selection: 128 bits, 192 bits, 256 bits*]** that meet the following: [*AES as specified in ISO 18033-3, CCM and CCM-8 as specified in NIST SP 800-38C and [selection: TDES as specified in NIST SP 800-67 Rev 2, CBC mode as specified in NIST SP 800-38A addendum, no others]*].

Application Note: *This requirement, in conjunction with FCS_COP.1/DataEncryption from the Base-PP, is used to support FCS_TTTC_EXT.1 and FCS_TTTS_EXT.1. Note that FCS_TTTC_EXT.1 and FCS_TTTS_EXT.1 may necessitate certain selections.*

FCS_STG_EXT.1 Cryptographic Key Storage

FCS_STG_EXT.1.1 Persistent private and secret keys shall be stored within the TSF using [*assignment: method of hardware-protected storage*].

Application Note: *This requirement ensures that persistent secret keys and private keys are stored securely when not in use. Methods of hardware protected storage can be direct or via encryption with a KEK which is protected by hardware.*

The application notes for FPT_KST_EXT.2.1 contain further discussion of private and secret keys referenced by this SFR.

FCS_TTTC_EXT.1 Thru-Traffic TLS Inspection Client Protocol

Support for through-traffic processing defined in this module requires that the TSF support the TLS client protocol using an implementation that provides the functionality negotiated by any server requested by a monitored client that is to be inspected. This functionality may not be appropriate to support communications with the TOE for other SFRs in the Base-PP. This SFR describes the TLS connection established to support STIP functionality between the TOE and the requested server, such that the TOE is operating as the TLS client. Because it may be necessary to support “legacy” TLS versions and cipher suites for mission reasons, the SFR requires support for current and legacy TLS versions as well as current and legacy cipher suites.

FCS_TTTC_EXT.1.1 The TSF shall implement [*TLS 1.2 (RFC 5246), TLS 1.0 (RFC 2246), and [selection: TLS 1.1 (RFC 4346), no other TLS versions]*] as a client to the requested server that supports the following cipher suites: [

- *TLS_ECDHE_ECDSA_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_RSA_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_RSA_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_DHE_RSA_AES_256_GCM_SHA384 as defined in RFC 5288*
- *TLS_DHE_RSA_AES_256_CBC_SHA256 as defined in RFC 5246*
- *TLS_RSA_AES_256_GCM_SHA384 as defined in RFC 5288*
- *TLS_RSA_AES_256_CBC_SHA256 as defined in RFC 5246*
- *TLS_ECDH_ECDSA_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_ECDH_ECDSA_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_DHE_RSA_AES_256_CCM as defined in RFC 6655*
- *TLS_RSA_AES_256_CCM as defined in RFC 6655*
- *TLS_ECDHE_ECDSA_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_RSA_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_RSA_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_DHE_RSA_AES_128_CCM as defined in RFC 6655*
- *TLS_DHE_RSA_AES_128_GCM_SHA256 as defined in RFC 5288*
- *TLS_DHE_RSA_AES_128_CBC_SHA256 as defined in RFC 5246*
- *TLS_ECDH_ECDSA_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDH_ECDSA_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_ECDH_RSA_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_RSA_AES_128_CCM as defined in RFC 6655*
- *TLS_RSA_AES_128_GCM_SHA256 as defined in RFC 5288*
- *TLS_RSA_AES_128_CBC_SHA256 as defined in RFC 5246*
- *TLS_ECDHE_ECDSA_AES_256_CBC_SHA as defined in RFC 4492*
- *TLS_ECDHE_RSA_AES_256_CBC_SHA as defined in RFC 4492*
- *TLS_DHE_RSA_AES_256_CBC_SHA as defined in RFC 3268*
- *TLS_ECDH_ECDSA_AES_256_CBC_SHA as defined in RFC 8422*
- *TLS_RSA_AES_256_CBC_SHA as defined in RFC 5246*
- *TLS_ECDHE_ECDSA_AES_128_CBC_SHA as defined in RFC 4492*
- *TLS_ECDHE_RSA_AES_128_CBC_SHA as defined in RFC 4492*
- *TLS_ECDH_ECDSA_AES_128_CBC_SHA as defined in RFC 8422*
- *TLS_DHE_RSA_AES_128_CBC_SHA as defined in RFC 5246*
- *TLS_RSA_AES_128_CBC_SHA as defined in RFC 5426*
- *TLS_RSA_AES_128_CCM_8 as defined in RFC 6655*
- *TLS_DHE_RSA_AES_128_CCM_8 as defined in RFC 6655*
- *TLS_DHE_RSA_AES_256_CCM_8 as defined in RFC 6655*
- *TLS_RSA_AES_256_CCM_8 as defined in RFC 6655*
- *[selection: [assignment: other ciphersuites supported],*
  TLS_ECDHE_3DES_EDE_CBC_SHA as defined in RFC 5246,
  TLS_DHE_3DES_EDE_CBC_SHA as defined in RFC 5246,

TLS_RSA_3DES_EDE_CBC_SHA as defined in RFC 5246, no other cipher suites]]

and also supports functionality for [*selection:*

- *mutual authentication,*
- *session renegotiation,*
- *none*

].

Application Note: *TLS version 1.2 and 1.0 must be supported; support for TLS version 1.1 is optional, and should be chosen if the STIP supports it. The list of cipher suites to support is mandatory but includes some selections in order to support legacy servers that may be required by the monitored clients; additional cipher suites can be included in the assignment. The order of the cipher suites above should be maintained in the ST; FCS_TTTC_EXT.1.4 indicates that the cipher suites are presented in order of preference in the Client Hello sent to the requested server, and that preference is defined as the order in the above SFR.*

The above list (as instantiated in the ST) limits the cipher suites that may be proposed by the TOE to the requested server. Behavior if the requested server responds with a cipher suite that is not in the list is defined in FDP_TEP_EXT.1.8.

The selection should indicate if mutual authentication and/or session renegotiation is supported. These selections must be the same for both FCS_TTTC_EXT.1.1 and FCS_TTTS_EXT.1.1. If mutual authentication is selected, the requirements in Section B.4 will be included by the ST authors. For this technology, mutual authentication is not desirable on these connections because the STIP will have to issue a certificate representing the client to the requested server, and the server will have to have a trust anchor for that certificate. If session renegotiation is selection, FCS_TTTC_EXT.4 from Section B.5 will be included by the ST authors.

The data encryption and decryption algorithms used in this element are performed in accordance with FCS_COP.1/STIP.

FCS_TTTC_EXT.1.2 The TSF shall verify that the presented identifier matches the reference identifier of the server requested by the monitored client using methods described in RFC 6125 section 6 for DNS name types, and via exact, byte-by-byte matching for IP address name types.

Application Note: *The rules for verification of identity are described in Section 6 of RFC 6125. The monitored client may specify the server name in the SNI extension of the Client Hello, or via some other method (e.g., DNS lookup) supported by the TSF. The method for determining that the identity presented matches that expected by the client should be fully described in the ST.*

Additionally, support for use of IP addresses in the Subject Name or Subject Alternative Name of TLS server certificates is discouraged as against best practices but may be implemented by requested servers. When no DNS name type reference ID is available from the monitored client and the certificate presented by the *requested server includes an IP address name type, exact byte-by-byte matching of the IP address to an IP address reference ID is required. If the certificate does not contain an identifier of type IP address, and no other name type is included as a reference Identifier, the IP address from the underlying transport layer protocol between the TSF and the requested servers should match the IP address reference identifier.*

FCS_TTTC_EXT.1.3 The TSF shall validate the certificate presented by the server and terminate the connection if the certificate is invalid, except as allowed by FIA_X509_EXT.2.2.

Application Note: *Validity is determined by the identifier verification, certificate path, the expiration date, processing of critical extensions, and the revocation status in accordance with RFC 5280. Certificate validity is specified by and tested in accordance with FIA_X509_EXT.1/STIP. The result of the checks will be one of 1) the certificate is valid; 2) the certificate is invalid; 3) the validity of the certificate is indeterminate because a connection cannot be established to check the revocation status of the certificate (but all other validity checks have passed). FCS_X509_EXT.2.2 (in conjunction with FDP_TEP_EXT.1.5) indicates what the TSF is supposed to do if a connection cannot be established to check the revocation status for this connection (the TOE to a requested server).*

FCS_TTTC_EXT.1.4 The TSF shall formulate the Client Hello such that it presents the highest version of the TLS protocol supported by the proxy function in the version field, and presents the list of cipher suites in descending order of preference associated with requested server.

Application Note: *This applies to the initial Client Hello sent to the requested server. This may result in a connection being established for an inspect operation, or may not lead to a connection if a bypass or block operation is determined. It should be noted that this transaction may be made even though the result will eventually be block or bypass, because the rule (see FDP_TEP_EXT.1) may require the verified identity of the server, so this connection would be required so that the server certificate could be obtained and verified.*

FCS_TTTC_EXT.5 Thru-Traffic TLS Inspection Client Support for Supported Groups Extension

FCS_TTTC_EXT.5.1 The TSF shall present the Supported Groups Extension in the Client Hello with the supported groups

[*selection:*

- ***secp256r1,***
- ***secp384r1,***
- ***secp521r1,***
- ***[assignment: other supported curves],***
- ***ffdhe2048(256),***
- ***ffdhe3072(257),***
- ***ffdhe4096(258),***
- ***ffdhe6144(259),***

- ***ffdhe8192(260)***].

Application Note: *Since support for all of the cipher suites listed in FCS_TTTC_EXT.1.1 is required, at least one of the curves and one of the finite field groups must be chosen by the ST author as appropriate for the cipher suites and the implementation.*

If additional elliptic curves are supported, ST author should describe the elliptic curve parameters for each supported elliptic curve in the assignment in accordance with RFC 7919. No additional Diffie-Hellman groups should be claimed in the assignment.

The Supported Groups Extension was previously referred to as the Supported Elliptic Curves Extension and is described in RFC 7919.

Since a requested server session might not adhere to RFC 7919 processing rules, the TOE should accept additional DH groups that might be presented in the requested server's key exchange message.

FCS_TTTS_EXT.1 Thru-Traffic TLS Inspection Server Protocol

Support for through-traffic processing defined in this module requires that the TSF support the TLS server protocol using an implementation that provides functionality expected for the set of monitored clients being protected by the TOE. In general, the functionality may not be appropriate to support communications with the TOE for other SFR in the Base-PP. This SFR describes the TLS connection established to support STIP functionality between the monitored client and the TOE, such that the TOE is operating as the TLS client. Because it may be necessary to support "legacy" TLS versions and cipher suites for mission reasons, the SFR requires support for current and legacy TLS versions as well as current and legacy cipher suites.

FCS_TTTS_EXT.1.1 The TSF shall implement [*TLS 1.2 (RFC 5246), TLS 1.0 (RFC 2246), and [selection: TLS 1.1 (RFC 4346), no other TLS versions]*] as a server to the monitored client that supports the following cipher suites: [

- *TLS_ECDHE_ECDSA_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_RSA_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_RSA_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_DHE_RSA_AES_256_GCM_SHA384 as defined in RFC 5288*
- *TLS_DHE_RSA_AES_256_CBC_SHA256 as defined in RFC 5246*
- *TLS_RSA_AES_256_GCM_SHA384 as defined in RFC 5288*
- *TLS_RSA_AES_256_CBC_SHA256 as defined in RFC 5246*
- *TLS_ECDH_ECDSA_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_ECDH_ECDSA_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_DHE_RSA_AES_256_CCM as defined in RFC 6655*
- *TLS_RSA_AES_256_CCM as defined in RFC 6655*
- *TLS_ECDHE_ECDSA_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_RSA_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_RSA_AES_128_CBC_SHA256 as defined in RFC 5289*

- *TLS_DHE_RSA_AES_128_CCM as defined in RFC 6655*
- *TLS_DHE_RSA_AES_128_GCM_SHA256 as defined in RFC 5288*
- *TLS_DHE_RSA_AES_128_CBC_SHA256 as defined in RFC 5246*
- *TLS_ECDH_ECDSA_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDH_ECDSA_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_ECDH_RSA_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_RSA_AES_128_CCM as defined in RFC 6655*
- *TLS_RSA_AES_128_GCM_SHA256 as defined in RFC 5288*
- *TLS_RSA_AES_128_CBC_SHA256 as defined in RFC 5246*
- *TLS_ECDHE_ECDSA_AES_256_CBC_SHA as defined in RFC 4492*
- *TLS_ECDHE_RSA_AES_256_CBC_SHA as defined in RFC 4492*
- *TLS_DHE_RSA_AES_256_CBC_SHA as defined in RFC 3268*
- *TLS_ECDH_ECDSA_AES_256_CBC_SHA as defined in RFC 8422*
- *TLS_RSA_AES_256_CBC_SHA as defined in RFC 5246*
- *TLS_ECDHE_ECDSA_AES_128_CBC_SHA as defined in RFC 4492*
- *TLS_ECDHE_RSA_AES_128_CBC_SHA as defined in RFC 4492*
- *TLS_ECDH_ECDSA_AES_128_CBC_SHA as defined in RFC 8422*
- *TLS_DHE_RSA_AES_128_CBC_SHA as defined in RFC 5246*
- *TLS_RSA_AES_128_CBC_SHA as defined in RFC 5426*
- *TLS_RSA_AES_128_CCM_8 as defined in RFC 6655*
- *TLS_DHE_RSA_AES_128_CCM_8 as defined in RFC 6655*
- *TLS_DHE_RSA_AES_256_CCM_8 as defined in RFC 6655*
- *TLS_RSA_AES_256_CCM_8 as defined in RFC 6655*
- *[selection: [assignment: other cipher suites supported], TLS_ECDHE_3DES_EDE_CBC_SHA as defined in RFC 5246, TLS_DHE_3DES_EDE_CBC_SHA as defined in RFC 5246, TLS_RSA_3DES_EDE_CBC_SHA as defined in RFC 5246, no other cipher suites]*]

and no other cipher suites, and also supports functionality for [*selection:*

- *mutual authentication,*
- *session renegotiation,*
- *none*

].

Application Note: *TLS version 1.2 and 1.0 must be supported; support for TLS version 1.1 is optional, and should be chosen if the STIP supports it. The list of cipher suites to support is mandatory but includes some selections in order to support legacy clients that may be required by the organization; additional cipher suites can be included in the assignment.*

The above list (as instantiated in the ST) limits the cipher suites that may be specified by the TOE when responding to the monitored client.

The selection should indicate if mutual authentication and/or session renegotiation is supported. These selections must be the same for both FCS_TTTC_EXT.1.1 and FCS_TTTS_EXT.1.1. If mutual authentication is selected, the requirements in Section B.4 will be included by the ST authors. For this technology, mutual authentication is not desirable on these connections because the STIP will have to issue a certificate representing the client to the requested server, and the server will have to have a trust anchor for that certificate. If session renegotiation is selection, FCS_TTTS_EXT.4 in section B.5 will be included by the ST authors.

The data encryption and decryption algorithms used in this element are performed in accordance with FCS_COP.1/STIP.

FCS_TTTS_EXT.1.2 The TSF shall deny connections from clients requesting [*SSL 2.0, SSL 3.0, and [selection: TLS 1.1, none]*] for through-traffic processing.

Application Note: *All SSL versions are denied regardless of exception specifications. Any TLS versions not selected in FCS_TTTS_EXT.1.1 should be selected here. (If "none" is the selection for this element then the ST author may omit the words "and none".)*

FCS_TTTS_EXT.1.3 The TSF shall perform key establishment for TLS with a monitored client using [

- *RSA with key size 2048, [selection: 1024 bits, 1536 bits, 3072 bits, 4096 bits, no other size];*
- *[selection:*
  - *Diffie-Hellman parameters of size 2048, [selection: 1024 bits, 1536 bits, 3072 bits, 4096 bits, 8192 bits, no other size]];*
  - *Diffie-Hellman groups ffdhe2048, [selection: ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, no other groups]*

  ];
- *EC Diffie-Hellman parameters using elliptic curves [selection: secp256r1, secp384r1, secp521r1, [assignment: other curves]] and no other curves*].

Application Note: *The selections in this element should indicate all key establishment sizes and/or groups supported.*

5.2.3 User Data Protection (FDP)

FDP_CER_EXT.1 Certificate Profiles for Server Certificates

FDP_CER_EXT.1.1 The TSF shall implement a certificate profile function for TLS server certificates issued by a CA embedded within the TOE, and shall ensure that issued certificates are consistent with configured profiles.

FDP_CER_EXT.1.2 The TSF shall generate certificates using profiles that comply with requirements for certificates as specified in IETF RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" as refined below. At a minimum, the TSF shall ensure that:

a) The version field shall contain the integer 2.

b) The issuerUniqueID or subjectUniqueID fields are not populated.

c) The serialNumber shall be unique with respect to the issuing Certification Authority.

d) The validity field shall specify a notBefore value that does not precede the current time and a notAfter value that does not precede the value specified in notBefore.

e) The issuer field is not empty and is populated with the **[*selection: Security Administrator, CA Operations Staff*]**-configured CA name.

f) The signature field and the algorithm in the subjectPublicKeyInfo field shall contain the OID for a signature algorithm specified in FCS_COP.1**/SigGen in the NDcPP**.

g) The following extensions are supported:
   a. authorityKeyIdentifier
   b. keyUsage
   c. extendedKeyUsage
   d. certificatePolicy
   e. [*selection: subjectKeyIdentifier, basicConstraints, cRLDistributionPoints, authorityInfoAccess, no other extensions*]

h) A subject field containing a null Name (e.g., a sequence of zero relative distinguished names) is accompanied by a populated critical subjectAltName extension.

i) The authorityKeyIdentifier extension in any certificate issued by the TOE must be populated and must be the same as the subjectKeyIdentifier extension contained in the TOE's embedded CA's signing certificate.

j) Populated keyUsage and extendedKeyUsage fields in the same certificate shall contain consistent values reflecting exclusive TLS server use as follows:

keyUsage	**extendedKeyUsage**
digitalSignature	serverAuth
digital Signature, keyEncipherment	serverAuth
digital Signature, keyAgreement	serverAuth

k) [*selection: The subjectKeyIdentifier extension is populated with a value unique for each public key contained in a certificate issued by the TSF, no other constraints*].

Application Note: *RFC updates to RFC 5280 are included in this requirement.*

The inclusion of the cRLDistributionPoints and authorityInfoAccess extensions depend on the selections made in FDP_CSI_EXT.1.3.

Uniqueness for the subject key identifier (item k above) is specific to the instance of the embedded CA. The same configured CA should not issue certificates with different public keys having the same subject key identifier.

If subjectKeyIdentifier is chosen in the selection in item g, then the ST author selects the first selection in item k; otherwise, select "no other constraints."

FDP_CER_EXT.1.3 The TSF shall implement the following rules for populating certificate fields based on constraints imposed by the TOE's embedded CA's signing certificate:

- The validity field shall specify a notAfter time that does not exceed the notAfter time of the CA's signing certificate.
- The issuer field identifies the [*selection: subject, [assignment:* ***[selection: Security Administrator, CA Operations Staff]*** *assigned identifying information]*] of the CA's signing certificate.
- [*selection:*
    - *The subject name is limited by name constraints specified in the CA's signing certificate,*
    - *[assignment: list of rules],*
    - *no other rules*].

