collaborative Protection Profile for *Hardcopy Devices*

Acknowledgements

This collaborative Protection Profile (cPP) was developed by the Hardcopy Device international Technical Community (iTC) also known as HCD-iTC with representatives from industry, Government agencies, Common Criteria Test Laboratories, and members of academia.

INDUSTRY

Vendors

COMMON CRITERIA TESTING LABORATORIES

ITSEF Name

GOVERNMENT AGENCIES

Government Agency Names

Revision History

Table 1. Revision history

Version	Date	Description
0.6	8 June 2020	Initial Release for HCD iTC Review

Table of Contents

Preface

The technology type needs to be specified here, but the rest is boilerplate.

Objectives of Document

This document presents the Common Criteria (CC) collaborative Protection Profile (cPP) to express the security functional requirements (SFRs) and security assurance requirements (SARs) for *some technology type*. The Evaluation activities that specify the actions the evaluator performs to determine if a product satisfies the SFRs captured within this cPP, are described in [SD].

The rest of this section is boilerplate and should not need edits.

Scope of Document

The scope of the cPP within the development and evaluation process is described in the Common Criteria for Information Technology Security Evaluation. In particular, a cPP defines the IT security requirements of a generic type of TOE and specifies the functional security measures to be offered by that TOE to meet stated requirements [[CC1], Section B.14].

Intended Readership

The target audiences of this cPP are developers, CC consumers, system integrators, evaluators and schemes.

Although the cPP and SD may contain minor editorial errors, the cPP is recognized as living document and the iTC is dedicated to ongoing updates and revisions. Please report any issues to the HCD-iTC.

Related Documents

Edit the Supporting Document in the list.

- [CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017.
- [CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017.
- [CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.
- [CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1 Revision 5, April 2017.
- [SD] Supporting Document

For more see the Common Criteria Portal.

1. PP Introduction

1.1. PP Reference Identification

- PP Reference: collaborative Protection Profile for _Hardcopy Devices_
- PP Version: 0.6.2
- PP Date: 2020-07-14

1.2. TOE Overview

The Target of Evaluation in this PP is an HCD. HCDs support job functions to convert hardcopy documents into digital form (scanning), convert digital documents into hardcopy form (printing), duplicate hardcopy documents (copying), or transmit documents over a PSTN connection (PSTN faxing). Hardcopy documents typically take the form of paper, but can take other forms (e.g. transparencies).

For the purpose of this cPP, a conforming HCD must support at least one of the job functions printing, scanning, or copying and must support the functions network communications and administration.

The job functions supported by the HCD and the network communications and administration functions are “Required Uses” of a conforming HCD and are mandatory functions. A conforming HCD may also support “Conditionally Mandatory Uses”. Conditionally Mandatory Uses are optional functions, the presence of which in a HCD is not required for conformance, but which must meet conditionally mandatory requirements if they are present in a HCD

1.3. TOE Design

> This may not be necessary depending on the technology type. It may already be clear what the design is, or it is covered in the Overview. For example in the Network cPP there is an entire section dedicated to use case/design selections to deal with distributed TOEs.

1.4. TOE Use Case

1.4.1. USE CASE 1: Required Use Cases

The security-relevant use cases for Required Uses of a conforming HCD are:

1. One or more of the following:
    a. Printing: A Network User sends a Document from an External IT Entity to the HCD over a LAN with instructions for printing. The HCD has the capability to protect the User’s Document from unauthorized disclosure or alteration while it is in transit to the HCD, in Temporary Storage in the HCD, and before printed output is released to a User.
    b. Scanning: A Local User initiates scanning a Document on the HCD and the HCD sends the digital image to an External IT Entity. The HCD has the capability to protect the User’s Document from unauthorized disclosure or alteration while it is in Temporary Storage in the HCD and while it is in transit to the External IT Entity.
    c. Copying: A Local User scans a Document on the HCD and the HCD prints the Document. The HCD has the capability to protect the User’s Document from unauthorized disclosure and alteration while it is in Temporary Storage in the HCD.
2. Configuration: A Local or Network User with administrative privileges configures the security settings of the HCD. The HCD has the capability to assign Users to roles that distinguish Users

who can perform administrative functions from Users who can perform User functions. The HCD also has the capability to protect its security settings from unauthorized disclosure and alteration when they are stored in the HCD and in transit to or from an External IT Entity.

3. Auditing: Authorized personnel monitor security-relevant events in an audit log. The HCD generates audit log records when security-relevant events occur. It is mandatory that the HCD is able to securely transmit audit logs to an External IT Entity for storage, and the HCD has the capability to protect it from unauthorized disclosure or alteration while in transit to the External IT Entity.
4. Verifying software updates: Authorized personnel install updated software on the HCD. The HCD ensures that only authorized personnel are permitted to install software, has the capability to help the installer to verify the authenticity of the software update.
5. Verifying HCD function: The HCD checks itself for malfunctions by performing a self-test each time that it is powered on.

1.4.2. USE CASE 2: Conditionally Mandatory Use Cases

Security-relevant use cases for Conditionally Mandatory Uses (if present) of a conforming HCD may include:

1. Sending PSTN faxes: A Local User scans a Document on the HCD, or a Network User sends a Document from an External IT Entity to the HCD; the User provides instructions for sending it to a remote PSTN fax destination; the HCD sends a facsimile of the Document over the PSTN to the PSTN fax destination using standard PSTN fax protocols. The HCD has the capability to protect the Network User's Document from unauthorized disclosure and alteration while in transit on the LAN. The HCD also has the capability to protect the User's Document from unauthorized disclosure and alteration while in Temporary Storage in the HCD.
2. Receiving PSTN faxes: A remote PSTN fax sender sends a facsimile of a Document over the PSTN to the HCD using standard PSTN fax protocols. The HCD has the capability to protect received PSTN faxes from unauthorized disclosure and alteration while it is present in the HCD. Further, the HCD has the capability to ensure that the PSTN fax modem is not used to access the LAN.
3. Storing and retrieving Documents: A Local or Network User instructs the HCD to store or retrieve an electronic Document in the HCD. The sources and destinations of such Documents may be any of the other operations such as scanning, printing, or PSTN faxing. The HCD has the capability to protect such Documents from unauthorized disclosure and alteration while in transit and in storage in the HCD.
4. Field-Replaceable Nonvolatile Storage Devices: Authorized personnel remove the HCD from service in its Operational Environment to perform preventative maintenance, repairs, or other servicing-related operations. The HCD has the capability to protect documents or confidential system information that may be present in Field-Replaceable Nonvolatile Storage Devices from exposure if such a device is removed from the HCD.

1.4.3. USE CASE 3: Optional Use Cases

Security-relevant use cases for Optional Uses (if present) of a conforming HCD may include:

1. Internal Audit Log Storage: If the audit log can also be stored in the HCD, the HCD has the

capability to protect its audit log from unauthorized disclosure and alteration.

2. Image Overwrite: At the conclusion of an image processing job, residual image data may be present in the HCD. The HCD has the capability to actively overwrite such image data.
3. Redeploying or Decommissioning the HCD: Authorized personnel remove the HCD from service in its Operational Environment to move it to a different Operational Environment, to permanently remove it from operation, or otherwise change its ownership. The HCD has the capability to make all customer data that may be present in the HCD unavailable for recovery if it is removed from the Operational Environment.

2. CC Conformance Claims

As defined by the references [CC1], [CC2] and [CC3], this cPP:

- conforms to the requirements of Common Criteria v3.1, Revision 5,
- is Part 2 extended,
- is Part 3 conformant,
- does not claim conformance to any other security functional requirement packages.

> The following paragraph may not be applicable for all cPPs and should be added or edited as appropriate.

In order to be conformant to this cPP, a ST shall demonstrate Exact Conformance. Exact Conformance, as a subset of Strict Conformance as defined by the CC, is defined as the ST containing all of the SFRs in Security Functional Requirements (these are the mandatory SFRs) of this cPP, and potentially SFRs from Consistency Rationale (these are selection-based SFRs) and Selection-Based Requirements (these are optional SFRs) of this cPP. While iteration is allowed, no additional requirements (from the CC parts 2 or 3, or definitions of extended components not already included in this cPP) are allowed to be included in the ST. Further, no SFRs in Security Functional Requirements of this cPP are allowed to be omitted.

> This section may not be applicable, especially early in the development of a cPP but may come back later. The site location here is a recommendation and all sections would be added to this page.

2.1. Components allowed with this cPP in a PP-Configuration

The list of packages, PP-Modules and cPPs that may be used in conjunction with this cPP can be found at: https://HCD.github.io/PP-config.html

The packages to which exact conformance can be claimed in conjunction with this PP are specified in the Allowed Packages list.

PP-Modules that are allowed to specify this cPP as a base PP are specified in the Base PP list.

Other cPPs that are allowed to be included in a PP-Configuration along with this cPP are specified in the Other cPP list.

3. Security Problem Definition

> The sections here are boilerplate, but the content needs to be filled in.

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 that the TOE is expected to enforce.

3.1. Threats

The following are Threats against the TOE that are countered by conforming products. Additional details about threats are in Appendix A.3.

3.1.1. Unauthorized Access to User Data

An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE’s interfaces [T.UNAUTHORIZED_ACCESS]. For example, depending on the design of the TOE, the attacker might access the printed output of a Network User’s print job, or modify the instructions for a job that is waiting in a queue, or read User Document Data that is in a User’s private or group storage area.

3.1.2. Unauthorized Access to TSF Data

An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE’s interfaces [T.TSF_COMPROMISE]. For example, depending on the design of the TOE, the attacker might use Unauthorized Access to TSF Data to elevate their own privileges, alter an Address Book to redirect output to a different destination, or use the TOE’s Credentials to gain access to an external server.

An attacker may cause the installation of unauthorized software on the TOE [T.UNAUTHORIZED_UPDATE]. For example, unauthorized software could be used to gain access to information that is processed by the TOE, or to attack other systems on the LAN.

3.1.3. Network Communication Attacks

An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication [T.NET_COMRPOMISE]. For example, here are several ways that network communications could be compromised: By monitoring clear-text communications on a wired LAN, the attacker might obtain User Document Data, User Credentials, or system Credentials, or hijack an interactive session. The attacker might record and replay a network communication session in order to log into the TOE as an authorized User to access

Documents or as an authorized Administrator to change security settings. The attacker might masquerade as a trusted system on the LAN in order to receive outgoing scan jobs, to record the transmission of system Credentials, or to send malicious data to the TOE.

3.1.4. Malfunction

A malfunction of the TSF may cause loss of security if the TOE is permitted to operate while in a degraded state [T.TSF_FAILURE]. Hardware or software malfunctions can produce unpredictable results, with a possibility that security functions will not operate correctly.

3.2. Assumptions

The following assumptions must be upheld so that the objectives and requirements can effectively counter the threats described in this Protection Profile. Additional details about assumptions are in Appendix A.5.

3.2.1. Physical Security

Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment [A.PHYSICAL]. The TOE is assumed to be located in a physical environment that is controlled or monitored such that a physical attack is prevented or detected.

3.2.2. Network Security

The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface [A.NETWORK]. The TOE is not intended to withstand network-based attacks from an unmanaged network environment.

3.2.3. Administrator Trust

TOE Administrators are trusted to administer the TOE according to site security policies [A.TRUSTED_ADMIN]. It is the responsibility of the TOE Owner to only authorize administrators who are trusted to configure and operate the TOE according to site policies and to not use their privileges for malicious purposes.

3.2.4. User Training

Authorized Users are trained to use the TOE according to site security policies [A.TRAINED_USERS]. It is the responsibility of the TOE Owner to only authorize Users who are trained to use the TOE according to site policies.

3.3. Organizational Security Policies

The following are Organizational Security Policies (OSPs) that are upheld by conforming products. Additional details about OSPs are in Appendix A.4.

3.3.1. User Authorization

Users must be authorized before performing Document Processing and administrative functions [P.AUTHORIZATION]. Authorization allows the TOE Owner to control who is able to use the resources of the TOE and who is permitted to perform administrative functions.

3.3.2. Auditing

Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity [P.AUDIT]. Stored on an External IT Entity (or, optionally, also in the TOE), an audit trail makes it possible for authorized personnel to review and identify suspicious activities and to account for TOE use as may be required by site policy or regulations.

3.3.3. Protected Communications

The TOE must be able to identify itself to other devices on the LAN [P.COMMS_PROTECTION]. Assuring identification helps prevent an attacker from masquerading as the TOE in order to receive incoming print jobs, recording the transmission of User Credentials, or sending malicious data to External IT Entities.

3.3.4. Storage Encryption (conditionally mandatory)

If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices , it will encrypt such data on those devices [P.STORAGE_ENCRYPTION]. Data is assumed to be protected by the TSF when the TOE is operating in its Operational Environment. However, if Field-Replaceable Nonvolatile Storage Devices are removed from the TOE for Servicing, redeployment to another environment, or decommissioning, an attacker may be able to expose or modify User Document Data or Confidential TSF Data. Encrypting such data prevents the attacker from doing so without access to encryption keys or keying material.

Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device [P.KEY_MATERIAL]. Unauthorized possession of key material in cleartext may allow an attacker to decrypt User Document Data or Confidential TSF Data.

3.3.5. PSTN Fax-Network Separation (conditionally mandatory)

If the TOE includes a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN [P.FAX_FLOW]. The TOE is assumed to be in an Operational Environment that is protected, such as by an external firewall. However, the PSTN fax modem may be connected to a public switched telephone network. Ensuring separation of the PSTN fax and network prevents an attacker from using the PSTN fax modem to bypass the firewall or other external protection to access the protected environment.

3.3.6. Image Overwrite (optional)

Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Devices [P.IMAGE_OVERWRITE]. A customer may be concerned that image data that has been dereferenced by the TOE operating software may remain on Field-Replaceable Nonvolatile Storage Devices in the TOE after a Document Processing job has been completed or cancelled. Such customers desire that the image data be made unavailable by overwriting it with other data.

3.3.7. Purge Data (optional)

The TOE shall provide a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices [P.PURGE_DATA]. A customer may be concerned that data which is considered confidential in the Operational Environment may remain in Nonvolatile Storage Devices in the TOE after the TOE is permanently removed from its Operational Environment to be decommissioned from service or to be redeployed to a different Operational Environment. Such customers desire that all customer-supplied User Data and TSF Data be purged from the TOE so that it cannot be retrieved outside of the Operational Environment.

4. Security Objectives

4.1. Security Objectives for the TOE

The following Security Objectives must be fulfilled by the TOE. Additional details about objectives for the TOE are in Appendices A.6 and A.7.

4.1.1. User Authorization

The TOE shall perform authorization of Users in accordance with security policies [O.USER_AUTHORIZATION].

This objective supports the policy that Users are authorized to administer the TOE or perform Document Processing functions that consume TOE resources. Users must be authorized to perform any of the Document Processing functions present in the TOE.

The mechanism for authorization is implemented within the TOE, and it may also depend on a trusted External IT Entity. If a conforming TOE supports more than one mechanism, then each should be evaluated as separate modes of operation.

In the case of printing (if that function is present in the TOE), User authorization may take place after the job has been submitted but must take place before printed output is made available to the User.

Users must be authorized to perform PSTN fax sending functions and document storage and retrieval functions, if such functions are provided by the conforming TOE.

Note that the TOE can receive a PSTN fax without any User authorization, but the received Document is subject to access controls.

4.1.2. User Identification and Authentication

The TOE shall perform identification and authentication of Users for operations that require access control, User authorization, or Administrator roles [O.USER_I&A].

The mechanism for identification and authentication (I&A) is implemented within the TOE, and it may also depend on a trusted External IT Entity (e.g., LDAP, Kerberos, or Active Directory). If a conforming TOE supports more than one mechanism, then each should be evaluated as separate modes of operation.