FDP_CER_EXT.1.4 The TSF shall implement the following rules for populating certificate fields based on the validated certificate and constraints imposed by the **[*selection: Security Administrator, CA Operations Staff*]**:

a) The Subject/Subject Alternative Name shall be copied from validated server certificate.

b) The notBefore field shall not precede the notBefore field of the validated server certificate.

c) The notAfter field shall not exceed the notAfter field of the validated server certificate.

d) The notAfter field shall not exceed the current time by more than a maximum validity duration value as configured by a **[*selection: Security Administrator, CA Operations Staff*]** user.

e) If the basicConstraints field is configured to be present, it shall be populated with the value cA=False.

f) The subject public key shall be generated in accordance with FCS_CKM.1.1 **in the NDcPP**.

g) [*selection:*

- *policy OID/policy mapping fields are populated in accordance with [assignment: a* ***[selection: Security Administrator, CA Operations Staff]*** *configured mapping from validated server certificate values to one or more stated policy OIDs]*
- *[assignment: list of rules]*
- *no additional rules*].

Application Note: *It is preferred that a new public key be generated each time a certificate is generated.*

FDP_CER_EXT.2 Certificate Request Matching of Server Certificates

FDP_CER_EXT.2.1 The TSF shall establish and record a linkage from validated certificates to issued certificates.

Application Note: *This requirement ensures that the TOE provides linkage between TLS server certificates validated during a TLS session establishment by the TOE and resulting certificates issued by the TOE to represent the requested server (or monitored client if supported). In terms of Certification authority operations, an automatically approved certificate request is implied by the validated certificate and the configured TLS session establishment policy identified in FDP_TEP_EXT.1*

FDP_CER_EXT.3 Certificate Issuance Rules for Server Certificates

FDP_CER_EXT.3.1 The TSF shall issue certificates in response to a validated server certificate according to the following rules: The issued certificate is in compliance with a current certificate profile defined in accordance with FDP_CER_EXT.1 and

- The TLS session establishment policy is configured to allow inspection of TLS sessions between monitored clients and a requested server authenticated to the TSF by the validated certificate,

[*selection:*

- *A valid certificate for the same subject is not present in cache,*
- *The embedded CA certificate's name space allows issuance of a certificate that represents the authenticated server*].

FDP_CER_EXT.3.2 The TSF shall reject all certificate requests originating external to the TOE.

FDP_CSIR_EXT.1 Certificate Status Information Required

FDP_CSIR_EXT.1.1 The TSF shall [*selection: generate certificate status information, only issue certificates with validity period of less than [24 hours]*].

Application Note: *Based on the selection, the ST author must choose the appropriate requirements from Appendix B.1 of this PP-Module.*

The ST should specify whether certificate status information is generated. If the TSF can be configured so the validity of issued certificates is longer than 24 hours, certificate status information must be able to be generated.

Certificate policies associated with the issuance of TLS server certificates imply that certificates issued by the TSF must be revoked within a certain time period of discovering they do not properly represent the asserted subject. Certificate status information is not required if the validity period of any issued certificate is less than the time in which this status information must be provided. Even for emergency revocations, this time period is typically greater than 24 hours.

FDP_PPP_EXT.1 Plaintext Processing Policy

FDP_PPP_EXT.1.1 The TSF shall enforce the TLS plaintext processing policy on information flows containing plaintext produced by inspection processing of the TOE between TLS session termination points and [*selection: distinct internal inspection processing* *functional components, internal inspection processing functional components and an interface to external inspection processing environment*].

Application Note: *This element identifies the policy (TLS plaintext processing) that is applied to decrypted TLS session data received by the TSF via an external interface for which the TLS session establishment policy, FDP_TEP_EXT.1, determines inspection processing is authorized, resulting in the exposure of the underlying plaintext associated to the TLS session. Information flows containing such data are referred to as TLS session threads.*

Every network packet decrypted under the TLS session establishment policy inspection operation is associated to a TLS session thread and has the ruleset that expresses this policy applied between each distinct inspection processing functional component, including the points where TLS encryption/decryption occurs. This PP-Module allows both internal and external inspection processing functional components. Internal inspection processing components, if supported, range from simple routing functions that determine whether to abort inspection processing of a TLS session thread based on an identifier, to complicated intrusion detection/prevention functions. External inspection processing components, if supported, are accessed via a controlled interface of the TOE to a protected computing environment, considered as part of the operational environment.

FDP_PPP_EXT.1.2 The TSF shall allow the definition of TLS plaintext processing policy rules using [*assignment: entity attributes of the requested server*], [*assignment: indicators of inspection processing results*] and distinct interfaces.

Application Note: *This element identifies the various attributes that are applicable when constructing rules to be enforced by this requirement. The attributes to be included in this requirement include those which are exposed only for TLS sessions undergoing inspection processing in accordance with FDP_TEP_EXT.1 after the TLS application payload is decrypted, or can simply be the thread indicator to implicitly include attributes obtained by the TLS session establishment policy. Indicators can include specific error alerts from an internal inspection processing functional component, or can be a timeout resulting from an inspection processing functional component blocking traffic requiring no explicit signaling.*

FDP_PPP_EXT.1.3 The TSF shall allow the following operations to be associated with the plaintext processing policy: permit, block, and [*selection: bypass, no other operation*], with the capability to log the operation.

Application Note: *This element defines the operations that can be associated with rules used to manage inspection processing of TLS session threads. Permit allows the information flow to continue between inspection processing functional components; bypass indicates that the information flow is not processed by the processing component, but is forwarded to either the TLS encryption/decryption buffer, or the next plaintext inspection functional processing component; block drops subsequent information flows associated to the TLS session thread and* *informs the TLS session establishment policy to transition the TLS session to a Block Operation for subsequent TLS messages to or from the monitored client or requested server. It is permissible to use timeouts as indicators between inspection processing functional components or between the TLS plaintext processing policy and the TLS session establishment policy.*

Note this requirement does not specify the behavior of the inspection processing functional components, as this functionality is out of scope of this PP-Module. It only specifies the policy controlling the TOEs response to indicators from those processing components or to take advantage of the requested server's subject attributes exposed by decryption.

FDP_PPP_EXT.1.4 The TSF shall allow the Plaintext Processing Policy to be applied at each information flow control point between inspection processing functional components, including any network interface used to support external inspection processing.

Application Note: *This element indicates where the TLS plaintext processing policy can be assigned. A conforming TOE must be able to assign processing rules to prevent TLS data from being exposed to unauthorized processing units based on the requested server attributes, and to allow TLS sessions containing malicious or unauthorized data, as determined by the inspection processing functional components, to be blocked at the earliest possible point, avoiding compromise of the TOE or the monitored client.*

FDP_PPP_EXT.1.5 The TSF shall

- drop Information flows between inspection processing components, including any interface to external inspection processing components, that cannot be associated to an existing TLS session thread.
- inform the TLS session establishment policy of the TLS session thread associated to any information flow that is blocked by the plaintext processing policy.

Application Note: *This element identifies state information shared by the TLS inspection processing policy and the TLS session establishment policy associated.*

The TSF may inform the TLS session establishment policy that it has blocked a data flow either explicitly, by sharing state information, signaling, or other mechanism, or implicitly via the use of time-out mechanisms.

FDP_PRC_EXT.1 Plaintext Routing Control

FDP_PRC_EXT.1.1 The TSF shall control the routing of information flows containing plaintext within a TLS session thread in accordance with the configured Plaintext Processing Policy identified in FDP_PPP_EXT.1.

FDP_PRC_EXT.1.2 The TSF shall separate information flows containing plaintext within different TLS session threads.

FDP_PRC_EXT.1.3 The TSF shall not expose plaintext within a TLS session thread except to inspection processing functional components identified in, and as authorized by the configured Plaintext Processing Policy, as described in FDP_PPP_EXT.1.

FDP_RIP.1 Subset Residual Information Protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [*selection: allocation of the resource to, deallocation of the resource from*] the following objects: [*assignment: list of objects*].

Application Note: *"Resources" in the context of this requirement are any data buffers used to implement STIP functions, including the TLS buffers containing decrypted TLS payloads. The concern is that a buffer or memory area might be reused in subsequent function or communication channel resulting in inappropriate disclosure of sensitive data. "Objects" refers to any sensitive data objects that are under control of the TSF.*

FDP_STG_EXT.1 Certificate Data Storage

FDP_STG_EXT.1.1 The TSF shall use [*selection: access controlled storage, an integrity mechanism*] to protect the trusted public keys and certificates (trust store elements) used to validate local logon, trusted channel, and external communication to the STIP.

Application Note: *If "an integrity mechanism" is selected, FCS_CKM_EXT.5 should be included in the ST.*

FDP_STIP_EXT.1 SSL/TLS Inspection Proxy Functions

FDP_STIP_EXT.1.1 The TSF shall be capable of performing the Inspection Operation consisting of establishing a TLS session between TOE and the requested server according to FCS_TTTC_EXT.1, establishing a TLS session between the monitored client and the TOE according to FCS_TTTS_EXT.1, and routing decrypted application data from either of these TLS sessions to or between inspection processing functional components within the TOE, or between the TOE and external inspection processing functional components to a unique TLS session thread, according to FDP_PPP_EXT.1 and FDP_PRC_EXT.1.

Application Note: *This defines the inspection operation, where the TLS connection is terminated at both ends on the TOE and the opportunity for inspection of the contents is allowed.*

FDP_STIP_EXT.1.2 The TSF shall obtain a certificate from the TOE CA that represents the requested server for establishment of the TLS session with the monitored client when performing an inspect operation.

Application Note: *Certificates are generated by the TOE's embedded CA function, or obtained from an optional certificate cache maintained by the TOE. Certificate caching is not required, however, in the case where certificate caching is supported, the TSF will still need to perform certificate generation if no corresponding cache entry can be found for the requested server that matches the current certificate profile.*

FDP_STIP_EXT.1.3 The TSF shall [*selection*:

- *require administrator confirmation of consent,*
- *provide a consent to monitor banner to the client, in accordance with FTA_TAB.1**/TLS**, and receive an affirmative response*]

prior to sending decrypted TLS application data from a monitored client to inspection processing functional component as part of an inspection operation.

Application Note: *The selection "require administrator confirmation of consent" means that there is a means for the administrator to approve the operation based on receiving consent from the monitored client(s). This would include "real-time" approval mechanisms (a pop-up, for instance, accessible to an administrator) as well as configuration settings indicating "pre-approval" (again, only accessible by the administrator) such as one-time approval at installation (prior to any decryption), or included in a logon banner for administrators. A particular mechanism is not specified as it is up to the implementation. The intent is simply to ensure consent is obtained prior to monitoring.*

FDP_STIP_EXT.1.4 The TSF shall provide the Bypass operation functionality by forwarding traffic between the monitored client and requested server such that monitored client can establish and maintain a TLS connection to the requested server.

Application Note: *This merely defines the Bypass operation, where the STIP does not inspect the traffic, and just forwards packets between the monitored client interface and the requested server interface.*

FDP_STIP_EXT.1.5 When initiating a Block operation, the TSF shall be capable of providing a [*selection: TLS error response, [assignment: other error message]*] to the monitored client associated with the blocked TLS session.

Application Note: *This requires the TOE to provide some form of notification to monitored client when the monitored client attempts to initiate a connection and that connection is blocked. This can be done through the TLS error response, or (using the "assignment" part of the selection) some other means defined by the ST author.*

FDP_TEP_EXT.1 SSL/TLS Inspection Proxy Policy

FDP_TEP_EXT.1.1 The TSF shall perform SSL/TLS Inspection Proxy functions and enforce SSL/TLS Inspection Proxy rules on TLS traffic received by the TSF from monitored clients and servers requested by monitored clients, and on TLS traffic controlled by the TSF to be sent to monitored clients and servers requested by monitored clients.

Application Note: *This element defines the policy and requires the rules (defined in other elements of this component) to be applied to TLS network traffic from monitored clients to requested servers that is processed at the TOE's network interfaces (as required in subsequent elements).*

This requirement is to be enforced even if the network interfaces are saturated/overwhelmed with network traffic.

The requirement only applies to network traffic at the external interfaces that is identified as TLS traffic between a monitored client and requested server. This does not apply, for instance, to TLS traffic associated with administration of the STIP.

FDP_TEP_EXT.1.2 The TSF shall allow the definition of SSL/TLS Inspection Proxy rules based on the following attributes of each monitored client and requested server: [

- *Network Protocol fields: [selection: IPv4, IPv6, [assignment: other internet protocol]]:*
    - o *Source address*
    - o *Destination address*
    - o *Source Port*
    - o *Destination Port*
    - o *[selection: [assignment: other fields containing identity attributes for the monitored client or requested server], no other fields]*
- *TLS Client Hello handshake message:*
    - o *Server_name extension of the requested server*
    - o *Client side interface*
- *TLS Server Certificate message:*
    - o *Issuer*
    - o *Subject*
    - o *SubjectAlternateName*
- *Distinct Interface*
- *[selection:*
    - o *TLS client certificate message [selection:*
        - ▪ *Certificate issuer*
        - ▪ *Certificate subject*
        - ▪ *Certificate subject alt name]*
    - o *[assignment: other attributes],*
    - o *no other attributes]*

].

Application Note: *This element identifies the various attributes that are applicable when constructing rules to be enforced by this requirement. The rules apply to external interfaces receiving TLS messages from a monitored client (client side interface), and to the TLS messages received by the TOE in response to the TSF initiating a*

TLS connection to a server requested by the monitored client (server side interface).

Network Protocol fields are used by the TSF to determine the IP address of the monitored client and the IP address of the requested server in traffic received on the client side interface only. Indicate which network protocols, including the internet layer and transport layer protocols that are used to determine the indicated fields that can be applicable when constructing rules for this policy.

The TLS Client Hello messages, and optional client certificate messages are received on the client side interface only. If the TSF supports client authentication, 'TLS client certificate message' should be selected (with the appropriate sub-selections supported by the TOE), and FCS_TTTS_EXT.3 in Appendix B.4, Authentication of Monitored Clients should be claimed.

The TLS certificate message is received on a server side interface prior to the TSF sending a Server Hello done message on the client side interface.

FDP_TEP_EXT.1.3 The TSF shall allow the following operations to be associated with SSL/TLS Inspection Proxy rules: block, bypass, or inspect, with the capability to log the operation.

FDP_TEP_EXT.1.4 The TSF shall be able to define monitored clients, requested servers, and [*selection: specific client-server connections, no other abstractions*] in terms of the attributes associated with the SSL/TLS Inspection Proxy function.

Application Note: *This element requires that there must be a mechanism to define a "monitored client" and "requested server" via the attributes specified in FDP_TEP_EXT.1.2. This entity will then have associated rules defined in other elements in this component related to the STIP functionality and operations. If the TOE is able to define a set of attributes that represent a unique client-server connection, then the first selection item should be chosen.*

FDP_TEP_EXT.1.5 The TSF shall be able to associate a monitored client, requested server, and [*selection: specific client-server connections, no other abstractions*] with the allowed TLS version or versions, TLS cipher suites (including TLS key exchange algorithms and key sizes), the supported groups per FCS_TTTC_EXT.5.1, and **[*selection: mutual authentication block-bypass, requested server certificate revocation status unavailable*, *critical extension in a certificate unrecognized, nothing else*]** that shall be used when performing the SSL/TLS Inspection Proxy operations.

Application Note: *This element requires a mechanism that defines, for each "monitored client" and "requested server" (and, if supported, unique client-server pairs), the allowed set of the indicated TLS characteristics associated with those entities. This association allows the enforcement of rules defined by other elements in this component.*

The first selection is chosen if the TOE supports rules based on both a monitored client and requested server pair.

The second selection indicates events specified in other requirements that need to be associated with monitored clients/requested servers in rules so that appropriate actions can be taken.

The first item is chosen if the TOE supports mutual authentication; FDP_TEP_EXT.1.7 and its application note have additional details.

The second item is chosen if FIA_X509_EXT.2 indicates a privileged user may indicate their choice on whether to accept a requested server certificate for which revocation information is not available using allowances. See also FDP_TEP_EXT.1.8.

The third item is chosen if the TOE supports detection of a critical extension in a certificate (being validated according to FIA_X509_EXT.1/STIP) that it cannot interpret. RFC 5280 indicates that this situation results in an invalid certificate, but FIA_X509_EXT.1/STIP provides an additional option that—instead of treating the certificate as invalid (and thus blocking the connection)—the administrator can indicate that the "Bypass" operation is to be applied to the connection instead (which essentially defers the decision to make the connection to the client). See also FDP_TEP_EXT.1.8.

FDP_TEP_EXT.1.6 The TSF shall allow the SSL/TLS Inspection Proxy rules to be assigned to each distinct network interface.

FDP_TEP_EXT.1.7 The TSF shall perform a [*selection: block, bypass, mutual authentication inspection*] operation on the session when receiving a TLS certificate request message from the requested server when establishing the TLS in accordance with FCS_TTTC_EXT.1.

Application Note: *A mutual authentication inspection operation is a variant of the inspection operation. If this item is selected, the mutual authentication SFR in appendix B.4 must be claimed. Inspection of mutual authenticated TLS requires both the client and server to trust the embedded CA, and therefore has limited use. It is preferred that inspection of mutual authenticated TLS be performed by components of the requested server security architecture (e.g. via a traffic filtering firewall or an attribute-based access control mechanism) and not be performed by devices described in this PP-Module. If mutual authentication inspection is selected, then the selection-based requirements in Section B.5 will be included by the ST authors, and the "mutual authentication" item will be selected in FCS_TTTC_EXT.1.1 and FCS_TTTS_EXT.1.1.*

If both block and bypass are selected, the 'mutual authentication block-bypass' exception specification must be claimed in FDP_TEP_EXT.1.5 and be configurable within the TLS session establishment policy to determine which of the supported operations will be applied for a specific requested server. It is expected, but not *required, that one of the selected operations will be a default operation and the other determined by the server matching the exception specification.*

FDP_TEP_EXT.1.8 The TSF shall

- Block the connection if the monitored client does not support a TLS version, cipher suite, key exchange, and key size that are in its allowed set as defined in FDP_TEP_EXT.1.5;
- Block the connection if the requested server does not negotiate a TLS version, cipher suite, key exchange, and key size that are in its allowed set as defined in FDP_TEP_EXT.1.5;
- Either Block, or [*selection: require administrative approval to inspect or bypass, no other rule*] the connection if the requested server does not negotiate a TLS version, cipher suite, key exchange, and key size that are in the set proposed by the monitored client in its Client Hello message;
- Block or [*selection: inspect, bypass, no other rule*] the connection if TOE certificate processing indicates revocation information is not available for a requested server or [*selection: monitored client, no other entity*];
- Block or [*selection: bypass, no other rule*] a connection if TOE certificate processing indicates an uninterpretable critical extension is present in the certificate of a requested server.

Application Note: *Support by a client for the revocation information unavailable case is determined by the TLS handshake protocol messages and fatal errors from the client received during TLS session negotiation with the TOE in accordance with FCS_TTTS_EXT.1*

In the case where a critical extension is encountered that cannot be interpreted by the TOE in accordance with FIA_X509_EXT.1.1/STIP "bypass" can be selected in the last bullet item above. Note that it is not allowed for the administrator to select "Inspect" in this case.

FDP_TEP_EXT.1.9 The TSF shall enforce the following default SSL/TLS Inspection Proxy rules on all SSL/TLS network traffic received from interfaces associated with monitored clients and requested servers:

- The TSF shall drop and be capable of [*selection: counting, logging*] invalid TLS messages;
- The TSF shall drop and be capable of logging TLS Client Hello messages for which no valid client can be determined.
- The TSF shall drop a TLS Client Hello message for which no valid server attribute can be determined.
- The TSF shall drop and be capable of [*selection: counting, logging*] TLS messages other than a Client Hello if the message is not associated with an existing TLS session thread established via the inspection operation or a TLS encrypted data flow established via a bypass operation.
- The TSF shall terminate a TLS session thread if it receives a fatal TLS error message from the monitored client.

- The TSF shall attempt to [***selection: resume the session, renegotiate the session, terminate the TLS session thread and provide a [selection: TLS error message, [assignment: send a notification] to the monitored client associated to the TLS session thread]***] if it receives a fatal TLS error message on the TLS session to the requested server.
- The TSF shall terminate a TLS session thread established via the inspect operation, and terminate a TLS encrypted data flow established by the bypass operation, if the TSF receives no traffic from the associated monitored client for a configurable period.
- The TSF shall transition a TLS session thread state from inspect operation to block operation, when indicated to do so by the TLS plaintext processing policy.

Application Note: *Dropping a message, performing a block operation, and transitioning to a block operation are different. Dropping a message is typically a silent operation; performing block operation may require messages to be sent to the monitored client associated to the TLS Client Hello; transitioning to a block operation involves termination of the TLS session thread, and potentially sending TLS alert messages to the requested server and TLS alert messages or other messages to the monitored client.*

FDP_TEP_EXT.1.10 The TSF shall block all connections for which an Inspection or Bypass operation is not defined.

Application Note: *This is the deny by default rule. Note that the block rule does not need to be explicitly defined. This element should not be interpreted that all Client Hello packets should be blocked; the intent is that the Client Hello is initiated from the monitored client, and then the TOE performs processing to determine what to do with the requested connection. If it cannot find a rule that applies for the requested connection, then this element requires that the connection be blocked.*

5.2.4 Identification and Authentication (FIA)

FIA_ENR_EXT.1 Certificate Enrollment

FIA_ENR_EXT.1.1 The TSF shall be able to generate a certificate request to an external certification authority to receive a certificate for the TOE’s embedded CA’s signing key using [*selection:*

- *PKCS#10 in accordance with FIA_X509_EXT.3,*
- *Enrollment over Secure Transport (EST) in accordance with FIA_ESTC_EXT.1*].

Application Note: *The external certification authority may be a root or intermediate certification authority that is used to issue and manage the TOE’s embedded CA’s certificate. It is not to be used to directly issue end entity certificates to requested servers instead of the TOE’s embedded CA.*

FIA_X509_EXT.1/STIP Certificate Validation (STIP)

FIA_X509_EXT.1.1/STIP The TSF shall validate certificates used for connections supporting STIP functions in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [*selection: the Online Certificate Status Protocol (OCSP) as specified in RFC 6960, a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3, Certificate Revocation List (CRL) as specified in RFC 5759 Section 5*].
- The TSF shall validate the extendedKeyUsage field according to the following rules depending on the certificate type and purpose:
  - Server certificates presented in a TLS certificate message for Thru-Traffic processing TLS shall have meet one of the following checks:
    - There is no extendedKeyUsage field,
    - The extendedKeyUsage field is present and contains the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1),
    - The extendedKeyUsage field is present and contains the ‘any’ purpose (id-…)
  - Server certificates presented for TLS not associated with the Thru-Traffic processing include an extendedKeyUsage field that contains the ServerAuthentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1),
  - Code-signing certificates include the extendedKeyUsage field that contains the CodeSigning purpose
  - Client certificates presented for TLS for any purpose shall include the extendedKeyUsage field that contains the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage 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 extendedKeyUsage field.
  - All other certificates used for any other purpose include an extendedKeyUsage field that DOES NOT contain the ‘any’ purpose.
- The TSF shall validate all extensions marked as critical and verify the value is appropriate for the functionality that uses the value.

FIA_X509_EXT.1.2/STIP 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.

Application Note: *FIA_X509_EXT.1.1/STIP lists the rules for validating certificates for STIP Functions. The text that says what to do if revocation information is not available, or if a critical extension cannot be processed, is provided in FCS_TTTC_EXT.1.3.*

The ST author selects whether revocation status is verified using OCSP or CRLs. The SFR indicates that the TOE be capable of supporting a minimum path length of three certificates. This means that the TOE supports a hierarchy comprising of at least a self-signed root CA certificate, a subordinate CA certificate, and a leaf certificate. The chain validation is expected to terminate with a trust anchor. This means the validation can terminate with any trusted CA certificate designated as a trust anchor. This CA certificate must be loaded into the trust store ('certificate store', ' trusted CA Key Store' or similar) managed by the TOE trust store. If the TOE's trust store supports loading of multiple hierarchical CA certificates or certificate chains, the TOE must clearly indicate all certificates that it considers trust anchors. The validation of X.509v3 leaf certificates comprises several steps:

a) *A Certificate Revocation Check refers to the process of determining the current revocation status of an otherwise structurally valid certificate. This must be performed every time a certificate is used for authentication. This check must be performed for each certificate in the chain up to, but not including, the trust anchor. This means that CA certificates that are not trust anchors, and leaf certificates in the chain, must be checked. It is not required to check the revocation status of any CA certificate designated a trust anchor, however if such check is performed it must be handled consistently with how other certificates are checked.*

b) *An expiration check must be performed. This check must be conducted for each certificate in the chain, up to and including the trust anchor.*

c) *The continuity of the chain must be checked, showing that the signature on each certificate that is presented to the TOE is valid and the chain terminates at the trust anchor.*

d) *The presence of relevant extensions in each certificate in the chain such as the extendedKeyUsage parameters of the leaf certificate must correspond to SFR-relevant functionality. For example, a peer acting as a web server should have TLS Web Server Authentication listed as an extendedKeyUsage parameter of its X.509v3 certificate. The TOE ensures that the relevant extensions in each certificate in the chain such as the extendedKeyUsage parameters of the leaf certificate correspond to the SFR-relevant functionality they are used with.*

It is expected that revocation checking is performed when a certificate is used in an authentication step. It is expected that revocation checking is performed on both leaf and intermediate CA certificates when a leaf certificate is presented to the TOE as part of the certificate chain during authentication. Revocation checking of any CA certificate designated a trust anchor is not required.

If the TOE implements mutual authentication or acts as a server, there is no expectation of performing any checks on TOE's own leaf certificate during authentication. FIA_X509_EXT.1.2/STIP applies to certificates that are used and processed by the TSF and restricts the certificates that may be added as trusted CA certificates.

5.2.5 Security Management (FMT)

FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [*modify the behaviour of*] the functions [*assignment: functions defined in the Management Functions and Privileges table that are claimed in FMT_SMF.1.1*] to [*assignment: roles defined in the Management Functions and Privileges table*].

Application Note: *The management functions defined in this table are the same as the management functions defined in FMT_SMF.1. The NDcPP only requires management functionality to be performed by a Security Administrator. However, the NDcPP contains several optional FMT_MOF iterations based on selections in FMT_SMF. In using this PP-Module, Table 2 (below) associated with this requirement is used, and the optional FMT_MOF.1.1 iterations from the NDcPP are not used. However, FMT_MOF.1/ManualUpdate applies as written and must be included in the ST.*

Table 3 uses the following key:

M: Mandatory (this role must perform this function)

CM: Conditionally Mandatory (if this role is part of the TSF it must perform this function but if the role itself does not exist it may be satisfied elsewhere)

C: Conditional (if a role does not exist to satisfy a conditionally mandatory function, this is that function's "backup" role)

O: Optional (this role may or may not perform this function)

The ST author should reproduce this table and update as needed to show which functions are implemented by which roles.

If a selectable function has a mandatory role mapping, this means that if the function is implemented it must be satisfied in a certain way; it does not mean that it is mandatory to implement that function.

If a selectable function does not have a mandatory role but is mapped to multiple optional roles, then at least one of them must be selected if the function is implemented.

Management Function	**Security Administrator**	**Auditor**	**Account Manager**	**CA Operations Staff**
Ability to administer the TOE locally and remotely	M	CM	CM	CM
Ability to configure the access banner	M		O	O
Ability to update the TOE, and to verify the updates	M		O	O
Ability to configure the authentication failure parameters for FIA AFL.1	M		O	O
Ability to manage user accounts	C		CM	
Ability to manage remote audit mechanism	M	CM		
Ability to perform on-demand integrity tests	O	O	O	O
Ability to import and remove X.509v3 certificates into/from the Trust Anchor Database	C			CM
Ability to configure identifying information for the TOE's embedded CA	C			CM
Ability to configure a maximum certificate validity duration	C			CM
Ability to manage inspection policy	O			O
Ability to configure inspection processing details	O			O
Selection-Based Management Functions (do not include if not claimed in FMT_SMF.1)				
Ability to start and stop services	O			O
Ability to configure local audit behavior	O	O		
Ability to modify the behavior of the transmission of audit data to an external IT entity, the handling of audit data, the audit functionality when Local Audit Storage Space is full	M	CM		
Ability to search local audit	C	CM		
Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1	M		O	
Ability to manage the cryptographic keys	M			CM
Ability to configure the cryptographic functionality	M			O
Ability to configure thresholds for SSH rekeying	M		O	O
Ability to configure the lifetime for IPsec SAs	M			
Ability to configure the interaction between TOE components	M	O		O

Management Function	Security Administrator	Auditor	Account Manager	CA Operations Staff
Ability to enable or disable automatic checking for updates or automatic updates	M			
Ability to re-enable an Administrator account	C		CM	
Ability to set the time which is used for time-stamps	M	O		O
Ability to configure NTP	M			
Ability to configure the reference identifier for the peer	M			O
Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors	M			CM
Ability to import X.509v3 certificates to the TOE's trust store	M			CM
Ability to configure and manage certificate profiles	C			CM
Ability to revoke issued certificates	C			CM
Ability to configure certificate status services	C			CM
Ability to configure automated process used to approve the revocation of a certificate or information about the revocation of a certificate	C			CM
Ability to clear a cache of valid issued certificates	M			CM
Ability to configure rules for automated issuance of certificates	C			CM
Ability to modify the CRL and/or OCSP configuration	C			CM
Ability to import private keys	C			CM
Ability to configure the TOE's behavior on validating certificates whose revocation status cannot be determined	M			CM
Ability to configure the TOE's behavior when non-supported critical extensions occur in a requested server certificate	C			CM
Ability to generate and export PKCS#10 messages	C			CM
Ability to configure EST functionality to generate and export EST requests	C			CM
Ability to configure TLS error responses for monitored clients	M			O
Ability to configure notification and consent message for monitored clients	M			O
Ability to configure rules for displaying a notification and consent message for acknowledgement prior to TLS inspection processing	M			O
Ability to search the certificate repository	C	CM		CM

Table 3 – Management Functions and Privileges

5.2.6 Protection of the TSF (FPT)

FPT_FLS.1 Failure with Preservation of Secure State

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: **DRBG failure, integrity test failure, external audit server is unavailable, [*selection: local audit storage is full, update signature verification failure, integrity failure on local audit, integrity failure on Trust Anchor database, [assignment: other potential TSF failures]*]**.

Application Note: *The intent of this requirement is to prevent the use of failed randomization and other events that can compromise the operation of the TOE. This means that the TOE must be able to attain a secure/safe state when any of the identified failures occurs. If the TOE should encounter a failure in the middle of a critical operation, the TOE should not just quit operating, leaving key material and user data unprotected.*

The failure of an Operational Environment component can be just as detrimental to security as a failure of the TSF itself. Therefore, in addition to describing the potential TSF failures and how the TOE preserves a secure state in response, the ST author is also expected to use this SFR to express how the TOE is made aware of any environmental failures and how it responds to these.

FPT_KST_EXT.1 No Plaintext Key Export

FPT_KST_EXT.1.1 The TSF shall prevent the plaintext export of [*assignment: list of all keys used by the TSF*].

Application Note: *Keys include all TOE secret and private keys which includes keys generated for issued certificates. The intent of this requirement is to prevent the keys from being exported, even by a security administrator.*

FPT_KST_EXT.2 TSF Key Protection

FPT_KST_EXT.2.1 The TSF shall prevent unauthorized use of all TSF private and secret keys.

Application Note: *The intent of this requirement is to protect TSF private and secret keys from both unauthorized users, privileged users, and unprivileged processes. Keys specific to the TOE that should be addressed in this requirement include, but are not limited to, the TOE's embedded CA's private signing key, private keys associated to certificates issued by the TOE's embedded CA and TLS session keys established to facilitate inspection of traffic. Users should not be able to access the keys through "normal" interfaces. Processes that use private or secret keys to meet the functionality described in this PP module are considered authorized; all other processes are unauthorized. When an interface allows both authorized and unauthorized access to a key (for example, certificate signing functions with access to the embedded CA's private signing key are authorized only when certificate to be signed corresponds to a valid certificate belonging to a requested,* *and is unauthorized at any other time), evidence of protection includes logging of accesses via the common interface, as indicated in Table 2 for FAU_GEN.1.*

FPT_RCV.1 Manual Trusted Recovery

FPT_RCV.1.1 After [*assignment: list of failures/service discontinuities*] the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

Application Note: *This requirement ensures that the TSF can determine that the TOE is started up without protection compromise and can recover without protection compromise after discontinuity of operations. Anticipated failures include actions that result in a system crash, media failures, or discontinuity of operations caused by erroneous administrative action or lack of erroneous administrative action. The data that needs to be restored includes the TSF keys needed for signature, the Trust Anchor Database, keys needed for management of certificates, all signed certificates, and any certificate status information.*

5.3 TOE Security Assurance Requirements

As a PP-Module of the NDcPP, this PP-Module does not define any additional assurance requirements above and beyond what is defined in the Base-PP. In general, application of the SARs to the TOE boundary described by both the NDcPP and this PP-Module is sufficient to demonstrate that the claimed SFRs have been implemented correctly by the TOE. However, in some cases it may be necessary to perform additional assurance activities in order to satisfy the SARs due to unique capabilities or limitations of the TOE that is specified by this PP-Module. Where applicable, these assurance activities are described below.

5.3.1 Class AVA: Vulnerability Assessment

Special attention to vulnerabilities related to outdated TLS versions and cipher suites required to process traffic between monitored clients and requested servers should be paid. Additionally, vulnerabilities related to the embedded CA functionality within this technology have significant consequences for both the TOE and the monitored clients the TOE is intended to protect and should be thoroughly researched.

Appendix A in the associated PP-Module Supporting Document provides a guide to the evaluator in performing vulnerability analysis and refining the activities defined by the Base-PP to address such vulnerabilities.

6 Consistency Rationale

6.1 NDcPP Base

6.1.1 Consistency of TOE Type

If this PP-Module is used to extend the NDcPP, the TOE type for the overall TOE is still a generic network device. However, one of the functions of the device must be the ability for it to act as SSL/TLS Inspection Proxy. The TOE boundary is simply extended to include that functionality.

6.1.2 Consistency of Security Problem Definition

The threats defined by this PP-Module (see section 3.1) supplement those defined in the NDcPP as follows:

PP-Module Threat	Consistency Rationale
T.UNTRUSTED_COMMUNICATION	The threat of untrusted communication can provide unauthorized access to unintended resources if using weak cryptography or use untrusted intermediate systems. This can be mitigated either by protocols defined in this PP-Module or in the Base-PP.
T.AUDIT	Auditing poses a threat if certain activities aren't logged, like the issuance of certificates. This threat can be mitigated if proper configurations are in place to prevent the compromise of audit data defined in this PP-Module or the base-PP.
T.UNAUTHORIZED_USERS	The threat of unauthorized users attempting to gain access to other users' credentials can be addressed by placing protections for logged-in users and only allow privileged user access methods defined in this PP-Module or in the Base-PP.
T.CREDENTIALS	Beyond the Base-PP, the threat of manipulation of the CA signing key can be mitigated by providing access protection to persistent keys.
T.SERVICES	The threat of misuse or manipulation of services is not yet defined in the Base-PP.
T.DEVICE_FAILURE	The failure of the certificate authority or routing traffic to inspection poses a threat not defined in the Base-PP.
T.UNAUTHORIZED_DISCLOSURE	The Base-PP does not include the threat of unauthorized disclosure to sensitive data that is only intended for the monitored client.
T.INNAPROPRIATE_ACCESS	The threat of inappropriate access to unintended servers could disclose unauthorized traffic to inspection processes which is not defined in the Base-PP.

6.1.3 Consistency of Objectives

The NDcPP does not define any TOE objectives; therefore, there is no inconsistency between it and this PP-Module. The TOE objectives defined in this PP-Module are traced to SFRs, which are analyzed for consistency with the NDcPP in the section below.

The environmental security objectives defined by this PP-Module (see section 4.2) supplement those defined in the NDcPP as follows:

PP-Module Objective	Consistency Rationale
OE.RESIDUAL_INFORMATION	This objective intends for the TOE's OE to destroy residual information like persistent secret and private keys.
OE.AUDIT	This objective intends for the TOE's OE to have adequate storage to retain the audit records of SSL/TLS inspection devices.
OE.CERT_REPOSITORY	This objective intends for the TOE's OE to provide a certificate repository.
OE.CERT_REPOSITORY_SEARCH	This objective intends for the TOE's OE which will provide a certificate repository to also have the capability to search within the repository.

6.1.4 Consistency of Requirements

This PP-Module identifies several SFRs from the NDcPP that are needed to support STIP functionality. This is considered to be consistent because the functionality provided by the NDcPP is being used for its intended purpose. The PP-Module also identifies a number of modified SFRs from the NDcPP as well as new SFRs that are used entirely to provide STIP functionality. The rationale for why this does not conflict with the claims defined by the NDcPP are as follows:

PP-Module Requirement	Consistency Rationale
Modified SFRs	
FAU_GEN.1	The ST author is instructed to add new auditable events for STIP functionality; the SFR behavior itself is otherwise unmodified.
FCS_CKM.4	The ST author is instructed to include security critical parameters and when key destruction is required.
FIA_X509_EXT.1/Rev	Other than this SFR becoming mandatory versus selection-based, there is no modification to this SFR.
FIA_X509_EXT.2	This SFR becomes mandatory versus selection-based when claiming conformance of this PP-Module. The SFR is modified to require TLS as a protocol used and leave other protocols selection-based.
FIA_X509_EXT.3	This SFR becomes mandatory versus optional when claiming conformance of this PP-Module.
FMT_SMF.1	The ST author is instructed to include additional management functions in this SFR and to specify additional management functions based on the STIP capability defined by the PP-Module.
FMT_SMR.2	The ST author is instructed to include additional roles in this SFR based on the STIP capability defined by the PP-Module.
Mandatory SFRs	
FAU_GCR_EXT.1	This SFR applies to storing certificates in a certificate repository which is not listed in the Base-PP.
FAU_STG.4	This SFR applies to the prevention of audit data loss by the inclusion of the auditor role which is not listed in the pp.
FCS_COP.1/STIP	This SFR provides encryption/decryption cipher suites used in support for the through-traffic processing of the TOE.