4.1.3. Access Control

The TOE shall enforce access controls to protect User Data and TSF Data in accordance with security policies [O.ACCESS_CONTROL].

The guiding principles for access control security policies in this PP are:

1. User Document Data [D.USER.DOC] can be accessed only by the Document owner or an Administrator.
2. User Job Data [D.USER.JOB] can be read by any User but can be modified only by the Job Owner or an Administrator.
3. Protected TSF Data [D.TSF.PROT] are data that can be read by any User but can be modified only by an Administrator or (in certain cases) a Normal User who is the owner of or otherwise associated with that data.
4. Confidential TSF Data [D.TSF.CONF] are data that can only be accessed by an Administrator or (in certain cases) a Normal User who is the owner of or otherwise associated with that data.

The Security Target of a conforming TOE must clearly specify its access control policies for User Data and TSF Data.

4.1.4. Administrator Roles

The TOE shall ensure that only authorized Administrators are permitted to perform administrator functions [O.ADMIN_ROLES].

This objective addresses the need to have at least one Administrator role that is distinct from Normal Users. A conforming TOE may have specialized Administrator sub-roles, such as for device management, network management, or audit management.

4.1.5. Software Update Verification

The TOE shall provide mechanisms to verify the authenticity of software updates [O.UPDATE_VERIFICATION].

This objective addresses the concern that malicious software may be introduced into the TOE as a software update. Verifying authenticity, such as with a digital signature or published hash, is required. Access control by itself does not satisfy this objective.

4.1.6. Self-test

The TOE shall test some subset of its security functionality to help ensure that subset is operating properly [O.TSF_SELF_TEST].

A malfunction of the TOE may compromise its security if the malfunction is not detected and the TOE is allowed to operate. Self-test is intended to detect such malfunctions. It is performed during power-up.

4.1.7. Communications Protection

The TOE shall have the capability to protect LAN communications of User Data and TSF Data from Unauthorized Access, replay, and source/destination spoofing [O.COMMS_PROTECTION]. This objective addresses the common concerns of network communications:

1. Sensitive data or Credentials are obtained by monitoring LAN data outside of the TOE.
2. A successfully authenticated session is captured and replayed on the LAN, permitting the attacker to masquerade as the authenticated User.
3. Sensitive data or Credentials are obtained by redirecting communications from the TOE or from an External IT Entity to a malevolent destination.

4.1.8. Auditing

The TOE shall generate audit data, and be capable of sending it to a trusted External IT Entity. Optionally, it may store audit data in the TOE [O.AUDIT].

The TOE must be able to send audit data to a trusted External IT Entity (e.g., an audit server such as a syslog server). Audit data may also be stored in the TOE with appropriate access controls to ensure confidentiality and integrity. If a conforming TOE supports both mechanisms, then each should be evaluated as separate modes of operation.

4.1.9. Storage Encryption (conditionally mandatory)

If the TOE stores User Document Data or Confidential TSF Data in Field-Replaceable Nonvolatile Storage devices, then the TOE shall encrypt such data on those devices. [O.STORAGE_ENCRYPTION].

This objective addresses the concern that User Document Data or Confidential TSF Data on a Field-Replaceable Nonvolatile Storage Device may be exposed if the device is removed from the TOE, such as for Servicing, Redeployment to another environment, or Decommissioning.

4.1.10. Protection of Key Material (conditionally mandatory)

The TOE shall protect from unauthorized access any cleartext keys, submasks, random numbers, or other values that contribute to the creation of encryption keys for storage of User Document Data or Confidential TSF Data in Field-Replaceable Nonvolatile Storage Devices; The TOE shall ensure that such key material is not stored in cleartext on the storage device that uses that material [O.KEY_MATERIAL].

This objective addresses the concern that unauthorized possession of keys or key material may be used to decrypt User Document Data or Confidential TSF Data.

4.1.11. PSTN Fax-Network Separation (conditionally mandatory)

If the TOE provides a PSTN fax function, then the TOE shall ensure separation of the PSTN fax telephone line and the LAN, by system design or active security function [O.FAX_NET_SEPARATION].

This objective addresses customer concerns about having a telephone line connected to a device that is inside their firewall. Depending on implementation, it may be satisfied in different ways, such as by system architecture (no data path from the PSTN fax interface to the network interface), by system design (fax chipset recognizes only PSTN fax protocols), or by active security function (flow control).

4.1.12. Image Overwrite (optional)

Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data in its Field-Replaceable Nonvolatile Storage Devices [O.IMAGE_OVERWRITE]. This objective addresses customer concerns that image data may remain on Field-Replaceable Nonvolatile Storage Devices in the TOE after a Document Processing job has been completed or cancelled.

4.1.13. Purge Data (optional)

The TOE provides a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices [O.PURGE_DATA]. This objective addresses customer concerns that data that is protected in the Operational Environment may remain in Nonvolatile Storage Devices after the TOE is permanently removed from its Operational Environment to be decommissioned from service or to be redeployed to a different Operational Environment.

4.2. Security Objectives for the Operational Environment

The following Security Objectives must be provided by the Operational Environment. Additional details about objectives for the Operational Environment are in Appendix A.7.

4.2.1. Physical Protection

The Operational Environment shall provide physical security, commensurate with the value of the TOE and the data it stores or processes [OE.PHYSICAL_PROTECTION].

Due to its intended function, this kind of TOE must be physically accessible to authorized Users, but it is not expected to be hardened against physical attacks. Therefore, the environment must provide an appropriate level of physical protection or monitoring to prevent physical attacks.

4.2.2. Network Protection

The Operational Environment shall provide network security to protect the TOE from direct, public access to its LAN interface [OE.NETWORK_PROTECTION].

This kind of TOE is not intended to be directly connected to a hostile network. Therefore, the environment must provide an appropriate level of network isolation.

4.2.3. Trusted Administrators

The TOE Owner shall establish trust that Administrators will not use their privileges for malicious purposes [OE.ADMIN_TRUST].

Administrators have privileges that can be misused for malicious purposes. It is the responsibility of the TOE Owner to grant administrator privileges only to individuals whom the TOE Owner trusts.

4.2.4. Trained Users

The TOE Owner shall ensure that Users are aware of site security policies and have the competence to follow them [OE.USER_TRAINING].

Site security depends on a combination of TOE security functions and appropriate use of those functions by Normal Users. Manufacturers may provide guidance to the TOE Owner regarding the TOE security functions that apply to Normal Users.

4.2.5. Trained Administrators

The TOE Owner shall ensure that Administrators are aware of site security policies and have the competence to use manufacturer’s guidance to correctly configure the TOE and protect passwords and keys accordingly [OE.ADMIN_TRAINING].

This kind of TOE may have many options for enabling and disabling security functions. Administrators must be able to understand and configure the TOE security functions to enforce site security policies.

4.3. Security Objectives Rationale

The following table describes how the assumptions, threats, and organizational security policies map to the security objectives.

Table 2. Mapping between Security Problem Defintion and Security Objectives

Threat, Assumption, or OSP	Security Objectives	Rationale

5. Security Functional Requirements

5.1. Conventions

> This section is boilerplate and should be left alone. Attention should be paid though as this is supposed to be followed in the SFRs.

The individual security functional requirements are specified in the sections below. The following conventions are used for the completion of operations:

- [*Italicized text within square brackets*] indicates an operation to be completed by the ST author.
- **Bold text** indicates additional text provided as a refinement.
- [**Bold text within square brackets**] indicates the completion of an assignment.
- [text within square brackets] indicates the completion of a selection.
- Number in parentheses after SFR name, e.g. (1) indicates the completion of an iteration.
- Extended SFRs are identified by having a label “EXT” at the end of the SFR name.

> The following sections have been included from CC Part 2 just as reference. Include only those classes in 5.2 - 5.12 for which the TOE will need to comply with one or more SFRs from that class. Any sections that do not have applicable SFRs can be removed.

5.2. Security Audit (FAU)

5.2.1. FAU_GEN.1Audit data generation

```
(for O.AUDIT)
Hierarchical to:    No other components.
Dependencies:       FPT_STM.1 Reliable time stamps
```

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a. Start-up and shutdown of the audit functions;

b. All auditable events for the **not specified** level of audit; and

c. **All auditable events specified in Table 1**, [assignment: *other specifically defined auditable events*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **additional information specified in Table 1**, [assignment: *other audit relevant information*].

Auditable Event	Relevant SFR	Additional Information
Job Completion	FDP_ACF.1	Type of Job
Unsuccessful User authentication	FIA_UAU.1	None
Unsuccessful User identification	FIA_UID.1	None
Use of management functions	FMT_SMF.1	None
Modification to the group of Users that are part of a role	FMT_SMR.1	None
Changes to the time	FPT_STM.1	None
Failure to establish session	FTP_ITC.1, FTP_TRP.1(a), FTP_TRP.1(b)	Reason for failure

Application Note:

In cases where user identification events are inseparable from user authentication events, they may be considered to be a single event for audit purposes.

Regarding FMT_SMR.1, if the relationship between users and roles is not modifiable, its auditable event cannot be generated and the requirement to generate an audit record can be ignored.

The ST author can include other auditable events directly in the table; they are not limited to the list presented.

5.2.2. FAU_GEN.2User identity association

```
(for O.AUDIT)
Hierarchical to:    No other components.
Dependencies:       FAU_GEN.1   Audit data generation
            FIA_UID.1   Timing of identification
```

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.2.3. FAU_STG_EXT.1Extended: External Audit Trail Storage

```
(for O.AUDIT)
Hierarchical to:    No other components.
Dependencies:       FAU_GEN.1   Audit data generation,
            FTP_ITC.1   Inter-TSF trusted channel.
```

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an External IT Entity using a trusted channel according to FTP_ITC.1.

```
(for O.AUDIT)
Hierarchical to:    No other components.
Dependencies:       FAU_GEN.1 Audit data generation,
            FTP_ITC.1 Inter-TSF trusted channel.
```

5.3. Cryptograhic Support (FCS)

5.3.1. FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)

```
(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION)
Hierarchical to:    No other components.
Dependencies:   [[strikeout]FCS_CKM.2 Cryptographic key distribution, or[/strikeout]
    FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
    FCS_COP.1(d) Cryptographic Operation (AES Data Encryption/Decryption)
    FCS_COP.1(e) Cryptographic Operation (Key Wrapping)
    FCS_COP.1(f) Cryptographic operation (Key Encryption)
    FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
    FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)]
    FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
    FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)
```

FCS_CKM.1.1(b) Refinement: The TSF shall generate **symmetric** cryptographic keys **using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes [selection: 128 bit, 256 bit] that meet the following: No Standard.**

Application Note:

Symmetric keys may be used to generate keys along the key chain.

5.3.2. FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

```
(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA)
Hierarchical to:    No other components.
Dependencies:   [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or
    FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)],
    FCS_CKM.4 Cryptographic key destruction
```

FCS_CKM_EXT.4.1 The TSF shall destroy all plaintext secret and private cryptographic keys and cryptographic critical security parameters when no longer needed.

Application Note:

“Cryptographic Critical Security Parameters” are defined in FIPS 140-2 as “security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic module”.

Keys, including intermediate keys and key material that are no longer needed are destroyed by using an approved method, FCS_CKM.4.1. Examples of keys are intermediate keys, submasks, and BEV. There may be instances where keys or key material that are contained in persistent storage are no longer needed and require destruction. Based on their implementation, vendors will explain when certain keys are no longer needed. There are multiple situations in which key material is no longer necessary, for example, a wrapped key may need to be destroyed when a password is changed. However, there are instances when keys are allowed to remain in memory, for example, a device identification key.

5.3.3. FCS_CKM.4 Cryptographic key destruction

```
(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA)
Hierarchical to:    No other components.
Dependencies:   [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or
    FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
```

FCS_CKM.4.1 Refinement: The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**selection:**

For volatile memory, the destruction shall be executed by a [selection: single overwrite consisting of [selection: a pseudo-random pattern using the TSF's RBG, zeroes, ones, a new value of a key, [assignment: any value that does not contain any CSP]], removal of power to the memory, destruction of reference to the key directly followed by a request for garbage collection];

For nonvolatile storage, the destruction shall be executed by a [selection: [selection: single, [assignment: ST author defined multi-pass]] overwrite consisting of [selection: zeroes, ones, pseudo-random pattern, a new value of a key of the same size, [assignment: any value that does not contain any CSP]], block erase];

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

Application Note:

In the first selection, the ST Author is presented options for destroying disused cryptographic keys based on whether they are in volatile memory or non-volatile memory within the TOE.

The selection of block erase for non-volatile memory applies only to flash memory.

Within the selections is the option to overwrite the memory location with a new value of a key. The intent is that a new value of a key (as specified in another SFR within the PP) can be used to "replace" an existing key.

Several selections allow assignment of a 'value that does not contain any CSP'. This means that the TOE uses some other specified data not drawn from a source that may contain key material or reveal information about key material, and not being any of the particular values listed as other selection options. The point of the phrase 'does not contain any CSP' is to ensure that the overwritten data is carefully selected, and not taken from a general 'pool' that might contain current or residual data that itself requires confidentiality protection.

5.3.4. FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)

```
(for O.COMMS_PROTECTION)
Hierarchical to:    No other components.
Dependencies:   [[strikeout]FDP_ITC.1 Import of user data without security attributes,
or
    FDP_ITC.2 Import of user data with security attributes, or[/strikeout]
    FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
    FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
```

FCS_COP.1.1(a) Refinement: The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **AES operating in [assignment: one or more modes]** and cryptographic key sizes **128-bits and 256-bits** that meets the following:

- **FIPS PUB 197, "Advanced Encryption Standard (AES)"**
- **[Selection:** ***NIST SP 800-38A, NIST SP 800-38B, NIST SP 800-38C, NIST SP 800-38D*****]**

Application Note:

For the assignment, the ST author should assign the mode or modes in which AES operates to support the cryptographic protocols chosen for FTP_ITC and FTP_TRP.

For the selection, the ST author should choose the standards that describe the modes specified in the assignment.

5.3.5. FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)

```
(for O.UPDATE_VERIFICATION, O.COMMS_PROTECTION)
Hierarchical to:    No other components.
Dependencies:   [[strikeout]FDP_ITC.1 Import of user data without security attributes,
or
    FDP_ITC.2 Import of user data with security attributes, or
    FCS_CKM.1 Cryptographic key generation[/strikeout]
    FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)]
    FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
```

FCS_COP.1.1(b) Refinement: The TSF shall perform cryptographic signature services in accordance with a [selection:

- ***Digital Signature Algorithm (DSA) with key sizes (modulus) of*** **[assignment:** ***2048 bits or greater*****],**
- ***RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of*** **[assignment:** ***2048 bits or greater*****], or**
- ***Elliptic Curve Digital Signature Algorithm (ECDSA) with key sizes of*** **[assignment:** ***256 bits***

***or greater*]]**

that meets the following **[selection:**

Case: Digital Signature Algorithm

- ***FIPS PUB 186-4, “Digital Signature Standard”***

Case: RSA Digital Signature Algorithm

- ***FIPS PUB 186-4, “Digital Signature Standard”***

Case: Elliptic Curve Digital Signature Algorithm

- ***FIPS PUB 186-4, “Digital Signature Standard”***
- ***The TSF shall implement “NIST curves” P-256, P384 and [selection: P521, no other curves] (as defined in FIPS PUB 186-4, “Digital Signature Standard”).***

].

Application Note:

The ST Author should choose the algorithm implemented to perform digital signatures; if more than one algorithm is available, this requirement (and the corresponding FCS_CKM.1 requirement) should be iterated to specify the functionality. For the algorithm chosen, the ST author should make the appropriate assignments/selections to specify the parameters that are implemented for that algorithm.

For elliptic curve-based schemes, the key size refers to the log2 of the order of the base point.