PP-Module Requirement	Consistency Rationale
FCS_STG_EXT.1	This SFR applies to the storage of persistent private and secret keys which is not defined in the Base-PP.
FCS_TTTC_EXT.1	This SFR applies to thru-traffic TLS inspection client protocol which is not defined in the Base-PP.
FCS_TTTC_EXT.5	This SFR applies to client supported groups extension for thru-traffic TLS inspection.
FCS_TTTS_EXT.1	This SFR applies to thru-traffic TLS inspection server protocol which is not defined in the Base-PP.
FDP_CER_EXT.1	This SFR applies to the implementation of certificate profile functionality for server certificates which is not defined in the Base-PP.
FDP_CER_EXT.2	This SFR applies to the establishing and recording a linkage from validated to issued certificates which is not defined in the Base-PP.
FDP_CER_EXT.3	This SFR applies to rules for the issuance of certificates which is not defined in the Base-PP.
FDP_CSIR_EXT.1	This SFR applies to the ability to generate certificate status information if the validity period can be configured to last longer than 24 hours.
FDP_STIP_EXT.1	This SFR applies to STIP-specific processing operations which are not defined in an RFC or specified in the Base-PP.
FDP_PPP_EXT.1	This SFR applies to the enforcement of the TLS processing policy which is not defined in the Base-PP.
FDP_PRC_EXT.1	This SFR applies to the routing of information flows containing plaintext which is not defined in the Base-PP.
FDP_TEP_EXT.1	This SFR applies to the enforcement of the TLS session establishment policy which is not defined by the Base-PP.
FDP_RIP.1	This SFR applies to providing the capability to allocation or deallocation of resources which in this PP-Module is any data buffers used to implement STIP functionality which is not defined in the Base-PP.
FDP_STG_EXT.1	This SFR enforces protection of trusted public keys and certificates implemented using access control or integrity mechanism which is not defined in the Base-PP.
FIA_ENR_EXT.1	This SFR applies to the ability to generate a certificate request which is not defined in the Base-PP.
FIA_X509_EXT.1/STIP	This SFR specifies validation of certificates used for connections supporting STIP functions.
FMT_MOF.1	This SFR applies to the restriction of management functions to certain roles which are not defined in the Base-PP which only requires management functionality to be performed by a security administrator.
FPT_FLS.1	This SFR applies to preserving a secure state when different failures occur which is not defined in the Base-PP.
FPT_KST_EXT.1	This SFR applies to the prevention of plaintext key export which is not defined in the Base-PP.

PP-Module Requirement	Consistency Rationale
FPT_KST_EXT.2	This SFR applies to the prevention of unauthorized use of private and secret keys which is not defined in the Base-PP.
FPT_RCV.1	This SFR applies to the maintenance mode that provides the ability to return to a secure state is provided which is not defined in the Base-PP.
Optional SFRs	
FAU_SAR.1	This SFR applies to who can view all the audit records which includes the added role of the auditor, which is not defined in the Base-PP.
FAU_SAR.3	This SFR applies to the ability to search within audit records based on various identifiers which is not defined in the Base-PP.
FDP_PIN_EXT.1	This SFR applies to certificate pinning which is not defined in the Base-PP.
Selection-Based SFRs	
FAU_SCR_EXT.1	This SFR applies to providing the capability to search the certificate repository which is not defined by the Base-PP.
FCS_CKM_EXT.5	This SFR applies to the protection of persistent public keys from undetected modification which is not defined in the Base-PP.
FCS_TTTC_EXT.4	This SFR applies to session renegotiation for thru-traffic TLS inspection (client-side).
FCS_TTTS_EXT.4	This SFR applies to session renegotiation for thru-traffic TLS inspection (server-side).
FDP_CRL_EXT.1	This SFR applies to the revocation of certificates which is not defined in the Base-PP.
FDP_CSI_EXT.1	This SFR applies to generating certificate status information which is not defined in the Base-PP.
FDP_OCSP_EXT.1	This SFR applies to generating OCSP responses which is not defined in the Base-PP.
FDP_OCSPS_EXT.1	This SFR applies to OCSP stapling which is not defined in the Base-PP.
FIA_ESTC_EXT.1	This SFR applies to the enforcement of Enrollment of Secure Transport to obtain its embedded CA certificate which is not defined in the Base-PP.
FTA_TAB.1/TLS	This SFR applies to having a notice and consent warning message at the start of an SSL/TLS inspection session which is not defined in the Base-PP.
FCS_TTTC_EXT.3	This SFR applies to thru-traffic TLS Inspection Client Protocol with mutual authentication which is not defined in the Base-PP.
FCS_TTTS_EXT.3	This SFR applies to thru-traffic TLS Inspection Server Protocol with mutual authentication which is not defined in the Base-PP.
FDP_CER_EXT.4	This SFR applies to the implementation of the certificate profile functionality.
FDP_CER_EXT.5	This SFR applies to the certificate issuance rules applied for client certificates which is not defined in the Base-PP.
FDP_CSI_EXT.2	This SFR applies to generating certificate status information for issued client certificates which is not defined in the Base-PP.

PP-Module Requirement	Consistency Rationale
FDP_STIP_EXT.2	This SFR applies to the TLS session implementation of the inspection operation that is not defined in the Base-PP.
Objective Requirements	
FIA_ESTC_EXT.2	This SFR applies to the generation of TLS unique values used by client which is not defined in the Base-PP.

A. Optional Requirements

As indicated in section 2, the baseline requirements (those that must be performed by the TOE) are contained in the body of this PP-Module. Additionally, there are three other types of requirements specified in Appendices A, B, and C.

- Appendix A: Requirements that can be included in the ST, but are not required in order for a TOE to claim conformance to this PP-Module.
- Appendix B: Requirements based on selections in the body of the EP: if certain selections are made, then additional requirements in that appendix must be included.
- Appendix C: Components that are not required in order to conform to this PP-Module, but will be included in the baseline requirements in future versions of this PP, so adoption by vendors is encouraged.

Note that the ST author is responsible for ensuring that requirements that may be associated with those in the appendices, but not listed (e.g., FMT-type requirements) are also included in the ST.

A.1 Persistent Local Audit Storage

The SFRs in this section are optional. They should be claimed if the TOE provides local audit storage (i.e., if FAU_STG.1 is claimed in the base NDcPP) and that local audit storage is intended to provide a persistent, searchable record of security events within the TOE, either as a backup or replacement of an external audit capability.

FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [*selection: Security Administrators, Auditors*] with the capability to read all information from the local audit records.

FAU_SAR.1.2 The TSF shall provide the local audit records in a manner suitable for the administrator to interpret the information.

FAU_SAR.3 Selectable Audit Review

FAU_SAR.3.1 The TSF shall provide the ability to apply **searches** of **local** audit data based on **[*assignment: object identifier of certificate*] associated with the event**.

Application Note: *FAU_SCR_EXT.1 defines the ability of the TOE to search a certificate repository and/or audit trail to find certificates based on certain values of individual fields. The TSF will likely identify certificates using some form of unique identifier that is not immediately identifiable to an auditor. The intent of this SFR along with FAU_SCR_EXT.1 is that the auditor has the ability to obtain a certificate's unique identifier by searching for other known fields and then using that unique identifier as an input to searching audit data for all activities involving that certificate.*

A.2 Certificate Pinning

FDP_PIN_EXT.1 Certificate Pinning

Certificate pinning is an optional feature to address the threat of unauthorized access to user data managed by the TOE via unauthorized STIP or adversary man-in-the-middle exploits. This feature is desirable since implementation of a STIP to protect a client enclave will prevent the clients from effectively providing this feature.

FDP_PIN_EXT.1.1 The TSF shall be able to detect and [*selection: alert, [assignment: perform a [Security Administrator] managed action]*] to changes in the [*selection: public key, certificate, certificate issuer*] used by requested servers according to **[*selection: a security administrator configurable number of the most common requested servers, a security administrator specified list of servers, [assignment: security administrator configurable rules based on attributes of the certificates used by the server]*]**.

Application Note: *This requirement should be claimed if implemented by the TOE. If claimed, additional FMT_MOF.1 and audit events associated with the function must be claimed.*

B. Selection-Based Requirements

As indicated in the introduction to this PP-Module, the baseline requirements (those that must be performed by the TOE) are contained in the body of the PP-Module. There are additional requirements based on selections in the body of the EP: if certain selections are made, then additional requirements below will need to be included.

B.1 Certificate Status Information

FDP_CRL_EXT.1 Certificate Revocation List Generation

FDP_CRL_EXT.1.1 When the TSF is configured to generate CRLs, the TSF shall verify that all mandatory fields in any generated CRL contains values in accordance with ITU-T Recommendation X.509. At a minimum, the following items shall be validated:

a) If the version field is present, then it shall contain a 1.
b) If the CRL contains any critical extensions, then the version field shall be present and contain the integer 1.
c) The [*selection: issuer, issuerAltName*] fields shall indicate the configured name of the CA.
d) If the issuer field contains a null Name (e.g., a sequence of zero relative distinguished names), then the CRL shall contain a critical issuerAltName extension.
e) The signature and signatureAlgorithm fields shall contain the OID for a digital signature algorithm in accordance with FCS_COP.1**/SigGen in the NDcPP**.
f) The thisUpdate field shall indicate the issue date of the CRL.
g) The time specified in the nextUpdate field (if populated) shall not precede the time specified in the thisUpdate field.

Application Note: *This requirement should be claimed if 'ITU-T Recommendation X.509v2 CRL' is selected in FDP_CSI_EXT.1.1*

FDP_CSI_EXT.1 Certificate Status Information

FDP_CSI_EXT.1.1 The TSF shall generate certificate status information whose format complies with [*selection: ITU-T Recommendation X.509v2 CRL, the OCSP standard as defined by RFC 6960*].

FDP_CSI_EXT.1.2 The TSF shall support changes to the status of a certificate by [*selection: **[selection: Security Administrator, CA Operations staff]**, [assignment: automated revocation rules]*].

FDP_CSI_EXT.1.3 The TSF shall [*selection: provide, interface with the Operational Environment to provide*] certificate status information generated in accordance with FDP_CSI_EXT.1.1 via [*selection: posting CRLs at the location specified in the cRLDistributionPoints of the issued certificate, an OCSP mechanism indicated in the authorityInfoAccess extension of the issued certificate, OCSP Stapling in accordance with FDP_OCSPS_EXT.1*].

Application Note: *This SFR should be claimed if claimed if the selection 'generate certificate status information' is selected in FDP_CSIR_EXT.1.1.*

The ST should specify the format(s) used to supply certificate status information in FDP_CSI_EXT.1.1, and the mechanism(s) used to provide the status to relying parties including all monitored clients in the second selection in FDP_CSI_EXT.1.3. If CRLs are identified in FDP_CSI_EXT.1.1, then cRLDistributionPoints must be claimed in FDP_CSI_EXT.1.3 and in FDP_CER_EXT.1.2 item (g), sub-item (g). If the OCSP standard is selected in FDP_CSI_EXT.1.1, then at least one of the last two options in the second selection of FDP_CSI_EXT.1.3 must be claimed. If the second option (OCSP) is claimed, authorityInfoAccess must be claimed in FDP_CER_EXT.1.2 item (g), sub-item (g). OCSP stapling may also be claimed if the TOE only generates CRLs, but interfaces with an external OCSP responder that uses those CRLs.

Automated rules for revoking certificates in response to the TOE's discovery that a previously issued certificate is no longer appropriate for the subject, or due to cache clearing, timeouts, or other rules should be described in the assignment of FDP_CSI_EXT.1.2.

FDP_OCSP_EXT.1 OCSP Basic Response Generation

FDP_OCSP_EXT.1.1 When the TSF is configured to generate OCSP responses of the basic response type, the TSF shall ensure that all mandatory fields in the OCSP basic response contain values in accordance with RFC 6960. At a minimum, the following items shall be validated:

a) The version field shall contain a 0.
b) The signatureAlgorithm field shall contain the object identifier (OID) for a digital signature algorithm in accordance with FCS_COP.1**/SigGen in the NDcPP**.
c) The thisUpdate field shall indicate the time at which the status being indicated is known to be correct.
d) The producedAt field shall indicate the time at which the OCSP responder signed the response.
e) The time specified in the nextUpdate field (if populated) shall not precede the time specified in the thisUpdate field.

Application Note: *This requirement should be claimed if 'the OCSP standard as defined by RFC 6960' is selected in FDP_CSI_EXT.1.1.*

FDP_OCSPS_EXT.1 OCSP Stapling

FDP_OCSPS_EXT.1.1 The TSF shall be able to process [*selection: Certificate Status Request extension in accordance with RFC 6066 section 8, Certificate Status Request List V2 in accordance with RFC 6961*].

FDP_OCSPS_EXT.1.2 The TSF shall [*selection: generate OCSP response information in accordance with FDP_OCSP_EXT.1, interface with an OCSP provider to obtain an OCSP response*] and populate a Certificate Status Message in accordance with RFC 6066.

Application Note: *This SFR must be claimed in situations where the TOE computes OCSP responses for inclusion in TLS certificate status messages. It may also be claimed if the TOE includes a separate certificate status component (CRL or OCSP provider) and provides an interface to an internal or external OCSP responder that processes certificate status information provided to it by the TOE. When claimed, certificate status is provided via OCSP stapling contained within TLS Server certificate status message(s).*

B.2 Certificate Enrollment

FIA_ESTC_EXT.1 Enrollment over Secure Transport (EST) Client

FIA_ESTC_EXT.1.1 The TSF shall use the Enrollment over Secure Transport (EST) as specified in RFC 7030 to obtain its embedded CA certificate and [*assignment: other certificates for the TOE*] from an external certification authority (external CA) associated with an authorized EST server.

FIA_ESTC_EXT.1.2 The TSF shall be able to obtain EST server and CA certificates for authorized EST services via [*selection: implicit Trust Anchor/Trust Store (TA) configured by* ***[selection: Security Administrator, CA Operations Staff]****, an explicit TA populated via a TLS-authenticated EST CA certificate request in accordance with RFC 7030 section 4.1.2 and FCS_TLSC_EXT.1*].

FIA_ESTC_EXT.1.3 The TSF shall authenticate EST servers using X.509 certificates that chain to trust store elements from the [*selection: implicit Trust Anchor database, explicit Trust Anchor/Trust Store*] in accordance with FIA_X509_EXT.1**/Rev** for all EST requests.

FIA_ESTC_EXT.1.4 The TSF shall authenticate its certificate enrollment requests to receive the signing certificate of its embedded CA and [*assignment: other certificates required to authenticate the TOE*], from an authorized EST server using [*selection*:

- *HTTP basic authentication transported over TLS in accordance with RFC* 7030 section 3.2.3 and FCS_TLSC_EXT.1;
- *HTTP digest authentication using a cryptographic hash algorithm in accordance with FCS_COP.1****/Hash****, transported over TLS in accordance with RFC 7030 section 3.2.3 and FCS_TLSC_EXT.1;*
- *Certificate-based authentication in accordance with RFC 7030 section 3.3.2 and FCS_TLSC_EXT.2 using [assignment: a pre-existing certificate authorized by the EST server]*].

FIA_ESTC_EXT.1.5 The TSF shall generate authenticated re-enrollment requests in accordance with RFC 7030 Section 3.3.2 and FCS_TLSC_EXT.1 **in the NDcPP**, using an existing valid certificate with the same subject name as the requested certificate and which was issued by the external CA.

Application Note: *This SFR should be claimed if 'Enrollment over Secure Transport…' is claimed in FIA_ENR_EXT.1.1.*

In FIA_ESTC_EXT.1.1, the external CA can be a root or intermediate CA operator selected by a privileged user.

The third choice in the selection for FIA_ESTC_EXT.1.4 is selected if a pre-existing certificate exists. The assignment should specify whether this pre-existing certificate is established by the vendor, or installed by a privileged user.

B.3 Inspection Policy Banner

Local policy may require explicit consent to monitoring before inspection of TLS encrypted data. If the STIP may be deployed in an environment where clients might not already have granted this approval, the TOE might be required to obtain this consent. The requirement in this section should be claimed if the TLS session establishment policy requires it.

FTA_TAB.1/TLS TOE Access Banner (Consent to Monitor Banners for TLS Inspection)

FTA_TAB.1.1/TLS Before forwarding decrypted application data intended for the requested server to inspection processing components the TSF shall display **to the monitored client, a Security Administrator-specified** advisory **notice and consent** warning message regarding use of the TOE.

Application Note: *This SFR should be claimed if 'provide a consent to monitor banner..' is selected in FDP_STIP_EXT.1.3.*

B.4 Authentication of Monitored Clients

This section describes support for mutual authentication of clients when requested by the TOE to support the following use cases:

- TOE requested mutual authentication: Mutual authentication provides authenticated client attributes that can be used to define exception processing. If the ST claims to support client authentication of monitored clients accessing the TOE, this SFR should be claimed in the selection of FDP_STIP_EXT.1.
- Certificate request from the requested server: Inspection of TLS sessions requiring mutual authentication is a narrow use case for the SSL/TLS inspection proxy, where both the client and server trust the TOE's embedded CA. In such instances, mutual authentication represents an assertion to the requested server that the client has been authenticated. There are other, preferred mechanisms such as SOAP, KERBEROS, XAML assertions, than TLS client authentication using proxy certificates that provide a more accurate representation of the role of a federated identity service provider, in accordance with NIST SP 800-63-03. Also, mutual authentication is typically used to control access to sensitive information authorized only to specific clients, and the willingness of the server's content owner to trust the proxy, providing access such sensitive content further restricts legitimate use cases. Finally, certificates issued to represent users subject to a certificate policy or certificate practice statement, especially those compliant with NIST FIPS 201, may be required to meet an equivalent certificate policy or certificate practice statement.

If mutual authentication by the TOE is to perform the TLS inspection operation on TLS sessions between monitored clients and requested servers requiring mutual authentication, FCS_TTTC_EXT.3, FCS_TTTS_EXT.3, FDP_CER_EXT.4, FDP_CER_EXT.5, FDP_CSI_EXT.2, and FDP_STIP_EXT.2 in this section must be claimed. In addition, the 'mutual authentication inspection' item should be selected in the selection for FDP_TEP_EXT.1.5 and an exception specification to identify servers which are authorized and configured to support mutual authentication inspection must be described in the assignment of FDP_TEP_EXT.1.4. TLS servers requesting mutual authentication are likely to also require revocation information, so it is recommended that FDP_CSIR_EXT.1 selections be made to provide certificate status information, even if the constraint for short validity periods is achieved.

FCS_TTTC_EXT.3 Thru-Traffic TLS Inspection Client Protocol with Mutual Authentication Representing Monitored Clients

FCS_TTTC_EXT.3.1 The TSF shall support mutual authentication using X.509v3 certificates generated in accordance with FDP_CER_EXT.5 for inspection processing operation between a monitored client represented in the generated certificate and a requested server that provides a certificate request in the TLS handshake.

Application note: *This SFR must be claimed if the TSF is capable of inspecting TLS sessions from monitored clients to requested servers requiring client authentication.*

FCS_TTTS_EXT.3 Thru-Traffic TLS Inspection Server Protocol with Mutual Authentication of Monitored Clients

FCS_TTTS_EXT.3.1 The TSF shall support mutual authentication of TLS clients using X.509v3 certificates.

FCS_TTTS_EXT.3.2 The TSF shall send a Certificate Request message to the TLS client when mutual authentication is required by the configured TLS session establishment policy as defined in FDP_TEP_EXT.1.

FCS_TTTS_EXT.3.3 The TSF shall validate the certificate presented by the client and [*selection: allow the connection if the certificate is invalid and an exception is permitted for the client, terminate the connection if the certificate is invalid*].

Application Note: *Validity is determined by the identifier verification, certificate path, the expiration date, and the revocation status in accordance with RFC 5280. Certificate validity is tested in accordance with testing performed for FIA_X509_EXT.1/STIP.*

FCS_TTTS_EXT.3.4 The TSF shall not establish a TLS session if the distinguished name (DN) or Subject Alternative Name (SAN) contained in a certificate does not match the expected identifier for the client.

Application Note: *The client identifier may be in the Subject field or the Subject Alternative Name extension of the certificate.*

FDP_CER_EXT.4 Certificate Profiles for Client Certificates

FDP_CER_EXT.4.1 The TSF shall implement a certificate profile function for TLS client certificates issued by a CA embedded within the TOE, and shall ensure that issued certificates are consistent with configured profiles.

Application Note: *The CA issuing client certificates may be required to support configured certificate profiles that differ significantly from server certificates, and to support multiple certificate profiles for the clients supported.*

FDP_CER_EXT.4.2 The TSF shall generate certificates representing monitored clients using profiles that comply with requirements for certificates as specified in IETF RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" as refined below. At a minimum, the TSF shall ensure that:

a) The version field shall contain the integer 2.
b) The issuerUniqueID or subjectUniqueID fields are not populated.
c) The serialNumber shall be unique with respect to the issuing Certification Authority.
d) The validity field shall specify a notBefore value that does not precede the current time and a notAfter value that does not precede the value specified in notBefore.
e) The issuer field is not empty and is populated with the **[*selection: Security Administrator, CA Operations Staff*]**-configured CA name.
f) The signature field and the algorithm in the subjectPublicKeyInfo field shall contain the OID for a signature algorithm specified in FCS_COP.1**/SigGen in the NDcPP**.
g) The following extensions are supported:
   a. subjectKeyIdentifier
   b. authorityKeyIdentifier
   c. keyUsage
   d. extendedKeyUsage
   e. certificatePolicy
   f. [*selection: basicConstraints, cRLDistributionPoints, authorityInfoAccess, no other extensions*]
h) A subject field containing a null Name (e.g., a sequence of zero relative distinguished names) is accompanied by a populated critical subjectAltName extension.
i) The subjectKeyIdentifier extension is populated with a value unique for each public key contained in a certificate issued by the TSF.
j) The authorityKeyIdentifier extension in any certificate issued by the TOE must be populated and must be the same as the subjectKeyIdentifier extension contained in the TOE's embedded CA's signing certificate.
k) Populated keyUsage and extendedKeyUsage fields in the same certificate shall contain consistent values reflecting exclusive TLS server use as follows:

keyUsage	extendedKeyUsage
digitalSignature	clientAuth
digital Signature, keyEncipherment	clientAuth
digital Signature, keyAgreement	clientAuth

Application Note: *RFC updates to RFC 5280 are included in this requirement.*

The inclusion of the cRLDistributionPoints and authorityInfoAccess extensions depend on the selections made in FDP_CSIR_EXT.1 and FDP_CSI_EXT.2.3 if claimed.

Uniqueness for the subject key identifier is specific to the instance of the embedded CA. The same configured CA should not issue certificates with different public keys having the same subject key identifier.

FDP_CER_EXT.4.3 The TSF shall implement the following rules for populating certificate fields based on constraints imposed by the TOE's embedded CA's signing certificate:

- The validity field shall specify a notAfter time that does not exceed the notAfter time of the CA's signing certificate.
- The issuer field identifies the [*selection: subject, [assignment:* ***[selection: Security Administrator, CA Operations Staff]*** *assigned identifying information]*] of the CA's signing certificate.
- [*selection:*
  - *The subject name is limited by name constraints specified in the CA's signing certificate,*
  - *[assignment: list of rules],*
  - *no other rules*].

FDP_CER_EXT.4.4 The TSF shall implement the following rules for populating certificate fields based on the validated certificate and constraints imposed by the **[*selection: Security Administrator, CA Operations Staff*]**:

a) The Subject/Subject Alternative Name shall be copied from validated client certificate.

b) The notBefore field shall not precede the notBefore field of the validated client certificate.

c) The notAfter field shall not exceed the notAfter field of the validated client certificate.

d) The notAfter field shall not exceed the current time by more than a maximum validity duration value as configured by a **[*selection: Security Administrator, CA Operations Staff*]** user.

e) If the basicConstraints field is configured to be present, it shall be populated with the value cA=False.

f) If configured to be present, the policy OID and policy mapping fields shall be populated according to [*selection:*

- *a* **[selection*: Security Administrator, CA Operations Staff]*** *configured mapping from validated client certificate values to one or more stated policy OIDs]*
- [*assignment: list of rules*].

Application Note: *Policy OIDs for proxy-issued certificates and mappings to FIPS 201 defined policies may be required to be supported for SSL/TLS inspection proxies issuing certificates* *representing person-entities subject to FIPS 201 authentication methods, since requested servers requiring client authentication are likely to expect to validate client certificates issued by the equivalent of such a certificate policy. If Policy OIDs are used, the embedded CA may be subject to additional constraints indicated in a Certificate Policy.*

FDP_CER_EXT.5 Certificate Issuance Rules for Client Certificates

FDP_CER_EXT.5.1 The TSF shall issue certificates in response to a validated client certificate according to the following rules: The issued certificate is in compliance with a current certificate profile defined in accordance with FDP_CER_EXT.4 and

- The TLS session establishment policy is configured to allow inspection of TLS sessions with mutual authentication between the monitored client whose certificate is validated by the TSF and one or more requested servers,
- The specific requested server includes a Certificate Request message in the TLS handshake,

[*selection:*

- *A valid certificate for the same subject is not present in cache,*
- *The embedded CA certificate's name space allows issuance of a certificate that represents the authenticated client,*
- *No other constraints*].

Application Note: *Caching client certificates is neither required nor preferred, since such storage of private keys associated to signature keys is strictly controlled by various certificate policies and practice statements, especially when the validated client certificate associated to the monitored client is issued under NIST FIPS 201. If supported, the time in cache for client certificates should be limited to the minimal revocation time (emergency revocation) allowed for validated certificates used by any monitored client.*

FDP_CER_EXT.5.2 The TSF shall reject all certificate requests originating external to the TOE.

FDP_CSI_EXT.2 Certificate Status Information for Client Certificates

FDP_CSI_EXT.2.1 The TSF shall generate certificate status information for issued client certificates whose format complies with [*ITU-T Recommendation X.509v2 CRL, the OCSP standard as defined by RFC 6960*].

FDP_CSI_EXT.2.2 The TSF shall support changes to the status of a certificate in accordance with the following rules:

- as directed by **[*selection: Security Administrator, CA Operations staff*]** and
- [*selection:*

- *a certificate in cache is revoked when a certificate representing the same subject is received for client authentication and either*
    - *the validation of the received certificate fails or*
    - *the validation of the received certificate passes and the certificate fields of the validated certificate would result in a different certificate being issued under the current profile in accordance with FDP_CER_EXT.4;*
- *[assignment: other rules for revocation of issued certificates];*
- *no other rules*].

Application Note: *In order to meet revocation requirements associated with credentials issued under FIPS 201, the first item of the second selection in this element must be claimed if cache is provided.*

Automated rules for revoking certificates in response to the TOE's discovery that a previously issued certificate is no longer appropriate for the subject, or due to cache clearing, timeouts, or other rules should be described in the assignment of FDP_CSI_EXT.2.2.

FDP_CSI_EXT.2.3 The TSF shall [*selection: provide, interface with the Operational Environment to provide*] certificate status information generated in accordance with FDP_CSI_EXT.2.1 via [*selection: posting CRLs at the location specified in the cRLDistributionPoints of the issued certificate, an OCSP mechanism indicated in the authorityInfoAccess extension of the issued certificate*].

Application Note: *Based on the selection, the ST author must choose the appropriate requirements from Appendix B.1 of this PP-Module.*

The ST should specify the format(s) used to supply certificate status information in FDP_CSI_EXT.2.1, and the mechanism(s) used to provide the status to relying parties including all servers authorized to use mutually authenticated TLS in accordance with the configured TLS session establishment policy, identified in FDP_TEP_EXT.1, in the second selection in FDP_CSI_EXT.2.3. If CRLs are identified in FDP_CSI_EXT.2.1, then cRLDistributionPoints must be claimed in FDP_CSI_EXT.2.3 and in FDP_CER_EXT.4.2 item (g), sub-item (g). If the OCSP standard is selected in FDP_CSI_EXT.2.1, then 'authorityInfoAccess' must be selected in the second selection of FDP_CSI_EXT.2.3 and in FDP_CER_EXT.4.2 item (g), sub-item (g).

FDP_STIP_EXT.2 Mutual Authentication Inspection Operation

FDP_STIP_EXT.2.1 The TSF shall be capable of providing mutual authentication of the monitored client to a requested server when performing the inspection operation when mutual authentication is allowed for the requested server by the configured policy, and the TLS handshake with the requested server includes a certificate request.

Application Note: *The policy is flexible; it could be static policy or a policy associated with certain clients, servers, or connections.*

FDP_STIP_EXT.2.2 After receiving the TLS client certificate from the monitored client, the TSF shall be able to generate a certificate representing the client in accordance with FDP_CER_EXT.5 and [*selection: obtain a valid certificate representing the client from cache, no other method*] matching the current certificate profile.

Application Note: *Certificate caching of client certificates is not required. However, in the case where certificate caching is supported, the TSF will still need to perform certificate generation if the cached certificate does not match the current profile determined by FDP_CER_EXT.4 which depends on values derived from the certificate provided by the monitored client.*

FDP_STIP_EXT.2.3 After obtaining a certificate representing the monitored client, the TSF shall send the client certificate and certificate verify messages to the requested server.

Application Note: *This element completes the TLS handshake between the TOE and the requested server as a complete TLS handshake with mutual authentication.*

B.5 Other Selection-Based SFRs

FAU_SCR_EXT.1 Certificate Repository Review

FAU_SCR_EXT.1.1 The TSF shall [*selection: provide, invoke the Operational Environment to provide*] the ability to search certificates containing specified values of the following certificate fields: **[*selection:***

- ***subject name,***
- ***individual components of Subject Alternative Name,***
- ***subject ID,***
- ***issuer ID,***
- ***algorithm ID,***
- ***public key,***
- ***key usage,***
- ***extended key usage,***
- ***serial number,***
- ***[assignment: list of other certificate fields]*]**,

returning all matching certificates and [*assignment: object identifier(s)*] of matching certificate(s).

Application Note: *This SFR must be claimed if the selection in FAU_GCR_EXT.1.1 is 'store.' It may be claimed if the selection in FAU_GCR_EXT.1.1 is 'invokes the Operational Environment to store' when the TSF provides an interface to the certificate repository to perform searches. The ability to search on certificate fields is useful for conducting forensic analysis. If the certificate repository is stored within the TOE boundary, then the first item of the first selection is chosen. If the repository* *is stored in the OE, but the auditor uses TSF interfaces to perform this function on the repository, then the second item of the first selection is chosen. It is allowed that this function be provided entirely by the OE (when the repository is stored in the OE); if this is the case, then this requirement is not included in the ST, but instead the OE.CERTIFICATE_REPOSITORY_SEARCH objective is included (this objective is omitted in the other two cases, when this SFR is included in the ST).*

In the second selection and assignment, the ST author includes/fills in the values that can be searched on for this function; at least one value is required to be selected.

FCS_CKM_EXT.5 Public Key Integrity

FCS_CKM_EXT.5.1 The TSF shall protect persistent public keys against undetected modification through the use of [*selection: digital signatures* ***(in accordance with FCS_COP.1/SigGen)****, keyed hashes* ***(in accordance with FCS_COP.1/KeyedHash)***].

FCS_CKM_EXT.5.2 The [*selection: digital signature, keyed hash*] used to protect a public key shall be verified upon [*assignment: criteria for automated verification*].

Application Note: *This SFR is included when the second selection in FDP_STG_EXT.1.1 is chosen, and applies to the public keys listed in that SFR.*

The selections in FCS_CKM_EXT.5.1 and FCS_CKM_EXT.5.2 should agree, and the assignment in FCS_CKM.5.2 for the criteria for automated verification can be event or time based and should provide operationally relevant integrity failure detection, for which recovery is feasible.

FCS_TTTC_EXT.4 STIP Client-Side Support for Renegotiation

FCS_TTTC_EXT.4.1 The TSF shall support secure renegotiation on STIP TLS connections through use of the "renegotiation_info" TLS extension in accordance with RFC 5746.

FCS_TTTC_EXT.4.2 The TSF shall include [*selection, choose only one of: renegotiation_info extension, TLS_EMPTY_RENEGOTIATION_INFO_SCSV cipher suite*] in the Client Hello message.

Application Note: *This SFR is included when "session renegotiation" in FCS_TTTC_EXT.1.1 is chosen. RFC 5746 defines an extension to TLS that binds renegotiation handshakes to the cryptography in the original handshake. The cipher suite included in the selection is a means for clients to be compatible with servers that don't support the extension. It is recommended that client implementations support both the cipher suite and the extension.*

FCS_TTTC_EXT.4.3 The TSF shall ensure that renegotiation is performed before [*selection: [assignment: renegotiation rules], 2^20 64-bit data blocks are encrypted using TDES cipher suites using the same key*].

Application Note: *If a TDES cipher suite is selected in FCS_TTTC_EXT.1.1, the amount of data* *encrypted with the same key is limited in accordance with NIST SP800-67R2, section 3.4, and the second selection should be chosen.*

FCS_TTTS_EXT.4 STIP Server-Side Support for Renegotiation

FCS_TTTS_EXT.4.1 The TSF shall support the "renegotiation_info" TLS extension in accordance with RFC 5746.

FCS_TTTS_EXT.4.2 The TSF shall include the renegotiation_info extension in Server Hello messages.

Application Note: *This SFR is included when "session renegotiation" in FCS_TTTS_EXT.1.1 is chosen. RFC 5746 defines an extension to TLS that binds renegotiation handshakes to the cryptography in the original handshake.*

C. Objective Requirements

This Appendix includes requirements that specify security functionality which also addresses threats. The requirements are not currently mandated in the body of this PP-Module as they describe security functionality not yet widely available in commercial technology. However, these requirements may be included in the ST such that the TOE is still conformant to this PP-Module, and it is expected that they be included as soon as possible.

FIA_ESTC_EXT.2 EST Client Use of TLS-Unique Value

FIA_ESTC_EXT.2.1 The TSF shall generate tls-unique values and integrate them into EST requests it generates in accordance with RFC 7030 section 3.5.

Application Note: *This SFR describes an optional element of RFC 7030 that strengthens the authentication provided by EST. While RFC 7030 requires EST servers to validate the tls-unique values when presented, this requirement is not implemented in current EST servers. FIA_ESTC_EXT.2.1 will be integrated into FIA_ESTC_EXT.1 in a subsequent release of this PP-Module and should be claimed if the EST implementation supports it.*

D. Extended Component Definitions

This Appendix provides a definition for all of the extended components introduced in this PP-Module. The families to which these components belong are identified in the following table:

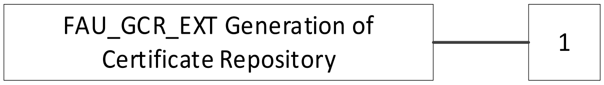
Functional Class	Functional Families
Security Audit (FAU)	FAU_GCR_EXT Generation of Certificate Repository
	FAU_SCR_EXT Certificate Repository Review
Cryptographic Support (FCS)	FCS_CKM_EXT Cryptographic Key Management
	FCS_STG_EXT Cryptographic Key Storage
	FCS_TTTC_EXT Thru-Traffic TLS Inspection Client Protocol
	FCS_TTTS_EXT Thru-Traffic TLS Inspection Server Protocol
User Data Protection (FDP)	FDP_CER_EXT Certificate Usage
	FDP_CRL_EXT Certificate Revocation List
	FDP_CSI_EXT Certificate Status Information
	FDP_CSIR_EXT Certificate Status Information Required
	FDP_OCSP_EXT Online Certificate Status Protocol
	FDP_OCSPS_EXT Online Certificate Status Protocol Stapling
	FDP_PIN_EXT Certificate Pinning
	FDP_PPP_EXT Plaintext Processing Policy
	FDP_PRC_EXT Plaintext Routing Control
	FDP_STG_EXT User Data Storage
	FDP_STIP_EXT SSL/TLS Inspection Proxy Functions
	FDP_TEP_EXT TLS Establishment Policy
Identification and Authentication (FIA)	FIA_ENR_EXT Certificate Enrollment
	FIA_ESTC_EXT Enrollment over Secure Transport Client Protocol
Protection of the TSF (FPT)	FPT_KST_EXT Key Storage

D.1 FAU_GCR_EXT Generation of Certificate Repository

Family Behavior

Components in this family define requirements for persistent certificate storage in a repository.

Component Leveling



FAU_GCR_EXT.1, Generation of Certificate Repository, requires a conformant TOE to specify how it stores certificates that are issued by the TSF.

Management: FAU_GCR_EXT.1

No specific management functions are identified.

Audit: FAU_GCR_EXT.1

There are no auditable events foreseen.

FAU_GCR_EXT.1 Generation of Certificate Repository

Hierarchical to: No other components

Dependencies: FDP_CER_EXT.1 Certificate Profiles for Server Certificates

FDP_CER_EXT.3 Certificate Issuance Rules for Server Certificates

FAU_GCR_EXT.1.1 The TSF shall [*selection: store, invoke the Operational Environment to store*] certificates issued by the TSF.

D.2 FAU_SCR_EXT Certificate Repository Review

Family Behavior

Components in this family define requirements for searching the contents of a certificate repository.

Component Leveling

FAU_SCR_EXT.1, Certificate Repository Review, requires a conformant TOE to support the searching of a certificate repository based on the values of specific certificate fields.