5.3.6. FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

```
(for O.STORAGE_ENCRYPTION and O.COMMS_PROTECTION)
Hierarchical to:    No other components.
Dependencies:   No dependencies.
```

FCS_RBG_EXT.1.1: The TSF shall perform all deterministic random bit generation services in accordance with [selection: *ISO/IEC 18031:2011, NIST SP 800-90A*] using [selection: *Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)*].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [selection: [assignment: *number of software-based sources*] software-based noise source(s), [assignment: *number of hardware-based sources*] hardware-based noise source(s)] with a minimum of [selection: *128 bits, 256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

Application Note:

ISO/IEC 18031:2011 contains different methods of generating random numbers; each of these, in turn, depends on underlying cryptographic primitives (hash functions/ciphers). The ST author will select the function used and include the specific underlying cryptographic primitives used in the requirement. While any of the identified hash functions (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) are allowed for Hash_DRBG or HMAC_DRBG, only AES-based implementations for CTR_DRBG are allowed. Table C.2 in ISO/IEC 18031:2011 provides an identification of Security strengths, Entropy and Seed length requirements for the AES-128 and 256 Block Cipher.

The CTR_DRGB in ISO/IEC 18031:2011 requires using derivation function, whereas NIST SP 800-90A does not. Either model is acceptable. In the first selection in FCS_RBG_EXT.1.1, the ST Author chooses the standard with which they are compliant.

The first selection in FCS_RBG_EXT.1.2 the ST author fills in how many entropy sources are used for each type of entropy source they employ. It should be noted that a combination of hardware and software based noise sources is acceptable.

It should be noted that the entropy source is considered to be a part of the RBG and if the RBG is included in the TOE, the developer is required to provide the entropy description outlined in Appendix E. The documentation ***and tests*** *required in the Evaluation Activity for this element necessarily cover each source indicated in FCS_RBG_EXT.1.2.*

5.4. User Data Protection (FDP)

Application Note:

The User Data Access Control SFP is composed of Table 2, Table 3, FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, and FMT_MSA.3.

5.4.1. FDP_ACC.1Subset access control

```
(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)
Hierarchical to:    No other components.
Dependencies:   FDP_ACF.1   Security attribute based access control
```

FDP_ACC.1.1 Refinement: The TSF shall enforce the **User Data Access Control SFP** on subjects, objects, and operations among subjects and objects specified in **Table 2 and Table 3**.

5.4.2. FDP_ACF.1Security attribute based access control

```
(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)
Hierarchical to:    No other components.
Dependencies:   FDP_ACC.1   Subset access control
    FMT_MSA.3   Static attribute initialization
```

FDP_ACF.1.1 Refinement: The TSF shall enforce the **User Data Access Control SFP** to objects based on the following: subjects, objects, and attributes specified in **Table 2 and Table 3**.

FDP_ACF.1.2 Refinement: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects specified in Table 2 and Table 3***.

FDP_ACF.1.3 Refinement: The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules* ***that do not conflict with the User Data Access Control SFP****, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4 Refinement: The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules* ***that do not conflict with the User Data Access Control SFP****, based on security attributes, that explicitly deny access of subjects to objects*].

Table 2 D.USER.DOC Access Control SFP

PRINT	"Create"	"Read"	"Modify"	"Delete"
Operation:	Submit a document to be printed	View image or Release printed output	Modify stored document	Delete stored document
Job owner	(note 1)			
U.ADMIN				
U.NORMAL		denied	denied	denied
Unauthenticated	(condition 1)	denied	denied	denied

SCAN	"Create"	"Read"	"Modify"	"Delete"
Operation:	Submit a document for scanning	View scanned image	Modify stored image	Delete stored image
Job owner	(note 2)			
U.ADMIN				
U.NORMAL		denied	denied	denied
Unauthenticated	denied	denied	denied	denied

COPY	"Create"	"Read"	"Modify"	"Delete"
Operation:	Submit a document for copying	View scanned image or Release printed copy output	Modify stored image	Delete stored image
Job owner	(note 2)			
U.ADMIN				
U.NORMAL		denied	denied	denied
Unauthenticated	denied	denied	denied	denied

FAX SEND	"Create"	"Read"	"Modify"	"Delete"
Operation:	Submit a document to send as a fax	View scanned image	Modify stored image	Delete stored image
Job owner	(note 2)			
U.ADMIN				
U.NORMAL		denied	denied	denied
Unauthenticated	denied	denied	denied	denied

FAX RECEIVE	"Create"	"Read"	"Modify"	"Delete"
Operation:	Receive a fax and store it	View fax image or Release printed fax output	Modify image of received fax	Delete image of received fax
Fax owner	(note 3)			
U.ADMIN	(note 4)			
U.NORMAL	(note 4)	denied	denied	denied
Unauthenticated		denied	denied	denied

STORAGE/RETRIEVAL	"Create"	"Read"	"Modify"	"Delete"
Operation:	Store document	Retrieve stored document	Modify stored document	Delete stored document
Job owner	(note 1)			
U.ADMIN				
U.NORMAL		denied	denied	denied
Unauthenticated	(condition 1)	denied	denied	denied

Table 3 D.USER.JOB Access Control SFP

"PRINT"	"Create" *	"Read"	"Modify"	"Delete"
Operation:	Create print job	View print queue / log	Modify print job	Cancel print job
Job owner	(note 1)			
U.ADMIN				
U.NORMAL			denied	denied
Unauthenticated			denied	denied

"SCAN"	"Create" *	"Read"	"Modify"	"Delete"

Operation:	Create scan job	View scan status / log	Modify scan job	Cancel scan job
Job owner	(note 2)			
U.ADMIN				
U.NORMAL			denied	denied
Unauthenticated	denied		denied	denied

"COPY"	"Create" *	"Read"	"Modify"	"Delete"
Operation:	Create copy job	View copy status / log	Modify copy job	Cancel copy job
Job owner	(note 2)			
U.ADMIN				
U.NORMAL			denied	denied
Unauthenticated	denied		denied	denied

"FAX SEND"	"Create" *	"Read"	"Modify"	"Delete"
Operation:	Create fax send job	View fax job queue / log	Modify fax send job	Cancel fax send job
Job owner	(note 2)			
U.ADMIN				
U.NORMAL			denied	denied
Unauthenticated	denied		denied	denied

"FAX RECEIVE"	"Create" *	"Read"	"Modify"	"Delete"
Operation:	Create fax receive job	View fax receive status / log	Modify fax receive job	Cancel fax receive job
Fax owner	(note 3)			
U.ADMIN	(note 4)			
U.NORMAL	(note 4)		denied	denied
Unauthenticated			denied	denied

"STORAGE/RETRIEVAL"	"Create" *	"Read"	"Modify"	"Delete"
Operation:	Create storage / retrieval job	View storage / retrieval log	Modify storage / retrieval log	Cancel storage / retrieval log
Job owner	(note 1)			
U.ADMIN				
U.NORMAL			denied	denied

Unauthenticated	(condition 1)		denied	denied

Application note:

In general, the ST Author may modify this SFP provided that any changes are more restrictive. As examples, the ST Author may: remove the rules related to Document Processing functions that are not present in a TOE, add or modify rules to further deny access, or subdivide User Data to further restrict access for some data (e.g., D.USER.JOB.PROT and D.USER.JOB.CONF). Empty cells in the table indicate that the operation may be permitted, but it is not required to be permitted.

In particular, referring to Table 2 and Table 3:

- *A cell marked "Denied" indicates that the user (row) must not be permitted to perform the operation (column). The ST Author cannot override this.*
- *A cell that is blank indicates that the user may be permitted to perform the operation. However, the ST author may add conditions or restrictions, or deny permission entirely.*
- *A cell that is marked with a Condition means that the user can be permitted to perform the operation, provided that it meets that Condition as specified below. As with blank cells, the ST author can make it more restrictive.*

Condition 1: *Jobs submitted by unauthenticated users must contain a credential that the TOE can use to identify the Job Owner.*

See also the following Notes that are referenced in Table 2 and Table 3:

Note 1: *Job Owner is identified by a credential or assigned to an authorized User as part of the process of submitting a print or storage Job.*

Note 2: *Job Owner is assigned to an authorized User as part of the process of initiating a scan, copy, fax send, or retrieval Job.*

Note 3: *Job Owner of received faxes is assigned by default or configuration. Minimally, ownership of received faxes is assigned to a specific user or U.ADMIN role.*

Note 4: *PSTN faxes are received from outside of the TOE, they are not initiated by Users of the TOE.*

5.5. Identification and Authentication (FIA)

5.5.1. FIA_AFL.1 Authentication failure handling

```
(for O.USER_I&A)
Hierarchical to:    No other components.
Dependencies:   FIA_UAU.1   Timing of authentication
```

FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: *positive integer number*], an administrator configurable positive integer within [assignment: *range of acceptable values*]] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed], the TSF shall [assignment: *list of actions*].

Application note:

This SFR applies only to internal identification and authentication.

5.5.2. FIA_ATD.1 User attribute definition

```
(for O.USER_AUTHORIZATION)
Hierarchical to:    No other components.
Dependencies:   No dependencies.
```

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].

Application note:

The list of security attributes should be the union of all attributes for each of the supported authentication methods.

5.5.3. FIA_PMG_EXT.1 Extended: Password Management

```
(for O.USER_I&A)
Hierarchical to:    No other components.
Dependencies:   No dependencies.
```

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for User passwords:

- Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [assignment: *other characters*]];
- Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater;

Application note:

This SFR applies only to password-based single-factor Internal Authentication.

5.5.4. FIA_UAU.1 Timing of authentication

```
(for O.USER_I&A)
Hierarchical to:    No other components.
Dependencies:   FIA_UID.1   Timing of identification
```

FIA_UAU.1.1 Refinement: The TSF shall allow [assignment: *list of TSF mediated actions* ***that do not conflict with the User Data Access Control SFP, and do not provide access to D.TSF.CONF, and do not change any TSF data***] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application note:

User authentication may be performed internally by the TOE or externally by an External IT Entity.

5.5.5. FIA_UAU.7 Protected authentication feedback

```
(for O.USER_I&A)
Hierarchical to:    No other components.
Dependencies:   FIA_UAU.1   Timing of authentication
```

FIA_UAU.7.1 The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.

Application note:

FIA_UAU.7 applies only to authentication processes in which the User interacts with the TOE.

5.5.6. FIA_UID.1 Timing of identification

```
(for O.USER_I&A and O.ADMIN_ROLES)
Hierarchical to:    No other components.
Dependencies:   No dependencies.
```

FIA_UID.1.1 Refinement: The TSF shall allow [assignment: *list of TSF-mediated actions* ***that do not conflict with the User Data Access Control SFP, and do not provide access to D.TSF.CONF, and do not change any TSF data***] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application note:

User identification may be performed internally by the TOE or externally by an External IT Entity.

5.5.7. FIA_USB.1 User-subject binding

```
(for O.USER_I&A)
Hierarchical to:    No other components.
Dependencies:   FIA_ATD.1   User attribute definition
```

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *list of user security attributes*].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *rules for the initial association of attributes*].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *rules for the changing of attributes*].

5.6. Security Management (FMT)

5.6.1. FMT_MOF.1 Management of security functions behavior

```
(for O.ADMIN_ROLES)
Hierarchical to:    No other components.
Dependencies:   FMT_SMR.1   Security roles
    FMT_SMF.1   Specification of Management Functions
```

FMT_MOF.1.1 Refinement: The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to **U.ADMIN**.

5.6.2. FMT_MSA.1Management of security attributes

```
(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)
Hierarchical to:    No other components.
Dependencies:   [FDP_ACC.1  Subset access control, [strikeout]or
    FDP_IFC.1 Subset information flow control][/strikeout]
    FMT_SMR.1   Security roles
    FMT_SMF.1   Specification of Management Functions
```

FMT_MSA.1.1 Refinement: The TSF shall enforce the User Data Access Control SFP to restrict the ability to *] the security attributes [assignment: _list of security attributes*] to [assignment: *the authorised identified roles*].

5.6.3. FMT_MSA.3Static attribute initialization

```
(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)
Hierarchical to:    No other components.
Dependencies:   FMT_MSA.1   Management of security attributes
    FMT_SMR.1   Security roles
```

FMT_MSA.3.1 Refinement: The TSF shall enforce the **User Data Access Control SFP** to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 Refinement: The TSF shall allow the [***selection: U.ADMIN, no role***] to specify alternative initial values to override the default values when an object or information is created.

Application note:

FMT_MSA.3.2 applies only to security attributes whose default values can be overridden.

5.6.4. FMT_MTD.1Management of TSF data

```
(for O.ACCESS CONTROL)
Hierarchical to:    No other components.
Dependencies:   FMT_SMR.1   Security roles
    FMT_SMF.1   Specification of Management Functions
```

FMT_MTD.1.1 Refinement: The TSF shall restrict the ability to **perform the specified operations on the specified TSF Data to the roles specified in Table 4.**

Table 4 Management of TSF Data

Data	Operation	Authorised role(s)
[assignment: list of TSF Data owned by a U.NORMAL or associated with Documents or jobs owned by a U.NORMAL]	[selection: change default, query, modify, delete, clear, [assignment: other operations]]	U.ADMIN, the owning U.NORMAL.
[assignment: list of TSF Data not owned by a U.NORMAL]	[selection: change default, query, modify, delete, clear, [assignment: other operations]]	U.ADMIN
[assignment: list of software, firmware, and related configuration data]	[selection: change default, query, modify, delete, clear, [assignment: other operations]]	U.ADMIN

5.6.5. FMT_SMF.1Specification of Management Functions

```
(for O.USER_AUTHORIZATION, O.ACCESS_CONTROL, and O.ADMIN_ROLES)
Hierarchical to:    No other components.
Dependencies:   No dependencies.
```

FMT_SMF.1.1: The TSF shall be capable of performing the following management functions: [assignment: *list of management functions provided by the TSF*].

Example 1. Application note:

Application note:

Regarding “management functions provided by the TSF”, the ST Author should consider management functions that support the security objectives of this protection profile.

The management functions should be restricted to the authorized identified role in FMT_MOF.1, FMT_MTD.1, FMT_MSA.1.

The ST Author may identify cases where a security objective is fulfilled without explicit manageability.

For example, the following management functions are categorized by security objectives:

For O.USER_AUTHORIZATION, O.USER_I&A, O.ADMIN_ROLES, O.ACCESS_CONTROL:

- User management (e.g., add/change/remove local user)
- Role management (e.g., assign/deassign role relationship with user)
- Configuring identification and authentication (e.g., selecting between local and external I&A)
- Configuring authorization and access controls (e.g., access control lists for TOE resources)
- Configuring communication with External IT Entities

For O.UPDATE_VERIFICATION:

- Configuring software updates

For O.COMMS_PROTECTION:

- Configuring network communications
- Configuring the system or network time source

For O.AUDIT:

- Configuring data transmission to audit server
- Configuring the system or network time source
- Configuring internal audit log storage

For O.STORAGE_ENCRYPTION, O.KEY_MATERIAL:

- Configuring and invoking encryption of Field-Replaceable Nonvolatile Storage Devices

(Optional) For O.IMAGE_OVERWRITE, O.PURGE DATA:

- Configuring and/or invoking image overwrite functions
- Configuring and/or invoking data purging functions

5.6.6. FMT_SMR.1Security roles

```
(for O.ACCESS_CONTROL, O.USER_AUTHORIZATION, and O.ADMIN_ROLES)
Hierarchical to:    No other components.
Dependencies:   FIA_UID.1   Timing of identification
```

FMT_SMR.1.1 The TSF shall maintain the roles **U.ADMIN, U.NORMAL**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.7. Privacy (FPR)

There are no class FPR requirements.