Management: FAU_SCR_EXT.1

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

- Ability to search the certificate repository.

Audit: FAU_SCR_EXT.1

There are no auditable events foreseen.

FAU_SCR_EXT.1 Certificate Repository Review

Hierarchical to: No other components

Dependencies: FAU_GCR_EXT.1 Generation of Certificate Repository

FAU_SCR_EXT.1.1 The TSF shall [*selection: provide, invoke the Operational Environment to provide*] the ability to search certificates containing specified values of the following certificate fields: [*assignment: list of certificate fields*], returning all matching certificates and [*assignment: object identifier(s)*] of matching certificate(s).

D.3 FCS_CKM_EXT Cryptographic Key Management

Family Behavior

Components in this family define requirements for the lifecycle of cryptographic keys in specific cases that are not addressed by the FCS_CKM family defined in CC Part 2.

Component Leveling

FCS_CKM_EXT.5, Public Key Integrity, requires the TSF to apply a cryptographic integrity validation method to public keys in persistent storage.

Management: FCS_CKM_EXT.5

No specific management functions are identified.

Audit: FCS_CKM_EXT.5

There are no auditable events foreseen.

FCS_CKM_EXT.5 Public Key Integrity

Hierarchical to: No other components

Dependencies: FCS_COP.1 Cryptographic Operation

FCS_CKM_EXT.5.1 The TSF shall protect persistent public keys against undetected modification through the use of [*selection: digital signatures, keyed hashes*].

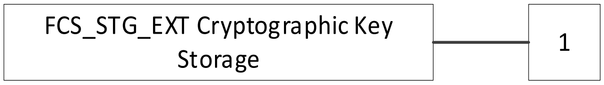
FCS_CKM_EXT.5.2 The [*selection: digital signature, keyed hash*] used to protect a public key shall be verified upon [*assignment: criteria for automated verification*].

D.4 FCS_STG_EXT Cryptographic Key Storage

Family Behavior

Components in this family define requirements for the secure storage of cryptographic keys.

Component Leveling



FCS_STG_EXT.1, Cryptographic Key Storage, requires the TSF to store persistent secret and private keys using a hardware-protected storage mechanism.

Management: FCS_STG_EXT.1

No specific management functions are identified.

Audit: FCS_STG_EXT.1

There are no auditable events foreseen.

FCS_STG_EXT.1 Cryptographic Key Storage

Hierarchical to: No other components

Dependencies: No dependencies

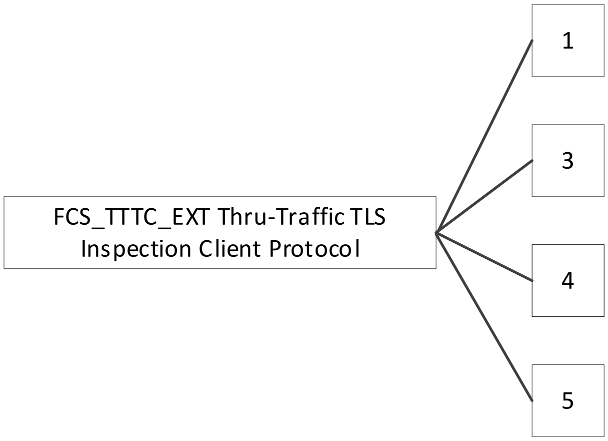
FCS_STG_EXT.1.1 Persistent private and secret keys shall be stored within the TSF using [*assignment: method of hardware-protected storage*].

D.5 FCS_TTTC_EXT Thru-Traffic TLS Inspection Client Protocol

Family Behavior

Components in this family define requirements for the TOE's ability to act as a TLS client for the purpose of reconstructing the original intended TLS connection that it is inserted into as a proxy.

Component Leveling



FCS_TTTC_EXT.1, Thru-Traffic TLS Inspection Client Protocol, defines the types of TLS client connections the TSF can support when acting as a proxy.

FCS_TTTC_EXT.3, Thru-Traffic TLS Inspection Client Protocol with Mutual Authentication Representing Monitored Clients, requires the TSF to present a TLS client certificate when connecting to the requested server as part of establishing a TLS proxy connection.

FCS_TTTC_EXT.4, STIP Client-Side Support for Renegotiation, requires the TSF to support session renegotiation when acting as a TLS client for a proxy connection.

FCS_TTTC_EXT.5, Thru-Traffic TLS Inspection Client Support for Supported Groups Extension, requires the TSF to use the TLS Supported Groups Extension when establishing a proxy connection to a requested server to ensure the use of appropriate key establishment parameters.

Management: FCS_TTTC_EXT.1

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

- Ability to configure the cryptographic functionality.

Management: FCS_TTTC_EXT.3, FCS_TTTC_EXT.4, FCS_TTTC_EXT.5

No specific management functions are identified.

Audit: FCS_TTTC_EXT.1

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Establishment of TLS session.

Audit: FCS_TTTC_EXT.3

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Successful and unsuccessful authorization of mutual authentication.

Audit: FCS_TTTC_EXT.4, FCS_TTTC_EXT.5

There are no auditable events foreseen.

FCS_TTTC_EXT.1 Thru-Traffic TLS Inspection Client Protocol

Hierarchical to: No other components

Dependencies: FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.2 Cryptographic Key Distribution

FCS_COP.1 Cryptographic Operation

FCS_RBG_EXT.1 Random Bit Generation

FCS_TTTS_EXT.1 Thru-Traffic TLS Inspection Server Protocol

FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.2 X.509 Certificate Authentication

FCS_TTTC_EXT.1.1 The TSF shall implement [*assignment: TLS versions*] as a client to the requested server that supports the following cipher suites: [*assignment: list of cipher suites and reference to RFC in which each is defined*] and also supports functionality for [*selection:*

- *mutual authentication,*
- *session renegotiation,*
- *none*

].

FCS_TTTC_EXT.1.2 The TSF shall verify that the presented identifier matches the reference identifier of the server requested by the monitored client using methods described in RFC 6125 section 6 for DNS name types, and via exact, byte-by-byte matching for IP address name types.

FCS_TTTC_EXT.1.3 The TSF shall validate the certificate presented by the server and terminate the connection if the certificate is invalid, except as allowed by FIA_X509_EXT.2.2.

FCS_TTTC_EXT.1.4 The TSF shall formulate the Client Hello such that it presents the highest version of the TLS protocol supported by the proxy function in the version field, and presents the list of cipher suites in descending order of preference associated with requested server.

FCS_TTTC_EXT.3 Thru-Traffic TLS Inspection Client Protocol with Mutual Authentication Representing Monitored Clients

Hierarchical to: No other components

Dependencies: FCS_TTTC_EXT.1 Thru-Traffic TLS Inspection Client Protocol

FDP_CER_EXT.5 Certificate Issuance Rules for Client Certificates

FCS_TTTC_EXT.3.1 The TSF shall support mutual authentication using X.509v3 certificates generated in accordance with FDP_CER_EXT.5 for inspection processing operation between a monitored client represented in the generated certificate and a requested server that provides a certificate request in the TLS handshake.

FCS_TTTC_EXT.4 STIP Client-Side Support for Renegotiation

Hierarchical to: No other components

Dependencies: FCS_TTTC_EXT.1 Thru-Traffic TLS Inspection Client Protocol

FCS_TTTC_EXT.4.1 The TSF shall support secure renegotiation on STIP TLS connections through use of the “renegotiation_info” TLS extension in accordance with RFC 5746.

FCS_TTTC_EXT.4.2 The TSF shall include [*selection, choose only one of: renegotiation_info extension, TLS_EMPTY_RENEGOTIATION_INFO_SCSV cipher suite*] in the Client Hello message.

FCS_TTTC_EXT.4.3 The TSF shall ensure that renegotiation is performed before [*selection: [assignment: renegotiation rules], 2^20 64-bit data blocks are encrypted using TDES cipher suites using the same key*].

FCS_TTTC_EXT.5 Thru-Traffic TLS Inspection Client Support for Supported Groups Extension

Hierarchical to: No other components

Dependencies: FCS_TTTC_EXT.1 Thru-Traffic TLS Inspection Client Protocol

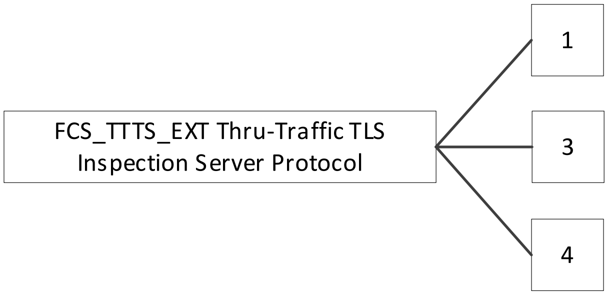
FCS_TTTC_EXT.5.1 The TSF shall present the Supported Groups Extension in the Client Hello with the supported groups [*assignment: list of permissible Supported Groups values*].

D.6 FCS_TTTS_EXT Thru-Traffic TLS Inspection Server Protocol

Family Behavior

Components in this family define requirements for the TOE’s ability to act as a TLS server for the purpose of reconstructing the original intended TLS connection that it is inserted into as a proxy.

Component Leveling



FCS_TTTS_EXT.1, Thru-Traffic TLS Inspection Server Protocol, defines the types of TLS server connections the TSF can support when acting as a proxy.

FCS_TTTS_EXT.3, Thru-Traffic TLS Inspection Server Protocol with Mutual Authentication of Monitored Clients, requires the TSF to validate a TLS client certificate when receiving a connection from a monitored client as part of establishing a TLS proxy connection.

FCS_TTTS_EXT.4, STIP Server-Side Support for Renegotiation, requires the TSF to support session renegotiation when acting as a TLS server for a proxy connection.

Management: FCS_TTTS_EXT.1

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

- Ability to configure the cryptographic functionality.

Management: FCS_TTTS_EXT.3, FCS_TTTS_EXT.4

No specific management functions are identified.

Audit: FCS_TTTS_EXT.1

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Establishment of TLS session.

Audit: FCS_TTTS_EXT.3

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Mutual authentication required and valid client certificate received.
- Mutual authentication not used.

Audit: FCS_TTTS_EXT.4

There are no auditable events foreseen.

FCS_TTTS_EXT.1 Thru-Traffic TLS Inspection Server Protocol

Hierarchical to: No other components

Dependencies: FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.2 Cryptographic Key Distribution

FCS_COP.1 Cryptographic Operation

FCS_RBG_EXT.1 Random Bit Generation

FCS_TTTC_EXT.1 Thru-Traffic TLS Inspection Client Protocol

FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.2 X.509 Certificate Authentication

FCS_TTTS_EXT.1.1 The TSF shall implement [*assignment: TLS versions*] as a server to the monitored client that supports the following cipher suites: [*assignment: list of cipher suites and reference to RFC in which each is defined*] and no other cipher suites, and also supports functionality for [*selection:*

- *mutual authentication,*
- *session renegotiation,*
- *none*

].

FCS_TTTS_EXT.1.2 The TSF shall deny connections from clients requesting [*assignment: unsupported TLS versions*] for through-traffic processing.

FCS_TTTS_EXT.1.3 The TSF shall perform key establishment for TLS with a monitored client using [*assignment: supported key establishment parameter types and key sizes/identifiers, based on the claimed cipher suites in FCS_TTTS_EXT.1.1*].

FCS_TTTS_EXT.3 Thru-Traffic TLS Inspection Server Protocol with Mutual Authentication of Monitored Clients

Hierarchical to: No other components

Dependencies: FCS_TTTS_EXT.1 Thru-Traffic TLS Inspection Server Protocol

FDP_TEP_EXT.1 SSL/TLS Inspection Proxy Policy

FCS_TTTS_EXT.3.1 The TSF shall support mutual authentication of TLS clients using X.509v3 certificates.

FCS_TTTS_EXT.3.2 The TSF shall send a Certificate Request message to the TLS client when mutual authentication is required by the configured TLS session establishment policy as defined in FDP_TEP_EXT.1.

FCS_TTTS_EXT.3.3 The TSF shall validate the certificate presented by the client and [*selection: allow the connection if the certificate is invalid and an exception is permitted for the client, terminate the connection if the certificate is invalid*].

FCS_TTTS_EXT.3.4 The TSF shall not establish a TLS session if the distinguished name (DN) or Subject Alternative Name (SAN) contained in a certificate does not match the expected identifier for the client.

FCS_TTTS_EXT.4 STIP Server-Side Support for Renegotiation

Hierarchical to:	No other components
Dependencies:	FCS_TTTS_EXT.1 Thru-Traffic TLS Inspection Server Protocol

FCS_TTTS_EXT.4.1 The TSF shall support the "renegotiation_info" TLS extension in accordance with RFC 5746.

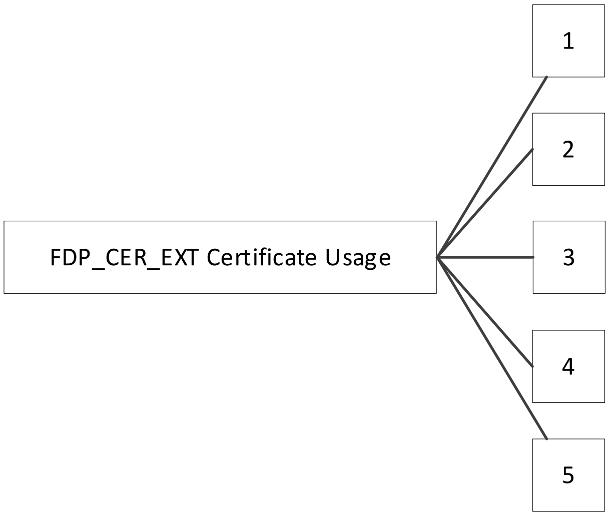
FCS_TTTS_EXT.4.2 The TSF shall include the renegotiation_info extension in Server Hello messages.

D.7 FDP_CER_EXT Certificate Usage

Family Behavior

Components in this family define requirements for the TOE's ability to issue certificates that allow the TOE to act as a proxy between remote entities attempting to establish a TLS connection with one another.

Component Leveling



FDP_CER_EXT.1, Certificate Profiles for Server Certificates, requires the TSF to implement a certificate profile function and to issue TLS server certificates that conform to profiles when acting as a CA.

FDP_CER_EXT.2, Certificate Request Matching of Server Certificates, requires the TSF to maintain a linkage between external certificates that it has validated and internal certificates that it has issued to represent the entities presenting those certificates when the TOE is acting as a proxy for a TLS connection to or from those entities.

FDP_CER_EXT.3, Certificate Issuance Rules for Server Certificates, requires the TSF to issue certificates in response to validated server certificates based on certain rules.

FDP_CER_EXT.4, Certificate Profiles for Client Certificates, requires the TSF to implement a certificate profile function and to issue TLS client certificates that conform to profiles when acting as a CA.

FDP_CER_EXT.5, Certificate Issuance Rules for Client Certificates, requires the TSF to issue certificates in response to validated client certificates based on certain rules.

Management: FDP_CER_EXT.1

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

- Ability to configure identifying information for the TOE's embedded CA.
- Ability to configure a maximum certificate validity duration.
- Ability to configure and manage certificate profiles.

Management: FDP_CER_EXT.2

No specific management functions are identified.

Management: FDP_CER_EXT.3

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

- Ability to configure rules for automated issuance of certificates.

Management: FDP_CER_EXT.4

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

- Ability to configure identifying information for the TOE's embedded CA.
- Ability to configure a maximum certificate validity duration.
- Ability to configure and manage certificate profiles.

Management: FDP_CER_EXT.5

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

- Ability to configure rules for automated issuance of certificates.

Audit: FDP_CER_EXT.1

There are no auditable events foreseen.

Audit: FDP_CER_EXT.2

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Linking of issued certificate to validated certificate.

Audit: FDP_CER_EXT.3

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Certificate generation.

Audit: FDP_CER_EXT.4

There are no auditable events foreseen.

Audit: FDP_CER_EXT.5

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Certificate generation.

FDP_CER_EXT.1 Certificate Profiles for Server Certificates

Hierarchical to: No other components

Dependencies: FCS_CKM.1 Cryptographic Key Generation

FCS_COP.1 Cryptographic Operation

FMT_SMR.1 Security Roles

FDP_CER_EXT.1.1 The TSF shall implement a certificate profile function for TLS server certificates issued by a CA embedded within the TOE, and shall ensure that issued certificates are consistent with configured profiles.

FDP_CER_EXT.1.2 The TSF shall generate certificates using profiles that comply with requirements for certificates as specified in IETF RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" as refined below. At a minimum, the TSF shall ensure that:

a) The version field shall contain the integer 2.
b) The issuerUniqueID or subjectUniqueID fields are not populated.
c) The serialNumber shall be unique with respect to the issuing Certification Authority.
d) The validity field shall specify a notBefore value that does not precede the current time and a notAfter value that does not precede the value specified in notBefore.
e) The issuer field is not empty and is populated with the [*assignment: authorized role(s)*]-configured CA name.
f) The signature field and the algorithm in the subjectPublicKeyInfo field shall contain the OID for a signature algorithm specified in FCS_COP.1.
g) The following extensions are supported:
   f. authorityKeyIdentifier
   g. keyUsage
   h. extendedKeyUsage
   i. certificatePolicy
   j. [*selection: subjectKeyIdentifier, basicConstraints, cRLDistributionPoints, authorityInfoAccess, no other extensions*]
h) A subject field containing a null Name (e.g., a sequence of zero relative distinguished names) is accompanied by a populated critical subjectAltName extension.
i) The authorityKeyIdentifier extension in any certificate issued by the TOE must be populated and must be the same as the subjectKeyIdentifier extension contained in the TOE's embedded CA's signing certificate.

j) Populated keyUsage and extendedKeyUsage fields in the same certificate shall contain consistent values reflecting exclusive TLS server use as follows:

keyUsage	**extendedKeyUsage**
digitalSignature	serverAuth
digital Signature, keyEncipherment	serverAuth
digital Signature, keyAgreement	serverAuth

l) [*selection: The subjectKeyIdentifier extension is populated with a value unique for each public key contained in a certificate issued by the TSF, no other constraints*].

FDP_CER_EXT.1.3 The TSF shall implement the following rules for populating certificate fields based on constraints imposed by the TOE's embedded CA's signing certificate:

- The validity field shall specify a notAfter time that does not exceed the notAfter time of the CA's signing certificate.
- The issuer field identifies the [*selection: subject, [assignment: [assignment: authorized role(s)] assigned identifying information]*] of the CA's signing certificate.
- [*selection:*
  - *The subject name is limited by name constraints specified in the CA's signing certificate,*
  - *[assignment: list of rules],*
  - *no other rules*].

FDP_CER_EXT.1.4 The TSF shall implement the following rules for populating certificate fields based on the validated certificate and constraints imposed by the [*assignment: authorized role(s)*]:

a) The Subject/Subject Alternative Name shall be copied from validated server certificate.

b) The notBefore field shall not precede the notBefore field of the validated server certificate.

c) The notAfter field shall not exceed the notAfter field of the validated server certificate.

d) The notAfter field shall not exceed the current time by more than a maximum validity duration value as configured by a [*assignment: authorized role(s)*] user.

e) If the basicConstraints field is configured to be present, it shall be populated with the value cA=False.

f) The subject public key shall be generated in accordance with FCS_CKM.1.1.

g) [*selection:*

- *policy OID/policy mapping fields are populated in accordance with [assignment: a [assignment: authorized role(s)] configured mapping from validated server certificate values to one or more stated policy OIDs]*
- *[assignment: list of rules]*
- *no additional rules*].

FDP_CER_EXT.2 Certificate Request Matching of Server Certificates

Hierarchical to: No other components

Dependencies: FDP_CER_EXT.1 Certificate Profiles for Server Certificates

FDP_CER_EXT.2.1 The TSF shall establish and record a linkage from validated certificates to issued certificates.

FDP_CER_EXT.3 Certificate Issuance Rules for Server Certificates

Hierarchical to: No other components

Dependencies: FDP_CER_EXT.1 Certificate Profiles for Server Certificates

FDP_CER_EXT.3.1 The TSF shall issue certificates in response to a validated server certificate according to the following rules: The issued certificate is in compliance with a current certificate profile defined in accordance with FDP_CER_EXT.1 and

- The TLS session establishment policy is configured to allow inspection of TLS sessions between monitored clients and a requested server authenticated to the TSF by the validated certificate,

[*selection:*

- *A valid certificate for the same subject is not present in cache,*
- *The embedded CA certificate's name space allows issuance of a certificate that represents the authenticated server*].

FDP_CER_EXT.3.2 The TSF shall reject all certificate requests originating external to the TOE.

FDP_CER_EXT.4 Certificate Profiles for Client Certificates

Hierarchical to: No other components

Dependencies: FCS_COP.1 Cryptographic Operation

FMT_SMR.1 Security Roles

FDP_CER_EXT.4.1 The TSF shall implement a certificate profile function for TLS client certificates issued by a CA embedded within the TOE, and shall ensure that issued certificates are consistent with configured profiles.

FDP_CER_EXT.4.2 The TSF shall generate certificates representing monitored clients using profiles that comply with requirements for certificates as specified in IETF RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" as refined below. At a minimum, the TSF shall ensure that:

a) The version field shall contain the integer 2.
b) The issuerUniqueID or subjectUniqueID fields are not populated.
c) The serialNumber shall be unique with respect to the issuing Certification Authority.
d) The validity field shall specify a notBefore value that does not precede the current time and a notAfter value that does not precede the value specified in notBefore.
e) The issuer field is not empty and is populated with the [*assignment: authorized role(s)f*]-configured CA name.
f) The signature field and the algorithm in the subjectPublicKeyInfo field shall contain the OID for a signature algorithm specified in FCS_COP.1.
g) The following extensions are supported:
   g. subjectKeyIdentifier
   h. authorityKeyIdentifier
   i. keyUsage
   j. extendedKeyUsage
   k. certificatePolicy
   l. [*selection: basicConstraints, cRLDistributionPoints, authorityInfoAccess, no other extensions*]
h) A subject field containing a null Name (e.g., a sequence of zero relative distinguished names) is accompanied by a populated critical subjectAltName extension.
i) The subjectKeyIdentifier extension is populated with a value unique for each public key contained in a certificate issued by the TSF.
j) The authorityKeyIdentifier extension in any certificate issued by the TOE must be populated and must be the same as the subjectKeyIdentifier extension contained in the TOE's embedded CA's signing certificate.
k) Populated keyUsage and extendedKeyUsage fields in the same certificate shall contain consistent values reflecting exclusive TLS server use as follows:

keyUsage	extendedKeyUsage
digitalSignature	clientAuth
digital Signature, keyEncipherment	clientAuth
digital Signature, keyAgreement	clientAuth

FDP_CER_EXT.4.3 The TSF shall implement the following rules for populating certificate fields based on constraints imposed by the TOE's embedded CA's signing certificate:

- The validity field shall specify a notAfter time that does not exceed the notAfter time of the CA's signing certificate
- The issuer field identifies the [*selection: subject, [assignment: [authorized role(s)] assigned identifying information]*] of the CA's signing certificate.
- [*selection:*

- o *The subject name is limited by name constraints specified in the CA's signing certificate,*
- o *[assignment: list of rules],*
- o *no other rules*].

FDP_CER_EXT.4.4 The TSF shall implement the following rules for populating certificate fields based on the validated certificate and constraints imposed by the [*assignment: authorized role(s)*]:

a) The Subject/Subject Alternative Name shall be copied from validated client certificate;
b) The notBefore field shall not precede the notBefore field of the validated client certificate
c) The notAfter field shall not exceed the notAfter field of the validated client certificate,
d) The notAfter field shall not exceed the current time by more than a maximum validity duration value as configured by a [*assignment: authorized role(s)*] user,
e) If the basicConstraints field is configured to be present, it shall be populated with the value cA=False.
f) If configured to be present, the policy OID and policy mapping fields shall be populated according to [*selection:*
   - *a [assignment: authorized role(s)] configured mapping from validated client certificate values to one or more stated policy OIDs]*
   - [*assignment: list of rules*].

FDP_CER_EXT.5 Certificate Issuance Rules for Client Certificates

Hierarchical to: No other components

Dependencies: FDP_CER_EXT.4 Certificate Profiles for Client Certificates

FDP_CER_EXT.5.1 The TSF shall issue certificates in response to a validated client certificate according to the following rules: The issued certificate is in compliance with a current certificate profile defined in accordance with FDP_CER_EXT.4 and

- The TLS session establishment policy is configured to allow inspection of TLS sessions with mutual authentication between the monitored client whose certificate is validated by the TSF and one or more requested servers,
- The specific requested server includes a Certificate Request message in the TLS handshake,

[*selection:*

- *A valid certificate for the same subject is not present in cache,*
- *The embedded CA certificate's name space allows issuance of a certificate that represents the authenticated client,*

- *No other constraints*].

FDP_CER_EXT.5.2 The TSF shall reject all certificate requests originating external to the TOE.

D.8 FDP_CRL_EXT Certificate Revocation List

Family Behavior

Components in this family define requirements for the usage of certificate revocation lists (CRLs) as a method of recording certificate status information.

Component Leveling

FDP_CRL_EXT Certificate Revocation List
1

FDP_CRL_EXT.1, Certificate Revocation List Generation, requires the TSF to include specific information in any certificate revocation lists that it creates.

Management: FDP_CRL_EXT.1

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

- Ability to modify the CRL configuration.

Audit: FDP_CRL_EXT.1

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Failure to generate CRL.

FDP_CRL_EXT.1 Certificate Revocation List Generation

Hierarchical to: No other components

Dependencies: FCS_COP.1 Cryptographic Operation

FDP_CSI_EXT.1 Certificate Status Information

FDP_CRL_EXT.1.1 When the TSF is configured to generate CRLs, the TSF shall verify that all mandatory fields in any generated CRL contains values in accordance with ITU-T Recommendation X.509. At a minimum, the following items shall be validated:

a) If the version field is present, then it shall contain a 1.
b) If the CRL contains any critical extensions, then the version field shall be present and contain the integer 1.
c) The [*selection: issuer, issuerAltName*] fields shall indicate the configured name of the CA.
d) If the issuer field contains a null Name (e.g., a sequence of zero relative distinguished names), then the CRL shall contain a critical issuerAltName extension.

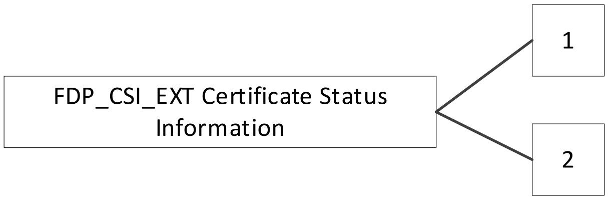
e) The signature and signatureAlgorithm fields shall contain the OID for a digital signature algorithm in accordance with FCS_COP.1.
f) The thisUpdate field shall indicate the issue date of the CRL.
g) The time specified in the nextUpdate field (if populated) shall not precede the time specified in the thisUpdate field.

D.9 FDP_CSI_EXT Certificate Status Information

Family Behavior

Components in this family define requirements for the TOE's ability to generate certificate status information and to modify the status of issued certificates.

Component Leveling



FDP_CSI_EXT.1, Certificate Status Information, requires the TSF to generate certificate status information using a supported method and to define conditions in which this information can be modified.

FDP_CSI_EXT.2, Certificate Status Information for Client Certificates, requires the TSF to generate certificate status information for client certificates (e.g. for mutually-authenticated TLS) using a supported method and to define conditions in which this information can be modified.

Management: FDP_CSI_EXT.1, FDP_CSI_EXT.2

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

- Ability to revoke issued certificates.
- Ability to configure certificate status services.
- Ability to configure automated process used to approve the revocation of a certificate or information about the revocation of a certificate.
- Ability to clear a cache of valid issued certificates.

Management: FDP_CSI_EXT.2

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

- Ability to revoke issued certificates.
- Ability to configure certificate status services.
- Ability to configure automated process used to approve the revocation of a certificate or information about the revocation of a certificate.
- Ability to clear a cache of valid issued certificates.

FDP_CSI_EXT.1 Certificate Status Information

Hierarchical to: No other components

Dependencies: [FDP_CRL_EXT.1 Certificate Revocation List Generation OR

FDP_OCSP_EXT.1 OCSP Basic Response Generation]

FDP_OCSPS_EXT.1 OCSP Stapling

FMT_SMR.1 Security Roles

FDP_CSI_EXT.1.1 The TSF shall generate certificate status information whose format complies with [*selection: ITU-T Recommendation X.509v2 CRL, the OCSP standard as defined by RFC 6960*].

FDP_CSI_EXT.1.2 The TSF shall support changes to the status of a certificate by [*selection: [assignment: authorized role(s)], [assignment: automated revocation rules]*].

FDP_CSI_EXT.1.3 The TSF shall [*selection: provide, interface with the Operational Environment to provide*] certificate status information generated in accordance with FDP_CSI_EXT.1.1 via [*selection: posting CRLs at the location specified in the cRLDistributionPoints of the issued certificate, an OCSP mechanism indicated in the authorityInfoAccess extension of the issued certificate, OCSP Stapling in accordance with FDP_OCSPS_EXT.1*].

FDP_CSI_EXT.2 Certificate Status Information for Client Certificates

Hierarchical to: No other components

Dependencies: FDP_CER_EXT.4 Certificate Profiles for Client Certificates

FDP_CSI_EXT.1 Certificate Status Information

[FDP_CRL_EXT.1 Certificate Revocation List Generation OR

FDP_OCSP_EXT.1 OCSP Basic Response Generation]

FDP_OCSPS_EXT.1 OCSP Stapling

FMT_SMR.1 Security Roles

FDP_CSI_EXT.2.1 The TSF shall generate certificate status information for issued client certificates whose format complies with [*ITU-T Recommendation X.509v2 CRL, the OCSP standard as defined by RFC 6960*].

FDP_CSI_EXT.2.2 The TSF shall support changes to the status of a certificate in accordance with the following rules:

- as directed by [*assignment: authorized role(s)*] and
- [*selection:*
  - *a certificate in cache is revoked when a certificate representing the same subject is received for client authentication and either*
    - *the validation of the received certificate fails or*
    - *the validation of the received certificate passes and the certificate fields of the validated certificate would result in a different*

certificate being issued under the current profile in accordance with FDP_CER_EXT.4;

- *[assignment: other rules for revocation of issued certificates];*
- *no other rules*].

FDP_CSI_EXT.2.3 The TSF shall [*selection: provide, interface with the Operational Environment to provide*] certificate status information generated in accordance with FDP_CSI_EXT.2.1 via [*selection: posting CRLs at the location specified in the cRLDistributionPoints of the issued certificate, an OCSP mechanism indicated in the authorityInfoAccess extension of the issued certificate*].

D.10 FDP_CSIR_EXT Certificate Status Information Required

Family Behavior

Components in this family define requirements for the association of certificate status information with certificates issued by the TOE.

Component Leveling

FDP_CSIR_EXT.1, Certificate Status Information Required, requires the TSF to maintain certificate status information for its issued certificates or to ensure that any certificates it issues are valid for a sufficiently short period of time that status information is unnecessary.

Management: FDP_CSIR_EXT.1

No specific management functions are identified.

Audit: FDP_CSIR_EXT.1

There are no auditable events foreseen.

FDP_CSIR_EXT.1 Certificate Status Information Required

Hierarchical to: No other components

Dependencies: FDP_CER_EXT.1 Certificate Profiles for Server Certificates

FDP_CER_EXT.3 Certificate Issuance Rules for Server Certificates

FDP_CSIR_EXT.1.1 The TSF shall [*selection: generate certificate status information, only issue certificates with validity period of less than [assignment: length of time]*].

D.11 FDP_OCSP_EXT Online Certificate Status Protocol

Family Behavior

Components in this family define requirements for the usage of the Online Certificate Status Protocol (OCSP) as a method of recording certificate status information.

Component Leveling

FDP_OCSP_EXT Online Certificate Status Protocol
1

FDP_OCSP_EXT.1, OCSP Basic Response Generation, requires the TSF to include specific information in any OCSP response that it creates.

Management: FDP_OCSP_EXT.1

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

- Ability to modify the OCSP configuration.

Audit: FDP_OCSP_EXT.1

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Failure to generate certificate status information

FDP_OCSP_EXT.1 OCSP Basic Response Generation

Hierarchical to: No other components

Dependencies: FCS_COP.1 Cryptographic Support

FDP_CSI_EXT.1 Certificate Status Information

FDP_OCSP_EXT.1.1 When the TSF is configured to generate OCSP responses of the basic response type, the TSF shall ensure that all mandatory fields in the OCSP basic response contain values in accordance with RFC 6960. At a minimum, the following items shall be validated:

a) The version field shall contain a 0.
b) The signatureAlgorithm field shall contain the object identifier (OID) for a digital signature algorithm in accordance with FCS_COP.1.
c) The thisUpdate field shall indicate the time at which the status being indicated is known to be correct.
d) The producedAt field shall indicate the time at which the OCSP responder signed the response.
e) The time specified in the nextUpdate field (if populated) shall not precede the time specified in the thisUpdate field.

D.12 FDP_OCSPS_EXT Online Certificate Status Protocol Stapling

Family Behavior

Components in this family define requirements for the usage of OCSP stapling as a method of communicating certificate revocation status information.

Component Leveling

FDP_OCSPS_EXT.1, OCSP Stapling, requires the TSF to perform OCSP Stapling by including OCSP response information in a TLS Certificate Status Message.

Management: FDP_OCSPS_EXT.1

No specific management functions are identified.

Audit: FDP_OCSPS_EXT.1

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Failure to include certificate status information in TLS handshake message

FDP_OCSPS_EXT.1 OCSP Stapling

Hierarchical to: No other components

Dependencies: FDP_OCSP_EXT.1 OCSP Basic Response Generation

FDP_OCSPS_EXT.1.1 The TSF shall be able to process [*selection: Certificate Status Request extension in accordance with RFC 6066 section 8, Certificate Status Request List V2 in accordance with RFC 6961*].

FDP_OCSPS_EXT.1.2 The TSF shall [*selection: generate OCSP response information in accordance with FDP_OCSP_EXT.1, interface with an OCSP provider to obtain an OCSP response*] and populate a Certificate Status Message in accordance with RFC 6066.

D.13 FDP_PIN_EXT Certificate Pinning

Family Behavior

Components in this family define requirements for implementation of certificate pinning.

Component Leveling

FDP_PIN_EXT.1, Certificate Pinning, requires the TSF to have the ability to associate certificate information with external servers and to take some action if one of these servers identifies itself using an unknown certificate.

Management: FDP_PIN_EXT.1

No specific management functions are identified.

Audit: FDP_PIN_EXT.1

There are no auditable events foreseen.

FDP_PIN_EXT.1 Certificate Pinning

Hierarchical to: No other components

Dependencies: FMT_SMR.1 Security Roles

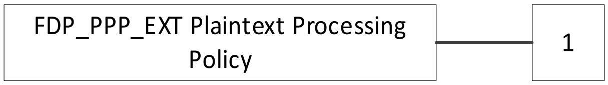
FDP_PIN_EXT.1.1 The TSF shall be able to detect and [*selection: alert, [assignment: perform a [assignment: authorized role(s) managed action]*] to changes in the [*selection: public key, certificate, certificate issuer*] used by requested servers according to [*assignment: characteristics of servers used for association between certificates and servers*].

D.14 FDP_PPP_EXT Plaintext Processing Policy

Family Behavior

Components in this family define requirements for the processing of plaintext data that has been decrypted from TLS.

Component Leveling



FDP_PPP_EXT.1, Plaintext Processing Policy, requires the TSF to apply rules to decrypted TLS traffic and take some information flow processing action against the traffic based on these rules.

Management: FDP_PPP_EXT.1

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

- Ability to manage inspection policy.

Audit: FDP_PPP_EXT.1

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Configuration changes to the plaintext processing policy.

FDP_PPP_EXT.1 Plaintext Processing Policy

Hierarchical to: No other components

Dependencies: FCS_TTTC_EXT.1 Thru-Traffic TLS Inspection Client Protocol

FCS_TTTS_EXT.1 Thru-Traffic TLS Inspection Server Protocol

FDP_PPP_EXT.1.1 The TSF shall enforce the TLS plaintext processing policy on information flows containing plaintext produced by inspection processing of the TOE between TLS session termination points and [*selection: distinct internal inspection processing functional components, internal inspection processing functional components and an interface to external inspection processing environment*].

FDP_PPP_EXT.1.2 The TSF shall allow the definition of TLS plaintext processing policy rules using [*assignment: entity attributes of the requested server*], [*assignment: indicators of inspection processing results*] and distinct interfaces.

FDP_PPP_EXT.1.3 The TSF shall allow the following operations to be associated with the plaintext processing policy: permit, block, and [*selection: bypass, no other operation*], with the capability to log the operation.

FDP_PPP_EXT.1.4 The TSF shall allow the Plaintext Processing Policy to be applied at each information flow control point between inspection processing functional components, including any network interface used to support external inspection processing.

FDP_PPP_EXT.1.5 The TSF shall

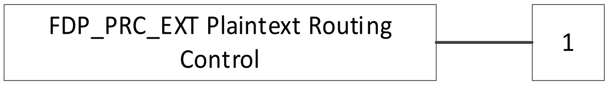
- drop Information flows between inspection processing components, including any interface to external inspection processing components, that cannot be associated to an existing TLS session thread.
- inform the TLS session establishment policy of the TLS session thread associated to any information flow that is blocked by the plaintext processing policy.

D.15 FDP_PRC_EXT Plaintext Routing Control

Family Behavior

Components in this family define requirements for the routing of decrypted TLS traffic.

Component Leveling



FDP_PRC_EXT.1, Plaintext Routing Control, requires the TSF to route decrypted TLS traffic based on the results of applicable plaintext processing policy rules.

Management: FDP_PRC_EXT.1

No specific management functions are identified.

Audit: FDP_PRC_EXT.1

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Plaintext routed to inspection processing functional component.