5.8. Protection of the TSF (FPT)

5.8.1. FPT_SKP_EXT.1 Extended: Protection of TSF Data

```
(for O.COMMS_PROTECTION)
Hierarchical to:    No other components.
Dependencies:   No dependencies.
```

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

Application Note:

The intent of the requirement is that an administrator is unable to read or view the identified keys (stored or ephemeral) through “normal” interfaces. While it is understood that the administrator could directly read memory to view these keys, doing so is not a trivial task and may require substantial work on the part of an administrator. Since the administrator is considered a trusted agent, it is assumed they would not engage in such an activity.

5.8.2. FPT_STM.1Reliable time stamps

```
(for.O.AUDIT)
Hierarchical to:    No other components.
Dependencies:   No dependencies.
```

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Application note:

The time may be set by a trusted administrator or by a network service (e.g., NTP) from a trusted External IT Entity.

5.8.3. FPT_TST_EXT.1Extended: TSF testing

```
(for O.TSF_SELF_TEST)
Hierarchical to:    No other components.
Dependencies:   No dependencies.
```

FPT_TST_EXT.1.1 The TSF shall run a suite of self-tests during initial start-up (and power on) to demonstrate the correct operation of the TSF.

Application note:

Power-on self-tests may take place before the TSF is operational, in which case this SFR can be satisfied by verifying the TSF image by digital signature as specified in FCS_COP.1(b), or by hash specified in FCS_COP.1(c).

5.8.4. FPT_TUD_EXT.1Extended: Trusted Update

```
(for O.UPDATE_VERIFICATION)
Hierarchical to:    No other components.
Dependencies:   FCS_COP.1(b) Cryptographic Operation (for signature
generation/verification),
    FCS_COP.1(c) Cryptographic operation (Hash Algorithm).
```

FPT_TUD_EXT.1.1 The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [selection: *published hash, no other functions*] prior to installing those updates.

Application note:

FPT_TUD_EXT.1.2 may be interpreted to allow an administrator to “pre-authorize” automatic updates, provided that they are verified according to FPT_TUD_EXT.1.3.

The digital signature mechanism is specified in FCS_COP.1(b). The published hash is generated by one of the functions specified in FCS_COP.1(c). It is acceptable to implement both mechanisms.

5.9. Resource Utilization (FRU)

There are no class FRU requirements.

5.10. TOE Access (FTA)

5.10.1. FTA_SSL.3TSF-initiated termination

```
(for O.USER_I&A)
Hierarchical to:    No other components.
Dependencies:   No dependencies.
```

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [assignment: *time interval of user inactivity*].

5.11. Trusted Paths/Channels (FTP)

5.11.1. FTP_ITC.1Inter-TSF trusted channel

```
(for O.COMMS_PROTECTION, O.AUDIT)
Hierarchical to:    No other components.
Dependencies:   [FCS_IPSEC_EXT.1 Extended: IPsec selected, or
    FCS_TLS_EXT.1 Extended: TLS selected, or
    FCS_SSH_EXT.1 Extended: SSH selected, or
    FCS_HTTPS_EXT.1 Extended: HTTPS selected].
```

FTP_ITC.1.1 Refinement: The TSF shall **use [selection: IPsec, SSH, TLS, TLS/HTTPS] to** provide **a trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: [selection: *authentication server, [assignment: other capabilities]*]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.

FTP_ITC.1.2 Refinement: The TSF shall permit **the TSF, or the authorized IT entities**, to initiate communication via the trusted channel

FTP_ITC.1.3 Refinement: The TSF shall initiate communication via the trusted channel for [assignment: ***list of services for which the TSF is able to initiate communications***].

Application note:

The assignment in FTP_ITC.1.3 should address the confidentiality and/or integrity requirements for communication of User and TSF Data between the TOE and another IT entity. FTP_TRP.1 is intended to be used for interactive communication between the TOE and remote users.

The intent of the above requirement is to use a cryptographic protocol to protect external communications with authorized IT entities that the TOE interacts with to perform its functions. Protection (by one of the listed protocols) is required at least for communications with the server that collects the audit information. If it communicates with an authentication server (e.g., RADIUS), then the ST author chooses "authentication server" in FTP_ITC.1.1 and this connection must be protected *by one of the listed protocols. If other authorized IT entities (e.g., NTP server) are protected, the ST author makes the appropriate assignments (for those entities) and selections (for the protocols that are used to protect those connections). After the ST author has made the selections, they are to select the detailed requirements in Appendix D.2 corresponding to their protocol selection to put in the ST. To summarize, the connection to an external audit collection server is required to be protected by one of the listed protocols. If an External Authentication server is supported, then it is required to protect that connection with one of the listed protocols. For any other external server, external communications are not required to be protected, but if protection is claimed, then it must be protected with one of the identified protocols.*

While there are no requirements on the party initiating the communication, the ST author lists in the assignment for FTP_ITC.1.3 the services for which the TOE can initiate the communication with the authorized IT entity.

The requirement implies that not only are communications protected when they are initially established, but also on resumption after an outage. It may be the case that some part of the TOE setup involves manually setting up tunnels to protect other communication, and if after an outage the TOE attempts to re-establish the communication automatically with (the necessary) manual intervention, there may be a window created where an attacker might be able to gain critical information or compromise a connection.

5.11.2. FTP_TRP.1(a) Trusted path (for Administrators)

```
(for O.COMMS_PROTECTION)
Hierarchical to:    No other components.
Dependencies:   [FCS_IPSEC_EXT.1 Extended: IPsec selected, or
    FCS_TLS_EXT.1 Extended: TLS selected, or
    FCS_SSH_EXT.1 Extended: SSH selected, or
    FCS_HTTPS_EXT.1 Extended: HTTPS selected].
```

FTP_TRP.1.1(a) Refinement: The TSF shall **use [selection, choose at least one of: IPsec, SSH, TLS, TLS/HTTPS] to** provide **a trusted** communication path between itself and **remote administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and detection of modification of the communicated data**.

FTP_TRP.1.2(a) Refinement: The TSF shall permit **remote administrators** to initiate communication via the trusted path

FTP_TRP.1.3(a) Refinement: The TSF shall require the use of the trusted path for **initial administrator authentication and all remote administration actions**.

Application Note:

This requirement ensures that authorized remote administrators initiate all communication with the TOE via a trusted path, and that all communications with the TOE by remote administrators is performed over this path. The data passed in this trusted communication path are encrypted as defined the protocol chosen in the first selection. The ST author chooses the mechanism or *mechanisms supported by the TOE, and then ensures the detailed requirements in Appendix D.2 corresponding to their selection are copied to the ST if not already present.*

6. Security Assurance Requirements

This section is boilerplate

The Security Objectives for the TOE were constructed to address [threats] identified in the Security Problem Definition. The Security Functional Requirements are a formal instantiation of the Security Objectives. This cPP identifies the Security Assurance Requirements to frame the extent to which the evaluator assesses the documentation applicable for the evaluation and performs independent testing.

This section lists the set of SARs from CC part 3 that are required in evaluations against this cPP. Individual Evaluation Activities to be performed are specified in [SD].

The general model for evaluation of TOEs against STs written to conform to this cPP is as follows:

After the ST has been approved for evaluation, the ITSEF (IT Security Evaluation Facility) will obtain the TOE, supporting environmental IT (if required), and the administrative/user guides for the TOE. The ITSEF is expected to perform actions mandated by the Common Evaluation Methodology (CEM) for the ASE and ALC SARs. The ITSEF also performs the Evaluation Activities contained within the SD, which are intended to be an interpretation of the other CEM assurance requirements as they apply to the specific technology instantiated in the TOE. The Evaluation Activities that are captured in the SD also provide clarification as to what the developer needs to provide to demonstrate the TOE is compliant with the cPP.

If the iTC decides to go above EAL1 requirements then this table (and the associated SARs) will need to be modified. If not, then this is boilerplate and can be left alone.

Table 3. Security Assurance Requirements

Assurance Class	Assurance Components
Security Target (ASE)	Conformance Claims (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)
	ST introduction (ASE_INT.1)
	Security objectives for the operational environment (ASE_OBJ.1)
	Stated security requirements (ASE_REQ.1)
	Security Problem Definition (ASE_SPD.1)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	Basic functional specification (ADV_FSP.1)

Guidance documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life cycle support (ALC)	Labeling of the TOE (ALC_CMC.1)
	TOE CM coverage (ALC_CMS.1)
Tests (ATE)	Independent testing – sample (ATE_IND.1)
Vulnerability assessment (AVA)	Vulnerability survey (AVA_VAN.1)

6.1. ASE: Security Target

This section is boilerplate except for the guidance noted here

The ST is evaluated as per ASE activities defined in the [CEM]. In addition, there may be Evaluation Activities specified within the [SD] that call for necessary descriptions to be included in the TSS that are specific to the TOE technology type.

As an option, the cPP may express a need for a more detailed description of how a TOE satisfies one or more SFRs. The level of detail required by the SD may include proprietary information, or simply information that should not be made public (i.e., provides attackers insight into the operation of the TOE that may increase the likelihood of a successful attack against the product). This information could be submitted as an appendix to the ST or as a separate document. The required information may take the form of a refinement as shown below, and the associated Evaluation Activity would be specified in the SD.

As long as you are doing EAL1, none of these sections until you get to AVA_VAN.1 will need to be modified.

6.2. ADV: Development

The design information about the TOE is contained in the guidance documentation available to the end user as well as the TSS portion of the ST, and any additional information required by this cPP that is not to be made public (e.g., Entropy Report).

6.2.1. Basic Functional Specification (ADV_FSP.1)

The functional specification describes the TOE Security Functions Interfaces (TSFIs). It is not necessary to have a formal or complete specification of these interfaces. Additionally, because TOEs conforming to this cPP will necessarily have interfaces to the Operational Environment that are not directly invokable by TOE users, there is little point specifying that such interfaces be described in and of themselves since only indirect testing of such interfaces may be possible. For this cPP, the Evaluation Activities for this family focus on understanding the interfaces presented in the TSS in response to the functional requirements and the interfaces presented in the AGD documentation.

No additional “functional specification” documentation is necessary to satisfy the Evaluation Activities specified in [SD].

The Evaluation Activities in [SD] are associated with the applicable SFRs; since these are directly associated with the SFRs, the tracing in element ADV_FSP.1.2D is implicitly already done and no additional documentation is necessary.

6.3. AGD: Guidance Documentation

The guidance documents will be provided with the ST. Guidance must include a description of how the IT personnel verifies that the Operational Environment can fulfill its role for the security functionality. The documentation should be in an informal style and readable by the IT personnel.

Guidance must be provided for every operational environment that the product supports as claimed in the ST. This guidance includes:

- instructions to successfully install the TSF in that environment; and
- instructions to manage the security of the TSF as a product and as a component of the larger operational environment; and
- instructions to provide a protected administrative capability.

Guidance pertaining to particular security functionality must also be provided; requirements on such guidance are contained in the Evaluation Activities specified in the [SD].

6.3.1. Operational User Guidance (AGD_OPE.1)

The operational user guidance does not have to be contained in a single document. Guidance to users, administrators and application developers can be spread among documents or web pages.

The developer should review the Evaluation Activities contained in the [SD] to ascertain the specifics of the guidance that the evaluator will be checking for. This will provide the necessary information for the preparation of acceptable guidance.

6.3.2. Preparative Procedures (AGD_PRE.1)

As with the operational guidance, the developer should look to the Evaluation Activities to determine the required content with respect to preparative procedures.

6.4. Class ALC: Life-cycle Support

At the assurance level provided for TOEs conformant to this cPP, life-cycle support is limited to end-user-visible aspects of the life-cycle, rather than an examination of the TOE vendor’s development and configuration management process. This is not meant to diminish the critical role that a developer’s practices play in contributing to the overall trustworthiness of a product; rather, it is a reflection on the information to be made available for evaluation at this assurance level.

6.4.1. Labelling of the TOE (ALC_CMC.1)

This component is targeted at identifying the TOE such that it can be distinguished from other products or versions from the same vendor and can be easily specified when being procured by an end user.

6.4.2. TOE CM Coverage (ALC_CMS.1)

Given the scope of the TOE and its associated evaluation evidence requirements, the evaluator performs the CEM work units associated with ALC_CMC.1.

6.5. Class ATE: Tests

Testing is specified for functional aspects of the system as well as aspects that take advantage of design or implementation weaknesses. The former is done through the ATE_IND family, while the latter is through the AVA_VAN family. For this cPP, testing is based on advertised functionality and interfaces with dependency on the availability of design information. One of the primary outputs of the evaluation process is the test report as specified in the following requirements.

6.5.1. Independent Testing – Conformance (ATE_IND.1)

Testing is performed to confirm the functionality described in the TSS as well as the operational guidance (includes “evaluated configuration” instructions). The focus of the testing is to confirm that the requirements specified in Section 5 are being met. The Evaluation Activities in the SD identify the specific testing activities necessary to verify compliance with the SFRs. The evaluator produces a test report documenting the plan for and results of testing, as well as coverage arguments focused on the platform/TOE combinations that are claiming conformance to this cPP.

6.6. Class AVA: Vulnerability Assessment

> AVA is a difficult subject. This is taken from the NDcPP v2.1 as an example, but will need to be determined by the iTC.

For the first generation of this cPP, the iTC is expected to survey open sources to discover what vulnerabilities have been discovered in these types of products and provide that content into the AVA_VAN discussion. In most cases, these vulnerabilities will require sophistication beyond that of a basic attacker. This information will be used in the development of future protection profiles.

6.6.1. Vulnerability Survey (AVA_VAN.1)

[SD] provides a guide to the evaluator in performing a vulnerability analysis.

Appendix A: Selection-Based Requirements

If there are selection-based requirements, the following paragraphs should be left

As indicated in the introduction to this cPP, the baseline requirements (those that shall be performed by the TOE) are contained in Security Functional Requirements. Additionally, there are two other types of requirements specified in Consistency Rationale.

The first type (in this Appendix) comprises requirements based on selections in other SFRs from the cPP: if certain selections are made, then additional requirements in this chapter will need to be included in the body of the ST.

The second type (in the next Appendix) comprises requirements that can be included in the ST, but are not mandatory for a TOE to claim conformance to this cPP.

It is likely (though not guaranteed) there will be selection-based requirements. If there are, then they should be placed here. If there are none, then that should be explicitly stated in this section.

A.1. Confidential Data on Field-Replaceable Nonvolatile Storage Devices

A.1.1. FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption)

```
 (for O. STORAGE_ENCRYPTION)
Hierarchical to:    No other components.
Dependencies:   [[so]FDP_ITC.1 Import of user data without security attributes, or
    FDP_ITC.2 Import of user data with security attributes, or[/so]
    FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
    FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
```

FCS_COP.1.1(d) The TSF shall perform **data encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [selection:** ***CBC, GCM, XTS*****] mode** and cryptographic key sizes [**selection:** ***128 bits, 256 bits***] that meet the following: **AES as specified in ISO/IEC 18033-3, [selection:** ***CBC as specified in ISO/IEC 10116, GCM as specified in ISO/IEC 19772, and XTS as specified in IEEE 1619***].

Application Note:

This PP allows for software encryption or hardware encryption.

If XTS Mode is selected, a cryptographic key of 256-bit or of 512-bit is allowed as specified in IEEE 1619. XTS-AES key is divided into two AES keys of equal size - for example, AES-128 is used as the underlying algorithm, when 256-bit key and XTS mode are selected. AES-256 is used when a 512-bit key and XTS mode are selected.

The intent of this requirement is to specify the approved AES modes that the ST Author may select for AES encryption of the appropriate information on the Field-Replaceable Nonvolatile Storage Device. For the first selection, the ST author should indicate the mode or modes supported by the TOE implementation. The second selection indicates the key size to be used, which is identical to that specified for FCS_CKM.1(b). The third selection must agree with the mode or modes chosen in the first selection. If multiple modes are supported, it may be clearer in the ST if this component was iterated.

A.1.2. FCS_COP.1(e) Cryptographic operation (Key Wrapping)

```
(selected in FCS_KYC_EXT.1.1)
Hierarchical to:    No other components.
Dependencies:   [[so]FDP_ITC.1 Import of user data without security attributes, or
    FDP_ITC.2 Import of user data with security attributes, or[/so]
    FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
    FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
```

FCS_COP.1.1(e) Refinement: The TSF shall perform **key wrapping** in accordance with a specified cryptographic algorithm **AES in the following modes and the cryptographic key size [selection: _128 bits, 256 bits]** that meet the following: **[ISO/IEC 18033-3 (AES), [selection:** ***NIST SP 800-38F, ISO/IEC 19772, no other standards***]].

Application Note:

This requirement is used in the body of the ST if the ST Author chooses to use key wrapping in the key chaining approach that is specified in FCS_KYC_EXT.1.

A.1.3. FCS_COP.1(f) Cryptographic operation (Key Encryption)

```
(selected from FCS_KYC_EXT.1.1)
Hierarchical to:    No other components.
Dependencies:   [[so]FDP_ITC.1 Import of user data without security attributes, or
    FDP_ITC.2 Import of user data with security attributes, or[/so]
    FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
    FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
```

FCS_COP.1.1(f) Refinement: The TSF shall perform **key encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [[selection:** ***CBC, GCM*****] mode]** and cryptographic key sizes [**selection:** ***128 bits, 256 bits***] that meet the following: [**AES as specified in ISO /IEC 18033-3, [selection:** ***CBC as specified in ISO/IEC 10116, GCM as specified in ISO/IEC 19772***].

Application Note:

This requirement is used in the body of the ST if the ST Author chooses to use AES encryption/decryption for protecting the keys as part of the key chaining approach that is specified in FCS_KYC_EXT.1.

A.1.4. FCS_COP.1(i) Cryptographic operation (Key Transport)

```
(selected in FCS_KYC_EXT.1.1)
Hierarchical to:    No other components.
Dependencies:   [[so]FDP_ITC.1 Import of user data without security attributes, or
    FDP_ITC.2 Import of user data with security attributes, or[/so]
    FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)]
    FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
```

FCS_COP.1.1(i) Refinement: The TSF shall perform **key transport** in accordance with a specified cryptographic algorithm **RSA in the following modes [selection: *KTS-OAEP, KTS-KEM-KWS*]** and the cryptographic key size **[selection: *2048 bits, 3072 bits*]** that meet the following: **NIST SP 800-56B, Revision 1**.

Application Note:

This requirement is used in the body of the ST if the ST Author chooses to use key transport in the key chaining approach that is specified in FCS_KYC_EXT.1.

A.1.5. FCS_SMC_EXT.1 Extended: Submask Combining

```
(selected in FCS_KYC_EXT.1.1)
Hierarchical to:    No other components.
Dependencies:   FCS_COP.1(c) Cryptographic operation (Hash Algorithm)
```

FCS_SMC_EXT.1.1 The TSF shall combine submasks using the following method [selection: *exclusive OR (XOR), SHA-256, SHA-512*] to generate an intermediary key or BEV.

Application Note:

This requirement specifies the way that a product may combine the various submasks by using either an XOR or an approved SHA-hash. The approved hash function is captured in FCS_COP.1(c) in Appendix D.3.1.

A.2. Protected Communications

As indicated in the FTP requirements, there are several methods by which conformant TOEs can mitigate threats against compromise of the communication channel between administrators, other portions of the TOE, or external IT entities. One of the secure communication protocols (IPsec, SSH, TLS, TLS/HTTPS) must be implemented in order to provide protected connectivity for (at a minimum) the audit server and remote administrators.

There are unique requirements associated with each of the protocol suites; these are specified in below. Depending on the selections for the FTP_ITC.1 and FTP_TRP.1 components, the ST author will need to include the associated SFRs and Assurance Activities in the ST.

A.2.1. FCS_IPSEC_EXT.1 Extended: IPsec selected

```
(selected in FTP_ITC.1.1, FTP_TRP.1.1)
Hierarchical to:    No other components.
Dependencies:       [so]FPT_ITT.1 Basic internal TSF data transfer protection,[/so]
    FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
    FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)
    FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
    FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
    FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
        FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
    FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)
```

Application Note:

In order to show that the TSF implements the RFCs in accordance with the requirements of this PP, the evaluator shall perform the assurance activities listed below.

The TOE is required to use the IPsec protocol to establish connections used to communicate with an IPsec Peer.

BRIANV - IMAGE TAG NEEDS TO BE ADDED TO EXTERNAL FILE

The evaluators shall minimally create a test environment equivalent to the test environment illustrated above. It is expected that the traffic generator is used to construct network packets and will provide the evaluator with the ability manipulate fields in the ICMP, IPv4, IPv6, UDP, and TCP packet headers. The evaluators must provide justification for any differences in the test environment.

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

Application Note:

RFC 4301 calls for an IPsec implementation to protect IP traffic through the use of a Security Policy Database (SPD). The SPD is used to define how IP packets are to be handled: PROTECT the packet (e.g., encrypt the packet), BYPASS the IPsec services (e.g., no encryption), or DISCARD the packet (e.g., drop the packet). The SPD can be implemented in various ways, including router access control lists, firewall rulesets, a “traditional” SPD, etc. Regardless of the implementation details, there is a notion of a “rule” that a packet is “matched” against and a resulting action that takes place.

While there must be a means to order the rules, a general approach to ordering is not mandated, as long as the SPD can distinguish the IP packets and apply the rules accordingly. There may be multiple SPDs (one for each network interface), but this is not required.

FCS_IPSEC_EXT.1.2 The TSF shall implement [selection: *tunnel mode, transport mode*].

FCS_IPSEC_EXT.1.3 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using [selection: *the cryptographic algorithms AES-CBC-128 (as specified by RFC 3602) together with a*

Secure Hash Algorithm (SHA)-based HMAC, AES-CBC-256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-GCM-128 as specified in RFC 4106, AES-GCM-256 as specified in RFC 4106].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [selection: *IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109*, [selection: *no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers*], and [selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]; *IKEv2 as defined in RFCs 5996*, [selection: *with no support for NAT traversal, with mandatory support for NAT traversal as specified in section 2.23*], and [selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]].

Application Note:

Either IKEv1 or IKEv2 support must be provided, although conformant TOEs can provide both; the first selection is used to make this choice. For IKEv1, the requirement is to be interpreted as requiring the IKE implementation conforming to RFC 2409 with the additions/modifications as described in RFC 4109. RFC 4304 identifies support for extended sequence numbers, which compliant TOEs can specify using the second selection. RFC 4868 identifies additional hash functions for use with both IKEv1 and IKEv2; if these functions are implemented, the third (for IKEv1) and fourth (for IKEv2) selection can be used.

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [selection: *IKEv1, IKEv2*] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 3602 and [selection: *AES-GCM-128, AES-GCM-256 as specified in RFC 5282, no other algorithm*].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [selection: *IKEv2 SA lifetimes can be established based on [selection: number of packets/number of bytes; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs]; IKEv1 SA lifetimes can be established based on [selection: number of packets/number of bytes ; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]].

Application Note:

The ST Author is afforded a selection based on the version of IKE in their implementation. If the lifetime limitations are configurable, then the evaluator verifies that the appropriate instructions for configuring these values are included in the operational guidance.

As far as SA lifetimes are concerned, the TOE can limit the lifetime based on the number of bytes transmitted, or the number of packets transmitted. Either packet-based or volume-based SA lifetimes are acceptable; the ST author makes the appropriate selection to indicate which type of lifetime limits are supported.

FCS_IPSEC_EXT.1.9 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [selection: *24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP, 5 (1536-bit MODP))*, [assignment: *other DH groups that are implemented by the TOE*], *no other DH groups*].

Application Note:

The above requires that the TOE support DH Group 14. If other groups are supported, then those should be selected (for groups 24, 19, 20, and 5) or specified in the assignment above; otherwise "no other DH groups" should be selected. This applies to IKEv1/IKEv2 exchanges.

FCS_IPSEC_EXT.1.10 The TSF shall ensure that all IKE protocols perform Peer Authentication using the [selection: *RSA*, *ECDSA*] algorithm and Pre-shared Keys.

Application Note:

The selected algorithm should correspond to an appropriate selection for FCS_COP.1(b). If IPsec is included in the TOE, the ST author also includes FIA_PSK_EXT from Appendix D.2.6.

A.2.2. FCS_TLS_EXT.1 Extended: TLS selected

```
(selected in FTP_ITC.1.1, FTP_TRP.1.1)
Hierarchical to:    No other components.
Dependencies:   FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)
    FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
    FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
    FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
    FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
    FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation).
```

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [selection: [so]TLS 1.0 (RFC 2246)[/so], TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)] supporting the following ciphersuites:

[so]Mandatory Ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA[/so]

Optional Ciphersuites:

[selection:

- [so]None[/so]
- *TLS_RSA_WITH_AES_128_CBC_SHA*
- *TLS_RSA_WITH_AES_256_CBC_SHA*
- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA*
- *TLS_RSA_WITH_AES_128_CBC_SHA256*
- *TLS_RSA_WITH_AES_256_CBC_SHA256*
- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA256*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA256*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA*

- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*
- *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384*

].

Application Note:

The ST author must make the appropriate selections and assignments to reflect the TLS implementation.

The ciphersuites to be tested in the evaluated configuration are limited by this requirement. The ST author should select the optional ciphersuites that are supported; if there are no ciphersuites supported other than the mandatory suites, then “None” should be selected. If administrative steps need to be taken so that the suites negotiated by the implementation are limited to those in this requirement, the appropriate instructions need to be contained in the guidance called for by AGD_OPE.

The Suite B algorithms (RFC 5430) listed above are the preferred algorithms for implementation. The TLS requirement may be changed in the next version of the HCD PP to comply with CNSSP 15 and NIST SP 800-131A.

A.2.3. FCS_SSH_EXT.1 Extended: SSH selected

```
(selected in FTP_ITC.1.1, FTP_TRP.1.1)
Hierarchical to:    No other components.
Dependencies:   FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)
    FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
    FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
    FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
    FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
    FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation).
```

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254, and [selection: *5656, 6668, no other RFCs*].

Application Note:

The ST author selects which of the additional RFCs to which conformance is being claimed. Note that these need to be consistent with selections in later elements of this component (e.g., cryptographic algorithms permitted).

In the next version of this PP, a requirement may be added regarding rekeying. The requirement would read "The TSF shall ensure that the SSH connection be rekeyed after no more than 228 packets have been transmitted using that key."

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [assignment: *number of bytes*] bytes in an SSH transport connection are dropped.

Application Note:

RFC 4253 provides for the acceptance of "large packets" with the caveat that the packets should be of "reasonable length" or dropped. The assignment should be filled in by the ST author with the maximum packet size accepted, thus defining "reasonable length" for the TOE.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, [selection: *AEAD_AES_128_GCM, AEAD_AES_256_GCM, no other algorithms*].

Application Note:

In the assignment, the ST author can select the AES-GCM algorithms, or "no other algorithms" if AES-GCM is not supported. If AES-GCM is selected, there should be corresponding FCS_COP entries in the ST.

FCS_SSH_EXT.1.5 The TSF shall ensure that the SSH transport implementation uses [selection: SSH_RSA, ecdsa-sha2-nistp256] and [selection: PGP-SIGN-RSA, PGP-SIGN-DSS, ecdsa-sha2-nistp384, no other public key algorithms,] as its public key algorithm(s).

FCS_SSH_EXT.1.6 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [selection: *HMAC-SHA1, HMAC-SHA1-96, HMAC-SHA2-256, HMAC-SHA2-512*].

Application Note:

RFC 6668 specifies the use of the SHA-2 algorithms in SSH.

FCS_SSH_EXT.1.7 The TSF shall ensure that diffie-hellman-group14-sha1 and [selection: ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, no other methods] are the only allowed key exchange method used for the SSH protocol.

A.2.4. FCS_HTTPS_EXT.1 Extended: HTTPS selected

```
(selected in FTP_ITC.1.1, FTP_TRP.1.1)
Hierarchical to:    No other components.
Dependencies:   FCS_TLS_EXT.1 Extended: TLS selected.
```

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

Application Note:

The ST author must provide enough detail to determine how the implementation is complying with the standard(s) identified; this can be done either by adding elements to this component, or by additional detail in the TSS.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

A.2.5. FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)

```
(selected with FCS_IPSEC_EXT.1.4)
Hierarchical to:    No other components.
Dependencies:   [[so]FDP_ITC.1 Import of user data without security attributes, or
    FDP_ITC.2 Import of user data with security attributes, or[/so]
    FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
    FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
    FCS_COP.1(c) Cryptographic operation (Hash Algorithm)
```

FCS_COP.1.1(g) Refinement: The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC-**[selection: ***SHA-1, SHA-224, SHA-256, SHA-384, SHA-512***], **key size** [assignment: **key size (in bits) used in HMAC**], **and message digest sizes** [selection: ***160, 224, 256, 384, 512***] **bits** that meet the following: **FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code, and FIPS PUB 180-3, “Secure Hash Standard.”**

A.2.6. FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition

```
(selected with FCS_IPSEC_EXT.1.4)
Hierarchical to: No other components.
Dependencies:   FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit
Generation)
```

Application Note:

The TOE must support pre-shared keys for use in the IPsec protocol. There are two types of pre-shared keys—text-based (which are required) and bit-based (which are optional)--supported by the TOE, as specified in the requirements below. The first type is referred to as “text-based pre-shared keys”, which refer to pre-shared keys that are entered by users as a string of characters from a standard character set, similar to a password. Such pre-shared keys must be conditioned so that the string of characters is transformed into a string of bits, which is then used as the key.

The second type is referred to as “bit-based pre-shared keys” (for lack of a standard term); this refers to keys that are either generated by the TSF on a command from the administrator, or input in "direct form" by an administrator. "Direct form" means that the input is used directly as the key, with no "conditioning" as was the case for text-based pre-shared keys. An example would be a string of hex *digits that represent the bits that comprise the key.*

The requirements below mandate that the TOE must support text-based pre-shared keys and optionally support bit-based pre-shared keys, although generation of the bit-based pre-shared keys may be done either by the TOE or in the Operational Environment.

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for IPsec.

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that are:

- 22 characters in length and [selection: [assignment: *other supported lengths*], *no other lengths*];
- composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")").

FIA_PSK_EXT.1.3 The TSF shall condition the text-based pre-shared keys by using [selection: *SHA-1, SHA-256, SHA-512*, [assignment: *method of conditioning text string*]] and be able to [selection: *use no other pre-shared keys; accept bit-based pre-shared keys; generate bit-based pre-shared keys using the random bit generator specified in FCS_RBG_EXT.1*].

Application Note:

For the length of the text-based pre-shared keys, a common length (22 characters) is required to help promote interoperability. If other lengths are supported they should be listed in the assignment; this assignment can also specify a range of values (e.g., "lengths from 5 to 55 characters") as well.

In the second selection for FIA_PSK_EXT.1.3, the ST author fills in the method by which the text string entered by the administrator is "conditioned" into the bit string used as the key. This can be done by using one of the specified hash functions, or some other method through the assignment statement. If "bit-based pre-shared keys" is selected, the ST author specifies whether the TSF merely accepts bit-based pre-shared keys, or is capable of generating them. If it generates them, the requirement specified that they must be generated using the RBG specified by the requirements. If the use of bit-based pre-shared keys is not supported, the ST author chooses "use no other pre-shared keys".