FDP_PRC_EXT.1 Plaintext Routing Control

Hierarchical to: No other components

Dependencies: FDP_PPP_EXT.1 Plaintext Processing Policy

FDP_PRC_EXT.1.1 The TSF shall control the routing of information flows containing plaintext within a TLS session thread in accordance with the configured Plaintext Processing Policy identified in FDP_PPP_EXT.1.

FDP_PRC_EXT.1.2 The TSF shall separate information flows containing plaintext within different TLS session threads.

FDP_PRC_EXT.1.3 The TSF shall not expose plaintext within a TLS session thread except to inspection processing functional components identified in, and as authorized by the configured Plaintext Processing Policy, as described in FDP_PPP_EXT.1.

D.16 FDP_STG_EXT User Data Storage

Family Behavior

Components in this family define requirements for the secure storage of public key and certificate data used by the TOE.

Component Leveling

FDP_STG_EXT User Data Storage
1

FDP_STG_EXT.1, Certificate Data Storage, requires the TSF to protect public key and certificate data using either access controlled storage or a cryptographic integrity mechanism.

Management: FDP_STG_EXT.1

No specific management functions are identified.

Audit: FDP_STG_EXT.1

There are no auditable events foreseen.

FDP_STG_EXT.1 Certificate Data Storage

Hierarchical to: No other components

Dependencies: FCS_CKM_EXT.5 Public Key Integrity

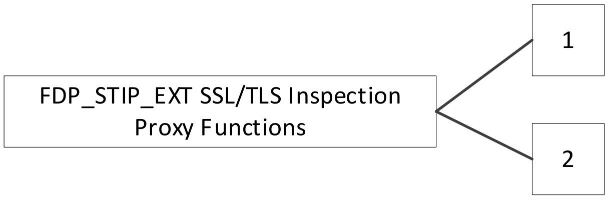
FDP_STG_EXT.1.1 The TSF shall use [*selection: access controlled storage, an integrity mechanism*] to protect the trusted public keys and certificates (trust store elements) used to validate local logon, trusted channel, and external communication to the STIP.

D.17 FDP_STIP_EXT SSL/TLS Inspection Proxy Functions

Family Behavior

Components in this family define requirements for the TOE to act as a man-in-the-middle for SSL/TLS connections by establishing two separate TLS connections between itself and the endpoints of the original connection.

Component Leveling



FDP_STIP_EXT.1, SSL/TLS Inspection Proxy Functions, requires the TSF to establish itself as a proxy for SSL/TLS connections between remote endpoints such that the TOE can observe the contents of the SSL/TLS traffic.

FDP_STIP_EXT.2, Mutual Authentication Inspection Operation, defines the ability of the TSF to act as an SSL/TLS inspection proxy for mutually authenticated SSL/TLS sessions.

Management: FDP_STIP_EXT.1

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

- Ability to configure inspection processing.
- Ability to configure TLS error responses for monitored clients.

Management: FDP_STIP_EXT.2

No specific management functions are identified.

Audit: FDP_STIP_EXT.1

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Establishment of a TLS inspection session thread.
- Establishment of an encrypted TLS data flow.
- Execution of Block operation.
- Bypass operation invoked.
- Block operation invoked.

Audit: FDP_STIP_EXT.2

There are no auditable events foreseen.

FDP_STIP_EXT.1 SSL/TLS Inspection Proxy Functions

Hierarchical to: No other components

Dependencies: FCS_TTTC_EXT.1 Thru-Traffic TLS Inspection Client Protocol

FCS_TTTS_EXT.1 Thru-Traffic TLS Inspection Server Protocol

FDP_PPP_EXT.1 Plaintext Processing Policy

FDP_PRC_EXT.1 Plaintext Routing Control

FTA_TAB.1 Default TOE Access Banners

FDP_STIP_EXT.1.1 The TSF shall be capable of performing the Inspection Operation consisting of establishing a TLS session between TOE and the requested server according to FCS_TTTC_EXT.1, establishing a TLS session between the monitored client and the TOE according to FCS_TTTS_EXT.1, and routing decrypted application data from either of these TLS sessions to or between inspection processing functional components within the TOE, or between the TOE and external inspection processing functional components to a unique TLS session thread, according to FDP_PPP_EXT.1 and FDP_PRC_EXT.1.

FDP_STIP_EXT.1.2 The TSF shall obtain a certificate from the TOE CA that represents the requested server for establishment of the TLS session with the monitored client when performing an inspect operation.

FDP_STIP_EXT.1.3 The TSF shall [*selection*:

- *require administrator confirmation of consent,*
- *provide a consent to monitor banner to the client, in accordance with FTA_TAB.1, and receive an affirmative response*]

prior to sending decrypted TLS application data from a monitored client to inspection processing functional component as part of an inspection operation.

FDP_STIP_EXT.1.4 The TSF shall provide the Bypass operation functionality by forwarding traffic between the monitored client and requested server such that monitored client can establish and maintain a TLS connection to the requested server.

FDP_STIP_EXT.1.5 When initiating a Block operation, the TSF shall be capable of providing a [*selection: TLS error response, [assignment: other error message]*] to the monitored client associated with the blocked TLS session.

FDP_STIP_EXT.2 Mutual Authentication Inspection Operation

Hierarchical to: No other components

Dependencies: FDP_STIP_EXT.1 SSL/TLS Inspection Proxy Functions

FDP_CER_EXT.5 Certificate Issuance Rules for Client Certificates

FDP_STIP_EXT.2.1 The TSF shall be capable of providing mutual authentication of the monitored client to a requested server when performing the inspection operation when mutual authentication is allowed for the requested server by the configured policy, and the TLS handshake with the requested server includes a certificate request.

FDP_STIP_EXT.2.2 After receiving the TLS client certificate from the monitored client, the TSF shall be able to generate a certificate representing the client in accordance with

FDP_CER_EXT.5 and [*selection: obtain a valid certificate representing the client from cache, no other method*] matching the current certificate profile.

FDP_STIP_EXT.2.3 After obtaining a certificate representing the monitored client, the TSF shall send the client certificate and certificate verify messages to the requested server.

D.18 FDP_TEP_EXT TLS Establishment Policy

Family Behavior

Components in this family define requirements for SSL/TLS inspection proxy functions.

Component Leveling

FDP_TEP_EXT.1, SSL/TLS Inspection Proxy Policy, requires the TSF perform SSL/TLS inspection and enforce SSL/TLS inspection proxy rules that define how SSL/TLS traffic received by the TOE is decrypted, inspected, re-encrypted, forwarded, discarded, or logged, depending on the applicable rules.

Management: FDP_TEP_EXT.1

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

- Ability to manage inspection policy.
- Ability to configure TLS error responses for monitored clients.

Audit: FDP_TEP_EXT.1

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- Mutual authentication authorized.

FDP_TEP_EXT.1 SSL/TLS Inspection Proxy Policy

Hierarchical to: No other components

Dependencies: FCS_TTTC_EXT.1 Thru-Traffic TLS Inspection Client Protocol

FCS_TTTC_EXT.3 Thru-Traffic TLS Inspection Client Protocol with Mutual Authentication Representing Monitored Clients

FCS_TTTC_EXT.5 Thru-Traffic TLS Inspection Client Support for Supported Groups Extension

FCS_TTTS_EXT.1 Thru-Traffic TLS Inspection Server Protocol

FCS_TTTS_EXT.3 Thru-Traffic TLS Inspection Server Protocol with Mutual Authentication of Monitored Clients

FDP_PPP_EXT.1 Plaintext Processing Policy

FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.2 X.509 Certificate Authentication

FDP_TEP_EXT.1.1 The TSF shall perform SSL/TLS Inspection Proxy functions and enforce SSL/TLS Inspection Proxy rules on TLS traffic received by the TSF from monitored clients and servers requested by monitored clients, and on TLS traffic controlled by the TSF to be sent to monitored clients and servers requested by monitored clients.

FDP_TEP_EXT.1.2 The TSF shall allow the definition of SSL/TLS Inspection Proxy rules based on the following attributes of each monitored client and requested server: [*assignment: list of attributes associated with TLS connection endpoints or the traffic that is transmitted between them*].

FDP_TEP_EXT.1.3 The TSF shall allow the following operations to be associated with SSL/TLS Inspection Proxy rules: block, bypass, or inspect, with the capability to log the operation.

FDP_TEP_EXT.1.4 The TSF shall be able to define monitored clients, requested servers, and [*selection: specific client-server connections, no other abstractions*] in terms of the attributes associated with the SSL/TLS Inspection Proxy function.

FDP_TEP_EXT.1.5 The TSF shall be able to associate a monitored client, requested server, and [*selection: specific client-server connections, no other abstractions*] with the allowed TLS version or versions, TLS cipher suites (including TLS key exchange algorithms and key sizes), the supported groups per FCS_TTTC_EXT.5.1, and [*assignment: other TLS connection characteristics or attributes*] that shall be used when performing the SSL/TLS Inspection Proxy operations.

FDP_TEP_EXT.1.6 The TSF shall allow the SSL/TLS Inspection Proxy rules to be assigned to each distinct network interface.

FDP_TEP_EXT.1.7 The TSF shall perform a [*selection: block, bypass, mutual authentication inspection*] operation on the session when receiving a TLS certificate request message from the requested server when establishing the TLS in accordance with FCS_TTTC_EXT.1.

FDP_TEP_EXT.1.8 The TSF shall

- Block the connection if the monitored client does not support a TLS version, cipher suite, key exchange, and key size that are in its allowed set as defined in FDP_TEP_EXT.1.5;
- Block the connection if the requested server does not negotiate a TLS version, cipher suite, key exchange, and key size that are in its allowed set as defined in FDP_TEP_EXT.1.5;
- Either Block, or [*selection: require administrative approval to inspect or bypass, no other rule*] the connection if the requested server does not negotiate a TLS version, cipher suite, key exchange, and key size that are in the set proposed by the monitored client in its Client Hello message;

- Block or [*selection: inspect, bypass, no other rule*] the connection if TOE certificate processing indicates revocation information is not available for a requested server or [*selection: monitored client, no other entity*];
- Block or [*selection: bypass, no other rule*] a connection if TOE certificate processing indicates an uninterpretable critical extension is present in the certificate of a requested server.

FDP_TEP_EXT.1.9 The TSF shall enforce the following default SSL/TLS Inspection Proxy rules on all SSL/TLS network traffic received from interfaces associated with monitored clients and requested servers:

- The TSF shall drop and be capable of [*selection: counting, logging*] invalid TLS messages;
- The TSF shall drop and be capable of logging TLS Client Hello messages for which no valid client can be determined.
- The TSF shall drop a TLS Client Hello message for which no valid server attribute can be determined.
- The TSF shall drop and be capable of [*selection: counting, logging*] TLS messages other than a Client Hello if the message is not associated with an existing TLS session thread established via the inspection operation or a TLS encrypted data flow established via a bypass operation.
- The TSF shall terminate a TLS session thread if it receives a fatal TLS error message from the monitored client.
- The TSF shall attempt to [*assignment: corrective or reactive actions*] if it receives a fatal TLS error message on the TLS session to the requested server.
- The TSF shall terminate a TLS session thread established via the inspect operation, and terminate a TLS encrypted data flow established by the bypass operation, if the TSF receives no traffic from the associated monitored client for a configurable period.
- The TSF shall transition a TLS session thread state from inspect operation to block operation, when indicated to do so by the TLS plaintext processing policy.

FDP_TEP_EXT.1.10 The TSF shall block all connections for which an Inspection or Bypass operation is not defined.

D.19 FIA_ENR_EXT Certificate Enrollment

Family Behavior

Components in this family define requirements for generation of certificate requests.

Component Leveling

FIA_ENR_EXT.1, Certificate Enrollment, requires the TSF to support PKCS#10 or Enrollment over Secure Transport as a method of requesting a certificate from an external CA.

Management: FIA_ENR_EXT.1

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

- Ability to generate and export PKCS#10 messages.

Audit: FIA_ENR_EXT.1

There are no auditable events foreseen.

FIA_ENR_EXT.1 Certificate Enrollment

Hierarchical to: No other components

Dependencies: [FIA_ESTC_EXT.1 Enrollment over Secure Transport (EST) Client, or

FIA_X509_EXT.3 X.509 Certificate Requests]

FIA_ENR_EXT.1.1 The TSF shall be able to generate a certificate request to an external certification authority to receive a certificate for the TOE's embedded CA's signing key using [*selection:*

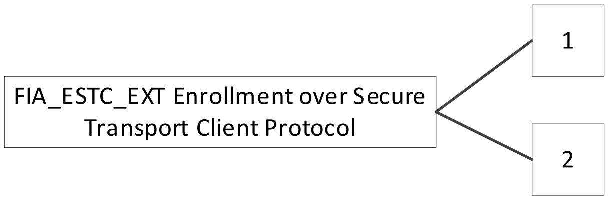
- *PKCS#10 in accordance with FIA_X509_EXT.3,*
- *Enrollment over Secure Transport (EST) in accordance with FIA_ESTC_EXT.1*].

D.20 FIA_ESTC_EXT Enrollment over Secure Transport Client Protocol

Family Behavior

Components in this family define requirements for the TOE's use of Enrollment over Secure Transport (EST) to obtain certificates from an external CA.

Component Leveling


FIA_ESTC_EXT Enrollment over Secure Transport Client Protocol
1
2

FIA_ESTC_EXT.1, Enrollment over Secure Transport (EST) Client, defines the ability of the TSF to perform Enrollment over Secure Transport (EST) as a client connecting to an external CA.

FIA_ESTC_EXT.2, EST Client Use of TLS-Unique Value, requires the TSF to generate tls-unique values as part of the EST process.

Management: FIA_ESTC_EXT.1

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

- Ability to generate and export EST messages.
- Ability to accept and process EST responses.

Management: FIA_ESTC_EXT.2

No specific management functions are identified.

Audit: FIA_ESTC_EXT.1

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- EST requests.

Audit: FIA_ESTC_EXT.2

There are no auditable events foreseen.

FIA_ESTC_EXT.1 Enrollment over Secure Transport (EST) Client

Hierarchical to: No other components

Dependencies: FCS_COP.1 Cryptographic Operation

[FCS_TLSC_EXT.1 TLS Client Protocol, or

FCS_TLSC_EXT.2 TLS Client Protocol with Authentication]

FIA_ENR_EXT.1 Certificate Enrollment

FIA_X509_EXT.1 X.509 Certificate Validation

FMT_SMR.1 Security Roles

FIA_ESTC_EXT.1.1 The TSF shall use the Enrollment over Secure Transport (EST) as specified in RFC 7030 to obtain its embedded CA certificate and [*assignment: other certificates for the TOE*] from an external certification authority (external CA) associated with an authorized EST server.

FIA_ESTC_EXT.1.2 The TSF shall be able to obtain EST server and CA certificates for authorized EST services via [*selection: implicit Trust Anchor/Trust Store (TA) configured by [assignment: authorized role(s)], an explicit TA populated via a TLS-authenticated EST CA certificate request in accordance with RFC 7030 section 4.1.2 and FCS_TLSC_EXT.1*].

FIA_ESTC_EXT.1.3 The TSF shall authenticate EST servers using X.509 certificates that chain to trust store elements from the [*selection: implicit Trust Anchor database, explicit Trust Anchor/Trust Store*] in accordance with FIA_X509_EXT.1 for all EST requests.

FIA_ESTC_EXT.1.4 The TSF shall authenticate its certificate enrollment requests to receive the signing certificate of its embedded CA and [*assignment: other certificates required to authenticate the TOE*], from an authorized EST server using [*selection*:

- *HTTP basic authentication transported over TLS in accordance with RFC* 7030 section 3.2.3 and FCS_TLSC_EXT.1;
- *HTTP digest authentication using a cryptographic hash algorithm in accordance with FCS_COP.1, transported over TLS in accordance with RFC 7030 section 3.2.3 and FCS_TLSC_EXT.1;*
- *Certificate-based authentication in accordance with RFC 7030 section 3.3.2 and FCS_TLSC_EXT.2 using [assignment: a pre-existing certificate authorized by the EST server]*].

FIA_ESTC_EXT.1.5 The TSF shall generate authenticated re-enrollment requests in accordance with RFC 7030 Section 3.3.2 and FCS_TLSC_EXT.1, using an existing valid certificate with the same subject name as the requested certificate and which was issued by the external CA.

FIA_ESTC_EXT.2 EST Client Use of TLS-Unique Value

Hierarchical to: No other components

Dependencies: FIA_ESTC_EXT.1 Enrollment over Secure Transport (EST) Client

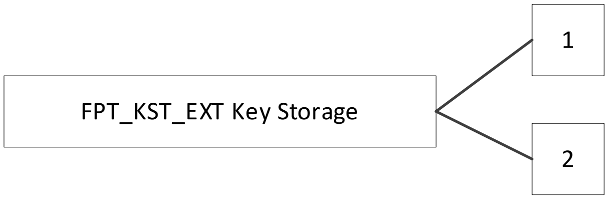
FIA_ESTC_EXT.2.1 The TSF shall generate tls-unique values and integrate them into EST requests it generates in accordance with RFC 7030 section 3.5.

D.21 FPT_KST_EXT Key Storage

Family Behavior

Components in this family define requirements for secure storage of keys and secrets used by the TOE.

Component Leveling



FPT_KST_EXT.1, No Plaintext Key Export, requires the TSF to prevent unauthorized disclosure of all TSF secret and private keys.

FPT_KST_EXT.2, TSF Key Protection, requires the TSF to prevent unauthorized usage of all TSF secret and private keys.

Management: FPT_KST_EXT.1, FPT_KST_EXT.2

No specific management functions are identified.

Audit: FPT_KST_EXT.1

There are no auditable events foreseen.

Audit: FPT_KST_EXT.2

The following actions should be auditable if FAU_GEN.1 Audit Data Generation is included in the PP/ST:

- All attempts to use the TOE’s embedded CA’s private signing keys.
- All attempts to use specified secret and private keys in the TOE’s key storage.

FPT_KST_EXT.1 No Plaintext Key Export

Hierarchical to: No other components

Dependencies: No dependencies

FPT_KST_EXT.1.1 The TSF shall prevent the plaintext export of [*assignment: list of all keys used by the TSF*].

FPT_KST_EXT.2 TSF Key Protection

Hierarchical to: No other components

Dependencies: No dependencies

FPT_KST_EXT.2.1 The TSF shall prevent unauthorized use of all TSF private and secret keys.

E. Entropy Documentation and Assessment

The TOE does not require any additional supplementary information to describe its entropy source(s) beyond the requirements outlined in the *Entropy Documentation and Assessment* section of the NDcPP. As with other NDcPP requirements, the only additional requirement is that the entropy documentation also applies to the capabilities of the TOE in addition to the base network device functionality.

F. References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017 • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017 • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017
[NDcPP]	collaborative Protection Profile for Network Devices, version 2.1, 24 September 2018

G. Acronyms

Acronym	Meaning
NIST	National Institute of Standards and Technology
TA	Trust Anchor/Trust Store
TOE	Target of Evaluation
TSF	TOE Security Functionality