A.3. Trusted Update

A.3.1. FCS_COP.1(c) Cryptographic operation (Hash Algorithm)

```
(selected in FPT_TUD_EXT.1.3, or with FCS_SNI_EXT.1.1)
Hierarchical to:    No other components.
Dependencies:   No dependencies.
```

FCS_COP.1.1(c) Refinement: The TSF shall perform **cryptographic hashing services** in accordance with [selection: ***SHA-1, SHA-256, SHA-384, SHA-512***] that meet the following: [**ISO/IEC 10118-3:2004**].

Application Note (for O.STORAGE_ENCRYPTION):

The hash selection should be consistent with the overall strength of the algorithm used for

FCS_COP.1(d). (SHA 256 should be chosen for AES 128-bit keys, SHA 512 should be chosen for AES-256-bit keys) The selection of the standard is made based on the algorithms selected.

Vendors are strongly encouraged to implement updated protocols that support the SHA-2 family; until updated protocols are supported, this PP allows support for SHA-1 implementations in compliance with SP 800-131A.

A.4. Passphrase-based Key Entry

The SFRs in this section are to be incorporated in the ST to support the optional Passphrase-based Key Entry function.

A.4.1. FCS_PCC_EXT.1 Extended: Cryptographic Password Construct and Conditioning

```
(for O. STORAGE_ENCRYPTION)
Hierarchical to:    No other components
Dependencies:   FCS_COP.1(h) Cryptographic Operation (for keyed-hash message
authentication)
```

FCS_PCC_EXT.1.1 A password used by the TSF to generate a password authorization factor shall enable up to [assignment: *positive integer of 64 or more*] characters in the set of {upper case characters, lower case characters, numbers, and [assignment: *other supported special characters*]} and shall perform Password-based Key Derivation Functions in accordance with a specified cryptographic algorithm [HMAC-[selection: *SHA-256, SHA-384, SHA-512*]], with [assignment: *positive integer of 1000 or more*] iterations, and output cryptographic key sizes [selection: *128, 256*] bits that meet the following: [**NIST SP 800-132**].

Application Note:

This SFR is conditionally required if the manual entry of a drive encryption passphrase is supported by the TOE.

A.4.2. FCS_KDF_EXT□Extended: Cryptographic Key Derivation

```
(for O. STORAGE_ENCRYPTION)
Hierarchical to:    No other components
Dependencies:  FCS_COP.1(h) Cryptographic Operation (for keyed-hash message
authentication),
    [if selected: FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit
Generation)]
```

FCS_KDF_EXT.1.1 The TSF shall accept [selection: *a RNG generated submask as specified in FCS_RBG_EXT.1, a conditioned password submask, imported submask*] to derive an intermediate key, as defined in [selection: *NIST SP 800-108 [selection: KDF in Counter Mode, KDF in Feedback Mode, KDF in Double-Pipeline Iteration Mode], NIST SP 800-132*], using the keyed-hash functions specified in FCS_COP.1(h), such that the output is at least of equivalent security strength (in number of bits) to the BEV.

A.4.3. FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)

```
(selected with FCS_PCC_EXT.1, FCS_KDF_EXT.1.1)
Hierarchical to:    No other components.
Dependencies:   [[so]FDP_ITC.1 Import of user data without security attributes, or
    FDP_ITC.2 Import of user data with security attributes, or[/so]
    FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
    FCS_COP.1(c) Cryptographic operation (Hash Algorithm),
    FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
```

FCS_COP.1.1(h) Refinement: The TSF shall perform [**keyed-hash message authentication**] in accordance with [**selection:** ***HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512***] and cryptographic key sizes [assignment: ***key size (in bits) used in HMAC***] that meet the following: [**ISO/IEC 9797-2:2011, Section** 7 **"MAC Algorithm 2"; ISO/IEC 10118**].

Application Note:

The key size [k] in the assignment falls into a range between L1 and L2 (defined in ISO/IEC 10118 for the appropriate hash function for example for SHA-256 L1 = 512, L2 =256) where L2 ≤ k ≤ L1.

A.4.4. FCS_SNI_EXT.1 Extended: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)

```
(selected with FCS_PCC_EXT.1, FCS_KDF_EXT.1.1)
Hierarchical to:    No other components
Dependencies:   FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit
Generation)
```

FCS_SNI_EXT.1.1 The TSF shall only use salts that are generated by a RNG as specified in FCS_RBG_EXT.1.

FCS_SNI_EXT.1.2 The TSF shall only use unique nonces with a minimum size of [64] bits.

FCS_SNI_EXT.1.3 The TSF shall create IVs in the following manner: [

- CBC: IVs shall be non-repeating,
- CCM: Nonce shall be non-repeating.
- XTS: No IV. Tweak values shall be non-negative integers, assigned consecutively, and starting at an arbitrary non-negative integer,
- GCM: IV shall be non-repeating. The number of invocations of GCM shall not exceed 2^32 for a given secret key.

].

Application Note:

This SFR is conditionally required if the manual entry of a drive encryption passphrase is supported by the TOE.

Appendix B: Optional Requirements

This should remain if there are any optional requirements

ST authors are free to choose none, some or all SFRs defined in this chapter. Just the fact that a product supports a certain functionality does not mandate to add any SFR defined in this chapter.

This section should contain any SFRs considered "optional" by the iTC. If there are none, then that should be stated (that there are no optional requirements in the cPP). The section should not be removed, but it should be explicitly stated there are no optional requirements.

B.1. Internal Audit Log Storage

The SFRs in this section are to be incorporated in the ST to support the optional Internal Audit Log Storage function.

B.1.1. FAU_SAR.1 Audit review

```
(for O.AUDIT)
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
```

FAU_SAR.1.1 The TSF shall provide [assignment: ***an Administrator***] with the capability to read **all records** from the audit records.

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

B.1.2. FAU_SAR.2 Restricted audit review

```
(for O.AUDIT)
Hierarchical to: No other components.
Dependencies: FAU_SAR.1 Audit review
```

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

B.1.3. FAU_STG.1 Protected audit trail storage

```
(for O.AUDIT)
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
```

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to **prevent** unauthorised modifications to the stored audit records in the audit trail.

B.1.4. FAU_STG.4 Prevention of audit data loss

```
(for O.AUDIT)
Hierarchical to: FAU_STG.3 Action in case of possible audit data loss
Dependencies: FAU_STG.1 Protected audit trail storage
```

FAU_STG.4.1 Refinement: The TSF shall [selection, choose one of: ***[so]"ignore audited events"[/so]***, *"prevent audited events, except those taken by the authorised user with special rights"*, *"overwrite the oldest stored audit records"*] and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full.

B.2. Image Overwrite

The SFRs in this section are to be incorporated in the ST to support the optional Image Overwrite function.

B.2.1. FDP_RIP.1(a) Subset residual information protection

```
(for O.IMAGE_OVERWRITE)
Hierarchical to: No other components.
Dependencies: No dependencies.
```

FDP_RIP.1.1(a) Refinement: The TSF shall ensure that any previous information content of a resource is made unavailable **by overwriting data** upon the **deallocation of the resource from** the following objects: **D.USER.DOC**.

B.3. Purge Data

The SFRs in this section are to be incorporated in the ST to support the optional Purge Data function.

B.3.1. FDP_RIP.1(b) Subset residual information protection

```
(for O.PURGE_DATA)
Hierarchical to: No other components.
Dependencies: No dependencies.
```

FDP_RIP.1.1(b) Refinement: The TSF shall ensure that any previous **customer-supplied** information content of a resource is made unavailable upon the **request of an Administrator to** the following objects: **D.USER**, **D.TSF**.

B.4. Asymmetric Key Generation

The SFR in this section is used if the TOE generates asymmetric key pairs for communications.

B.4.1. FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)

```
(for O.COMMS_PROTECTION)
Hierarchical to:    No other components.
Dependencies:   [[so]FCS_CKM.2 Cryptographic key distribution, or[/so]
    FCS_COP.1(b) Cryptographic Operation (for signature generation/ verification)
    FCS_COP.1(i) Cryptographic operation (Key Transport)]
    FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
```

FCS_CKM.1.1(a) Refinement: The TSF shall generate **asymmetric** cryptographic keys **used for key establishment** in accordance **with [selection:**

- ***NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes;***
- ***NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard")***
- ***NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes***

] and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.

Application Note:

The ST author selects the key generation scheme used for key establishment and device authentication. If multiple schemes are supported, then the ST author should iterate this component to capture this capability. When key generation is used for device authentication, the public key is expected to be associated with an X.509v3 certificate. If the TOE acts as a receiver in the RSA key establishment *scheme, the TOE does not need to implement RSA key generation.*

Since the domain parameters to be used are specified by the requirements of the protocol in this PP, it is not expected that the TOE will generate domain parameters, and therefore there is no additional domain parameter validation needed when the TOE complies with the protocols specified in this PP.

SP 800-56B references (but does not mandate) key generation according to FIPS 186-3. For purposes of compliance in this version of the HCD PP, RSA key pair generation according to FIPS 186-4 is allowed in order for the TOE to claim conformance to SP 800-56B.

The generated key strength of 2048-bit DSA and rDSA keys need to be equivalent to, or greater than, a symmetric key strength of 112 bits. See NIST Special Publication 800-57, “Recommendation for Key Management” for information about equivalent key strengths.

Appendix C: Extended Component Definitions

This appendix contains the definitions for the extended requirements that are used in the cPP, including those used in Consistency Rationale and Selection-Based Requirements .

(Note: formatting conventions for selections and assignments in this chapter are those in [CC2].)

> If Extended SFRs are created they must be defined here. An example is copied here from the Biometrics Security PP-Module (because it is short).

C.1. (FAU)

C.1.1. FAU_STG_EXTExtended: External Audit Trail Storage

C.1.1.1. Family Behaviour

This family defines requirements for the TSF to ensure that secure transmission of audit data from TOE to an External IT Entity.

C.1.1.2. Component Leveling

Component leveling

```
+-----------------------------------------+
|                                         |     +---+
| FAU_STG_EXT External Audit Trail Storage +---->| 1 |
|                                         |     +---+
+-----------------------------------------+
```

FAU_STG_EXT.1 External Audit Trail Storage requires the TSF to use a trusted channel implementing a secure protocol.

C.1.1.3. Management:

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

- The TSF shall have the ability to configure the cryptographic functionality.

C.1.1.4. Audit

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

- There are no auditable events foreseen.

C.1.1.5. FAU_STG_EXT.1Extended: Protected Audit Trail Storage

```
Hierarchical to:    No other components.
Dependencies:   FAU_GEN.1   Audit data generation,
    FTP_ITC.1   Inter-TSF  trusted channel
```

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an External IT Entity using a trusted channel according to FTP_ITC.1.

C.1.1.6. Rationale

The TSF is required that the transmission of generated audit data to an External IT Entity which relies on a non-TOE audit server for storage and review of audit records. The storage of these audit records and the ability to allow the administrator to review these audit records is provided by the Operational Environment in that case. The Common Criteria does not provide a suitable SFR for the transmission of audit data to an External IT Entity.

This extended component protects the audit records, and it is therefore placed in the FAU class with a single component.

C.2. (FCS)

C.2.1. FCS_CKM_EXTExtended: Cryptographic Key Management

C.2.1.1. Family Behaviour

This family addresses the management aspects of cryptographic keys. Especially, this extended component is intended for cryptographic key destruction.

C.2.1.2. Component Leveling

Component leveling

```
    +-----------------------------------------+
    |                                         |     +---+
    | FCS_CKM_EXT Cryptographic Key Management +---->| 4 |
    |                                         |     +---+
    +-----------------------------------------+
```

FCS_CKM_EXT.4 Cryptographic Key Material Destruction ensures not only keys but also key materials that are no longer needed are destroyed by using an approved method.

C.2.1.3. Management:

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

- There are no management actions foreseen.

C.2.1.4. Audit

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

- There are no auditable events foreseen.

C.2.1.5. FCS_CKM_EXT.4Extended: Cryptographic Key Material Destruction

```
Hierarchical to:    No other components.
Dependencies:   [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or
    FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)],
    FCS_CKM.4 Cryptographic key destruction
```

FCS_CKM_EXT.4.1 The TSF shall destroy all plaintext secret and private cryptographic keys and cryptographic critical security parameters when no longer needed.

C.2.1.6. Rationale

Cryptographic Key Material Destruction is to ensure the keys and key materials that are no longer needed are destroyed by using an approved method, and the Common Criteria does not provide a suitable SFR for the Cryptographic Key Material Destruction.

This extended component protects the cryptographic key and key materials against exposure, and it is therefore placed in the FCS class with a single component.

C.2.2. FCS_HTTPS_EXTExtended: HTTPS selected

C.2.2.1. Family Behaviour

Components in this family define requirements for protecting remote management sessions between the TOE and a Security Administrator. This family describes how HTTPS will be implemented. This is a new family defined for the FCS Class.

C.2.2.2. Component Leveling

Component leveling

```
    +------------------------------------------+
    |                                          |     +---+
    | FCS_HTTPS_EXT HTTPS selected             +---->| 1 |
    |                                          |     +---+
    +------------------------------------------+
```

FCS_HTTPS_EXT.1 HTTPS selected, requires that HTTPS be implemented according to RFC 2818 and supports TLS.

C.2.2.3. Management

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

- There are no management actions foreseen.

C.2.2.4. Audit

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

- Failure of HTTPS session establishment

C.2.2.5. FCS_HTTPS_EXT.1Extended: HTTPS selected

```
Hierarchical to:    No other components.
Dependencies:   [so]No dependencies[/so] FCS_TLS_EXT.1 Extended: TLS selected
```

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

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

C.2.2.6. Rationale

HTTPS is one of the secure communication protocols, and the Common Criteria does not provide a suitable SFR for the communication protocols using cryptographic algorithms.

This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

C.2.3. FCS_IPSEC_EXT□Extended: IPsec selected

C.2.3.1. Family Behaviour

This family addresses requirements for protecting communications using IPsec.

C.2.3.2. Component Leveling

Component leveling

```
    +------------------------------------------+
    |                                          |     +---+
    | FCS_IPSEC_EXT IPsec                      +---->| 1 |
    |                                          |     +---+
    +------------------------------------------+
```

FCS_IPSEC_EXT.1 IPsec requires that IPsec be implemented as specified.

C.2.3.3. Management

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

- There are no management actions foreseen.

C.2.3.4. Audit

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

- Failure to establish an IPsec SA

C.2.3.5. FCS_IPSEC_EXT.1Extended: IPsec selected

```
Hierarchical to:    No other components.
Dependencies:   FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition
    FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)
    FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
    FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
    FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
        FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
    FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)
```

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall implement [selection: tunnel mode, transport mode].

FCS_IPSEC_EXT.1.3 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using [selection: *the cryptographic algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC-256 (as specified by RFC 3602) together with a*

Secure Hash Algorithm (SHA)-based HMAC, AES-GCM-128 as specified in RFC 4106, AES-GCM-256 as specified in RFC 4106].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [selection: *IKEv1 using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109*, [selection: *no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers*], and [selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]; IKEv2 as defined in RFCs 5996 [selection: *with no support for NAT traversal, with mandatory support for NAT traversal as specified in section 2.23*], and [selection: *no other RFCs for hash functions, RFC 4868 for hash functions*]].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [selection: *IKEv1, IKEv2*] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC-256 as specified in RFC 3602 and [selection: *AES-GCM-128, AES-GCM-256 as specified in RFC 5282, no other algorithm*].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [selection: *IKEv2 SA lifetimes can be established based on* [selection: *number of packets/number of bytes; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]; *IKEv1 SA lifetimes can be established based on* [selection: *number of packets/number of bytes; length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs*]].

FCS_IPSEC_EXT.1.9 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [selection: *24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP, 5 (1536-bit MODP))*, [assignment: *other DH groups that are implemented by the TOE], no other DH groups*].

FCS_IPSEC_EXT.1.10 The TSF shall ensure that all IKE protocols perform Peer Authentication using the [selection: *RSA, ECDSA*] algorithm and Pre-shared Keys.

C.2.3.6. Rationale

IPsec is one of the secure communication protocols, and the Common Criteria does not provide a suitable SFR for the communication protocols using cryptographic algorithms.

This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

C.2.4. FCS_KDF_EXTExtended: Cryptographic Key Derivation

C.2.4.1. Family Behaviour

This family specifies the means by which an intermediate key is derived from a specified set of submasks.

C.2.4.2. Component Leveling

Component leveling

```
    +------------------------------------------+
    |                                          |     +---+
    | FCS_KDF_EXT Cryptographic Key Derivation +---->| 1 |
    |                                          |     +---+
    +------------------------------------------+
```

FCS_KDF_EXT.1 Cryptographic Key Derivation requires the TSF to derive intermediate keys from submasks using the specified hash functions.

C.2.4.3. Management

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

- There are no management actions foreseen.

C.2.4.4. Audit

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

- There are no auditable events foreseen.

C.2.4.5. FCS_KDF_EXT.1 Extended: Cryptographic Key Derivation

```
Hierarchical to: No other components
Dependencies:  FCS_COP.1(h) Cryptographic Operation (for keyed-hash message
authentication),
    [if selected: FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit
Generation)]
```

FCS_KDF_EXT.1.1 The TSF shall accept [selection: *a RNG generated submask as specified in FCS_RBG_EXT.1, a conditioned password submask, imported submask*] to derive an intermediate key, as defined in [selection: *NIST SP 800-108* [selection: *KDF in Counter Mode, KDF in Feedback Mode, KDF in Double-Pipeline Iteration Mode*], *NIST SP 800-132*], using the keyed-hash functions specified in FCS_COP.1(h), such that the output is at least of equivalent security strength (in number of bits) to the BEV.

C.2.4.6. Rationale

The TSF is required to specify the means by which an intermediate key is derived from a specified set of submasks using the specified hash functions.

This extended component protects the Data Encryption Keys using cryptographic algorithms in the maintained key chains, and it is therefore placed in the FCS class with a single component.

C.2.5. FCS_KYC_EXTExtended: Cryptographic Operation (Key Chaining)

C.2.5.1. Family Behaviour

This family provides the specification to be used for using multiple layers of encryption keys to ultimately secure the protected data encrypted on the storage.

C.2.5.2. Component Leveling

Component leveling

```
    +------------------------------------------+
    |                                          |     +---+
    | FCS_KYC_EXT Key Chaining                 +---->| 1 |
    |                                          |     +---+
    +------------------------------------------+
```

FCS_KYC_EXT Key Chaining, requires the TSF to maintain a key chain and specifies the characteristics of that chain.

C.2.5.3. Management

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

- There are no management actions foreseen.

C.2.5.4. Audit

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

- There are no auditable events foreseen.

C.2.5.5. FCS_KYC_EXT.1Extended: Key Chaining

```
Hierarchical to:    No other components.
Dependencies:   [FCS_COP.1(e) Cryptographic operation (Key Wrapping), FCS_SMC_EXT.1
Extended: Submask Combining,
FCS_COP.1(i) Cryptographic operation (Key Transport), FCS_KDF_EXT.1 Cryptographic
Operation (Key Derivation), and/or
FCS_COP.1(f) Cryptographic operation (Key Encryption)].
```

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: [selection: *one, using a submask as the BEVor DEK; intermediate keys originating from one or more submask(s) to the BEV or DEK using the following method(s)*: [selection: *key wrapping as specified in FCS_COP.1(e), key combining as specified in FCS_SMC_EXT.1, key encryption as specified in FCS_COP.1(f), key derivation as specified in FCS_KDF_EXT.1, key transport as specified in FCS_COP.1(i)*]] while maintaining an effective strength of [selection: *128 bits, 256 bits*].

C.2.5.6. Rationale

Key Chaining ensures that the TSF maintains the key chain, and also specifies the characteristics of that chain. However, the Common Criteria does not provide a suitable SFR for the management of multiple layers of encryption key to protect encrypted data.

This extended component protects the TSF data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

C.2.6. FCS_PCC_EXT Extended: Cryptographic Password Construction and Conditioning

C.2.6.1. Family Behaviour

This family ensures that passwords used to produce the BEV are robust (in terms of their composition) and are conditioned to provide an appropriate-length bit string.

C.2.6.2. Component Leveling

Component leveling

```
    +-------------------------------------------------------------+
    |                                                             |    +---+
    | FCS_PCC_EXT Cryptographic Password Construction and Conditioning +---->| 1 |
    |                                                             |    +---+
    +-------------------------------------------------------------+
```

FCS_PCC_EXT.1 Cryptographic Password Construction and Conditioning, requires the TSF to accept passwords of a certain composition and condition them appropriately.

C.2.6.3. Management

No specific management functions are identified

C.2.6.4. Audit

There are no auditable events foreseen.

C.2.6.5. FCS_PCC_EXT.1 Extended: Cryptographic Password Construction and Conditioning

```
Hierarchical to:    No other components
Dependencies:   FCS_COP.1(h) Cryptographic Operation (for keyed-hash message
authentication)
```

FCS_PCC_EXT.1.1 A password used by the TSF to generate a password authorization factor shall enable up to [assignment: *positive integer of 64 or more*] characters in the set of {upper case characters, lower case characters, numbers, and [assignment: *other supported special characters*]} and shall perform Password-based Key Derivation Functions in accordance with a specified cryptographic algorithm [*HMAC*-[selection: *SHA-256, SHA-384, SHA-512*]], with [assignment: *positive* *integer of 1000 or more*] iterations, and output cryptographic key sizes [selection: *128, 256*] bits that meet the following: [assignment: *PBKDF recommendation or specification*].

C.2.6.6. Rationale

The TSF is required to ensure that passwords used to produce the BEV are robust (in terms of their composition) and are conditioned to provide an appropriate-length bit string.

This extended component protects the Data Encryption Keys using cryptographic algorithms and Robust BEV in the maintained key chains, and it is therefore placed in the FCS class with a single component.

C.2.7. FCS_RBG_EXTExtended: Cryptographic Operation (Random Bit Generation)

C.2.7.1. Family Behaviour

This family defines requirements for random bit generation to ensure that it is performed in accordance with selected standards and seeded by an entropy source.

C.2.7.2. Component Leveling

Component leveling

```
    +-------------------------------------------+
    |                                           |     +---+
    | FCS_RBG_EXT Random Bit Generation         +---->| 1 |
    |                                           |     +---+
    +-------------------------------------------+
```

FCS_RBG_EXT.1 Random Bit Generation requires random bit generation to be performed in accordance with selected standards and seeded by an entropy source.

C.2.7.3. Management

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

- There are no management actions foreseen.

C.2.7.4. Audit

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

- There are no auditable events foreseen.

C.2.7.5. FCS_RBG_EXT.1Extended: Random Bit Generation

```
Hierarchical to:    No other components.
Dependencies:   No dependencies.
```

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with [selection: *ISO/IEC 18031:2011, NIST SP 800-90A*] using [selection: *Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)*].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from [selection: [assignment: *number of software-based sources*] *software-based noise source(s)*, [assignment: *number of hardware-based sources*] *hardware-based noise source(s)*] with a minimum of [selection: *128 bits, 256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security strength table for hash functions”, of the keys and hashes that it will generate.

C.2.7.6. Rationale

Random bits/number will be used by the SFRs for key generation and destruction, and the Common Criteria does not provide a suitable SFR for the random bit generation.

This extended component ensures the strength of encryption keys, and it is therefore placed in the FCS class with a single component.

C.2.8. FCS_SMC_EXT—Extended: Submask Combining

C.2.8.1. Family Behaviour

This family defines the means by which submasks are combined, if the TOE supports more than one submask being used to derive or protect the BEV.

C.2.8.2. Component Leveling

Component leveling

```
    +------------------------------------------+
    |                                          |     +---+
    | FCS_SMC_EXT Submask combining            +---->| 1 |
    |                                          |     +---+
    +------------------------------------------+
```

FCS_SMC_EXT.1 Submask combining requires the TSF to combine the submasks in a predictable fashion.

C.2.8.3. Management

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

- There are no management actions foreseen.

C.2.8.4. Audit

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

- There are no auditable events foreseen.

C.2.8.5. FCS_SMC_EXT.1Extended: Submask Combining

```
Hierarchical to:    No other components.
Dependencies:   FCS_COP.1(c) Cryptographic operation (Hash Algorithm)
```

FCS_SMC_EXT.1.1 The TSF shall combine submasks using the following method [selection: *exclusive OR (XOR), SHA-256, SHA-512*] to generate an intermediary key or BEV.

C.2.8.6. Rationale

Submask Combining is to ensure the TSF combine the submasks in order to derive or protect the BEV.

This extended component protects the TSF data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

C.2.9. FCS_SNI_EXT Extended: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation

C.2.9.1. Family Behaviour

This family ensures that salts, nonces, and IVs are well formed.

C.2.9.2. Component Leveling

Component leveling

```


+-------------------------------------------------------------------------------------
----+
    |
|     +---+
    | FCS_SNI_EXT Cryptographic Operation (Salt, Nonce, and Initialization Vector
Generation) +---->| 1 |
    |
|     +---+

+-------------------------------------------------------------------------------------
----+
```

FCS_SNI_EXT.1 Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation), requires the generation of salts, nonces, and IVs to be used by the cryptographic components of the TOE to be performed in the specified manner.

C.2.9.3. Management

No specific management functions are identified

C.2.9.4. Audit

There are no auditable events foreseen.

C.2.9.5. FCS_SNI_EXT.1 Extended: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)

```
Hierarchical to:    No other components
Dependencies:   FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit
Generation)
```

FCS_SNI_EXT.1.1 The TSF shall only use salts that are generated by a RNG as specified in FCS_RBG_EXT.1.

FCS_SNI_EXT.1.2 The TSF shall only use unique nonces with a minimum size of [64] bits.

FCS_SNI_EXT.1.3 The TSF shall create IVs in the following manner: [

CBC: IVs shall be non-repeating,

CCM: Nonce shall be non-repeating.

XTS: No IV. Tweak values shall be non-negative integers, assigned consecutively, and starting at an arbitrary non-negative integer,

GCM: IV shall be non-repeating. The number of invocations of GCM shall not exceed 2^32 for a given secret key.

].

C.2.9.6. Rationale

The TSF is required to ensure that the generation of salts, nonces, and IVs to be used by the cryptographic components of the TOE is to be performed in the specified manner.

This extended component protects the communication data and storage data using cryptographic algorithms with specified Salt, Nonce and Initialization Vector Generation, and it is therefore placed in the FCS class with a single component.

C.2.10. FCS_SSH_EXT Extended: SSH selected

C.2.10.1. Family Behaviour

This family addresses the ability for a server and/or a client to offer SSH to protect data between a client and the server using the SSH protocol.

C.2.10.2. Component Leveling

Component leveling

```
    +------------------------------------------+
    |                                          |     +---+
    | FCS_SSH_EXT SSH selected                 +---->| 1 |
    |                                          |     +---+
    +------------------------------------------+
```

FCS_SSH_EXT.1 SSH selected, requires the SSH protocol implemented as specified.

C.2.10.3. Management

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

- There are no management actions foreseen.

C.2.10.4. Audit

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

- Failure of SSH session establishment

C.2.10.5. FCS_SSH_EXT.1 Extended: SSH selected

```
Hierarchical to:    No other components.
Dependencies:   [so]No dependencies[/so] FCS_CKM.1(a) Cryptographic Key Generation
(for asymmetric keys)
    FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
    FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
    FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
    FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
    FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation).
```

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254, and [selection: *5656, 6668, no other RFCs*].

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [assignment: *number of bytes*] bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, [selection: *AEAD_AES_128_GCM, AEAD_AES_256_GCM, no other algorithms*].

FCS_SSH_EXT.1.5 The TSF shall ensure that the SSH transport implementation uses [selection: *SSH_RSA*, *ecdsa-sha2-nistp256*] and [selection: *PGP-SIGN-RSA*, *PGP-SIGN-DSS*, *ecdsa-sha2-nistp384*, *no other public key algorithms*] as its public key algorithm(s).

FCS_SSH_EXT.1.6 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [selection: *HMAC-SHA1*, *HMAC-SHA1-96*, *HMAC-SHA2-256*, *HMAC-SHA2-512*].

FCS_SSH_EXT.1.7 The TSF shall ensure that diffie-hellman-group14-sha1 and [selection: *ecdh-sha2-nistp256*, *ecdh-sha2-nistp384*, *ecdh-sha2-nistp521*, *no other methods*] are the only allowed key exchange method used for the SSH protocol.

C.2.10.6. Rationale

SSH is one of the secure communication protocols, and the Common Criteria does not provide a suitable SFR for the communication protocols using cryptographic algorithms.

This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

C.2.11. FCS_TLS_EXT□Extended: TLS selected

C.2.11.1. Family Behaviour

This family addresses the ability for a server and/or a client to use TLS to protect data between a client and the server using the TLS protocol.

C.2.11.2. Component Leveling

Component leveling

```
+----------------------------------------+
|                                        |    +---+
| FCS_TLS_EXT TLS selected               +---->| 1 |
|                                        |    +---+
+----------------------------------------+
```

FCS_TLS_EXT.1 TLS selected, requires the TLS protocol implemented as specified.

C.2.11.3. Management

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

- There are no management actions foreseen.

C.2.11.4. Audit

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

- Failure of TLS session establishment

C.2.11.5. FCS_TLS_EXT.1Extended: TLS selected

```
Hierarchical to:    No other components.
Dependencies:   [so]No dependencies[/so] FCS_CKM.1(a) Cryptographic Key Generation
(for asymmetric keys)
    FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
    FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
    FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
    FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
    FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation).
```

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [selection: [so]TLS 1.0 (RFC 2246),[/so] *TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)*] supporting the following ciphersuites:

[so]Mandatory Ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA[/so]

Optional Ciphersuites:

[selection:

- [so]None[/so]
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_ SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

].

C.2.11.6. Rationale

TLS is one of the secure communication protocols, and the Common Criteria does not provide a suitable SFR for the communication protocols using cryptographic algorithms.

This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

C.3. (FDP)

C.3.1. FDP_DSK_EXT Extended: Protection of Data on Disk

C.3.1.1. Family Behaviour

This family is to mandate the encryption of all protected data written to the storage.

C.3.1.2. Component Leveling

Component leveling

```
+------------------------------------------+
|                                          |     +---+
| FDP_DSK_EXT Protection of Data on Disk   +---->| 1 |
|                                          |     +---+
+------------------------------------------+
```

FDP_DSK_EXT.1 Extended: Protection of Data on Disk, requires the TSF to encrypt all the Confidential TSF and User Data stored on the Field-Replaceable Nonvolatile Storage Devices in order to avoid storing these data in plaintext on the devices.

C.3.1.3. Management

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

- There are no management actions foreseen.

C.3.1.4. Audit

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

- There are no auditable events foreseen.

C.3.1.5. FDP_DSK_EXT.1Extended: Protection of Data on Disk

```
Hierarchical to:    No other components.
Dependencies:   FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption)
```

FDP_DSK_EXT.1.1 The TSF shall [selection: *perform encryption in accordance with FCS_COP.1(d), use a self-encrypting Field-Replaceable Nonvolatile Storage Device that is separately CC certified to conform to the FDE EE cPP*] such that any Field-Replaceable Nonvolatile Storage Device contains no plaintext User Document Data and no plaintext confidential TSF Data.

FDP_DSK_EXT.1.2 The TSF shall encrypt all protected data without user intervention.

C.3.1.6. Rationale

Extended: Protection of Data on Disk is to specify that encryption of any confidential data without user intervention, and the Common Criteria does not provide a suitable SFR for the Protection of Data on Disk.

This extended component protects the Data on Disk, and it is therefore placed in the FDP class with a single component.

C.3.2. FDP_FXS_EXTExtended: Fax Separation

C.3.2.1. Family Behaviour

This family addresses the requirements for separation between Fax PSTN line and the LAN to which TOE is connected.

C.3.2.2. Component Leveling

Component leveling

```
    +-------------------------------------------+
    |                                           |     +---+
    | FDP_FXS_EXT Fax Separation                +---->| 1 |
    |                                           |     +---+
    +-------------------------------------------+
```

FDP_FXS_EXT.1 Fax Separation, requires the fax interface cannot be used to create a network bridge between a PSTN and a LAN to which TOE is connected.

C.3.2.3. Management

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

- There are no management actions foreseen.

C.3.2.4. Audit

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

- There are no auditable events foreseen.

C.3.2.5. FDP_FXS_EXT.1 Extended: Fax separation

```
Hierarchical to:    No other components.
Dependencies:   No dependencies.
```

FDP_FXS_EXT.1.1 The TSF shall prohibit communication via the fax interface, except transmitting or receiving User Data using fax protocols.

C.3.2.6. Rationale

Fax Separation is to protect a LAN against attack from PSTN line, and the Common Criteria does not provide a suitable SFR for the Protection of TSF or User Data.

This extended component protects the TSF Data or User Data, and it is therefore placed in the FDP class with a single component.

C.4. (FIA)

C.4.1. FIA_PMG_EXTExtended: Password Management

C.4.1.1. Family Behaviour

This family defines requirements for the attributes of passwords used by administrative users to ensure that strong passwords and passphrases can be chosen and maintained.

C.4.1.2. Component Leveling

Component leveling

```
    +-------------------------------------------+
    |                                           |     +---+
    | FIA_PMG_EXT Password management           +---->| 1 |
    |                                           |     +---+
    +-------------------------------------------+
```

FIA_PMG_EXT.1 Password management requires the TSF to support passwords with varying composition requirements, minimum lengths, maximum lifetime, and similarity constraints.

C.4.1.3. Management

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

- There are no management actions foreseen.

C.4.1.4. Audit

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

- There are no auditable events foreseen.

C.4.1.5. FIA_PMG_EXT.1Extended: Password management

```
Hierarchical to:    No other components.
Dependencies:   No dependencies.
```

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for User passwords:

- Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: *“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”*, [assignment: *other characters*]];
- Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater.

C.4.1.6. Rationale

Password Management is to ensure the strong authentication between the endpoints of communication, and the Common Criteria does not provide a suitable SFR for the Password Management.

This extended component protects the TOE by means of password management, and it is therefore placed in the FIA class with a single component.

C.4.2. FIA_PSK_EXTExtended: Pre-Shared Key Composition

C.4.2.1. Family Behaviour

This family defines requirements for the TSF to ensure the ability to use pre-shared keys for IPsec.

C.4.2.2. Component Leveling

Component leveling

```
    +-------------------------------------------+
    |                                           |     +---+
    | FIA_PSK_EXT Pre-Shared Key Composition   +---->| 1 |
    |                                           |     +---+
    +-------------------------------------------+
```

FIA_PSK_EXT.1 Pre-Shared Key Composition, ensures authenticity and access control for updates.

C.4.2.3. Management

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

- There are no management actions foreseen.

C.4.2.4. Audit

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

- There are no auditable events foreseen.

C.4.2.5. FIA_PSK_EXT.1Extended: Pre-Shared Key Composition

```
Hierarchical to:    No other components.
Dependencies:   FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit
Generation).
```

FIA_PSK_EXT.1.1 The TSF shall be able to use pre-shared keys for IPsec.

FIA_PSK_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that are:

- 22 characters in length and [selection: [assignment: *other supported lengths*], no other lengths];
- composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).

FIA_PSK_EXT.1.3 The TSF shall condition the text-based pre-shared keys by using [selection: *SHA-1, SHA-256, SHA-512*, [assignment: *method of conditioning text string*]] and be able to [selection: *use no other pre-shared keys; accept bit-based pre-shared keys; generate bit-based pre-shared keys using the random bit generator specified in FCS_RBG_EXT.1*].

C.4.2.6. Rationale

Pre-shared Key Composition is to ensure the strong authentication between the endpoints of communications, and the Common Criteria does not provide a suitable SFR for the Pre-shared Key Composition.

This extended component protects the TOE by means of strong authentication, and it is therefore placed in the FIA class with a single component.

C.5. (FPT)

C.5.1. FPT_KYP_EXT□Extended: Protection of Key and Key Material

C.5.1.1. Family Behaviour

This family addresses the requirements for keys and key materials to be protected if and when written to nonvolatile storage.

C.5.1.2. Component Leveling

Component leveling

```
+----------------------------------------------+
|                                              |     +---+
| FPT_KYP_EXT Protection of key and key material +---->| 1 |
|                                              |     +---+
+----------------------------------------------+
```

FPT_KYP_EXT.1 Extended: Protection of key and key material, requires the TSF to ensure that no plaintext key or key materials are written to nonvolatile storage.

C.5.1.3. Management

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

- There are no management actions foreseen.

C.5.1.4. Audit

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

- There are no auditable events foreseen.

C.5.1.5. FPT_KYP_EXT.1Extended: Protection of Key and Key Material

```
Hierarchical to:    No other components.
Dependencies:       FCS_KYC_EXT.1 Extended: Key Chaining
```

FPT_KYP_EXT.1.1 The TSF shall not store plaintext keys that are part of the keychain specified by FCS_KYC_EXT.1 in any Field-Replaceable Nonvolatile Storage Device, and not store any such plaintext key on a device that uses the key for its encryption.

C.5.1.6. Rationale

Protection of Key and Key Material is to ensure that no plaintext key or key material are written to nonvolatile storage, and the Common Criteria does not provide a suitable SFR for the protection of key and key material.

This extended component protects the TSF data, and it is therefore placed in the FPT class with a single component.

C.5.2. FPT_SKP_EXT Extended: Protection of TSF Data

C.5.2.1. Family Behaviour

This family addresses the requirements for managing and protecting the TSF data, such as cryptographic keys. This is a new family modelled as the FPT Class.

C.5.2.2. Component Leveling

Component leveling

```
    +-----------------------------------------+
    |                                         |     +---+
    | FPT_SKP_EXT Protection of TSF Data      +---->| 1 |
    |                                         |     +---+
    +-----------------------------------------+
```

FPT_SKP_EXT.1 Protection of TSF Data (for reading all symmetric keys), requires preventing symmetric keys from being read by any user or subject. It is the only component of this family.

C.5.2.3. Management

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

- There are no management actions foreseen.

C.5.2.4. Audit

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

- There are no auditable events foreseen.

C.5.2.5. FPT_SKP_EXT.1Extended: Protection of TSF Data

```
Hierarchical to:    No other components.
Dependencies:   No dependencies.
```

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

C.5.2.6. Rationale

Protection of TSF Data is to ensure the pre-shared keys, symmetric keys and private keys are protected securely, and the Common Criteria does not provide a suitable SFR for the protection of such TSF data.

This extended component protects the TOE by means of strong authentication using Pre-shared Key, and it is therefore placed in the FPT class with a single component.

C.5.3. FPT_TST_EXTExtended: TSF testing

C.5.3.1. Family Behaviour

This family addresses the requirements for self-testing the TSF for selected correct operation.

C.5.3.2. Component Leveling

Component leveling

```
    +------------------------------------------+
    |                                          |     +---+
    | FPT_TST_EXT TSF testing                  +---->| 1 |
    |                                          |     +---+
    +------------------------------------------+
```

FPT_TST_EXT.1 TSF testing requires a suite of self-testing to be run during initial start-up in order to demonstrate correct operation of the TSF.

C.5.3.3. Management

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

- There are no management actions foreseen.

C.5.3.4. Audit

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

- There are no auditable events foreseen.

C.5.3.5. FPT_TST_EXT.1Extended: TSF testing

```
Hierarchical to:    No other components.
Dependencies:    No dependencies.
```

FPT_TST_EXT.1.1 The TSF shall run a suite of self-tests during initial start-up (and power on) to demonstrate the correct operation of the TSF.

C.5.3.6. Rationale

TSF testing is to ensure the TSF can be operated correctly, and the Common Criteria does not provide a suitable SFR for the TSF testing. In particular, there is no SFR defined for TSF testing.

This extended component protects the TOE, and it is therefore placed in the FPT class with a single component.

C.5.4. FPT_TUD_EXTExtended: Trusted Update

C.5.4.1. Family Behaviour

This family defines requirements for the TSF to ensure that only administrators can update the TOE firmware/software, and that such firmware/software is authentic.

C.5.4.2. Component Leveling

Component leveling

```
    +------------------------------------------+
    |                                          |     +---+
    | FPT_TUD_EXT Trusted Update               +---->| 1 |
    |                                          |     +---+
    +------------------------------------------+
```

FPT_TUD_EXT.1 Trusted Update, ensures authenticity and access control for updates.

C.5.4.3. Management

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

- There are no management actions foreseen.

C.5.4.4. Audit

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

- There are no auditable events foreseen.

C.5.4.5. FPT_TUD_EXT.1Trusted Update

```
Hierarchical to:    No other components.
Dependencies:   [FCS_COP.1(b) Cryptographic Operation (for signature
generation/verification),
    FCS_COP.1(c) Cryptographic operation (Hash Algorithm)].
```

FPT_TUD_EXT.1.1 The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [selection: published hash, no other functions] prior to installing those updates.

C.5.4.6. Rationale

Firmware/software is a form of TSF Data, and the Common Criteria does not provide a suitable SFR for the management of firmware/software. In particular, there is no SFR defined for importing TSF Data.

This extended component protects the TOE, and it is therefore placed in the FPT class with a single component.

> The entire FIA_MBE_EXT section here is a complete example of an Extended Component Definition. Note the ditaa diagram showing the component levelling. This is a required feature of the ECD and needs to be included for all components.
>
> If extended components are being defined, all sections within the example must be filled out for each requirement.

C.6. Identification and Authentication (FIA)

C.6.1. Mobile biometric enrolment (FIA_MBE_EXT)

C.6.1.1. Family Behaviour

This component defines the requirements for the TSF to be able to enrol a user, create templates of sufficient quality and prevent presentation attacks.

C.6.1.2. Component levelling

Component leveling

```
+-----------------------------------------+
|                                         |     +---+
| FIA_MBE_EXT  Mobile biometric enrollment +---->| 1 |
|                                         |     +---+
+-----------------------------------------+
```

FIA_MBE_EXT.1 Mobile biometric enrolment requires the TSF to enrol a user.

FIA_MBE_EXT.2 Quality of biometric templates for mobile biometric enrolment requires the TSF to create templates of sufficient quality.

FIA_MBE_EXT.3 Presentation attack detection for mobile biometric enrolment requires the TSF to prevent presentation attacks during the mobile biometric enrolment.

C.6.1.3. Management: FIA_MBE_EXT.1

There are no management activities foreseen.

C.6.1.4. Management: FIA_MBE_EXT.2

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

a) the management of the TSF data (setting threshold values for quality scores to generate templates) by an administrator.

C.6.1.5. Management: FIA_MBE_EXT.3

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

a) the management of the TSF data (setting values for detecting artificial presentation attack instruments) by an administrator.

C.6.1.6. Audit: FIA_MBE_EXT.1, FIA_MBE_EXT.2

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

a) Basic: Success or failure of the mobile biometric enrollment

C.6.1.7. Audit: FIA_MBE_EXT.3

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

a) Basic: Detection of presentation attacks

C.6.1.8. FIA_MBE_EXT.1 Mobile biometric enrolment

Hierarchical to: No other components

Dependencies: No dependencies

FIA_MBE_EXT.1.1 The TSF shall provide a mechanism to enrol an authenticated user.

Application Note 1

> User shall be authenticated by the mobile device using the Password Authentication Factor before beginning biometric enrolment.

C.6.1.9. FIA_MBE_EXT.2 Quality of biometric templates for mobile biometric enrolment

Hierarchical to: No other components Dependencies: FIA_MBE_EXT.1 Mobile biometric enrolment

FIA_MBE_EXT.2.1 The TSF shall create templates of sufficient quality.

Application Note 2

> ST author may refine “sufficient quality” to specify quality standards if the TOE follows such standard.

C.6.1.10. FIA_MBE_EXT.3 Presentation attack detection for mobile biometric enrolment

Hierarchical to: No other components Dependencies: FIA_MBE_EXT.1 Mobile biometric enrolment

FIA_MBE_EXT.3.1 The TSF shall prevent use of artificial presentation attack instruments from being successfully enrolled.

Appendix D: Entropy Documentation and Assessment

> This section may not always be applicable when talking about PP-Modules (which may rely on entropy from a base PP). This particular section is copied from the NDcPP. If you need an entropy review, it would be simplest to probably leave this intact.

This appendix describes the required supplementary information for each entropy source used by the TOE.

The documentation of the entropy source(s) should be detailed enough that, after reading, the evaluator will thoroughly understand the entropy source and why it can be relied upon to provide sufficient entropy. This documentation should include multiple detailed sections: design description, entropy justification, operating conditions, and health testing. This documentation is not required to be part of the TSS.

D.1. Design Description

Documentation shall include the design of each entropy source as a whole, including the interaction of all entropy source components. Any information that can be shared regarding the design should also be included for any third-party entropy sources that are included in the product.

The documentation will describe the operation of the entropy source to include how entropy is produced, and how unprocessed (raw) data can be obtained from within the entropy source for testing purposes. The documentation should walk through the entropy source design indicating where the entropy comes from, where the entropy output is passed next, any post-processing of the raw outputs (hash, XOR, etc.), if/where it is stored, and finally, how it is output from the entropy source. Any conditions placed on the process (e.g., blocking) should also be described in the entropy source design. Diagrams and examples are encouraged.

This design must also include a description of the content of the security boundary of the entropy source and a description of how the security boundary ensures that an adversary outside the boundary cannot affect the entropy rate.

If implemented, the design description shall include a description of how third-party applications can add entropy to the RBG. A description of any RBG state saving between power-off and power-on shall be included.

D.2. Entropy Justification

There should be a technical argument for where the unpredictability in the source comes from and why there is confidence in the entropy source delivering sufficient entropy for the uses made of the RBG output (by this particular TOE). This argument will include a description of the expected min-entropy rate (i.e. the minimum entropy (in bits) per bit or byte of source data) and explain that sufficient entropy is going into the TOE randomizer seeding process. This discussion will be part of a justification for why the entropy source can be relied upon to produce bits with entropy.

The amount of information necessary to justify the expected min-entropy rate depends on the type of entropy source included in the product.

For developer-provided entropy sources, in order to justify the min-entropy rate, it is expected that a large number of raw source bits will be collected, statistical tests will be performed, and the min-entropy rate determined from the statistical tests. While no particular statistical tests are required at this time, it is expected that some testing is necessary in order to determine the amount of min-entropy in each output.

For third-party provided entropy sources, in which the TOE vendor has limited access to the design and raw entropy data of the source, the documentation will indicate an estimate of the amount of min-entropy obtained from this third-party source. It is acceptable for the vendor to “assume” an amount of min-entropy, however, this assumption must be clearly stated in the documentation provided. In particular, the min-entropy estimate must be specified and the assumption included in the ST.

Regardless of the type of entropy source, the justification will also include how the DRBG is initialized with the entropy stated in the ST, for example by verifying that the min-entropy rate is multiplied by the amount of source data used to seed the DRBG or that the rate of entropy expected based on the amount of source data is explicitly stated and compared to the statistical rate. If the amount of source data used to seed the DRBG is not clear or the calculated rate is not explicitly related to the seed, the documentation will not be considered complete.

The entropy justification shall not include any data added from any third-party application or from any state saving between restarts.

D.3. Operating Conditions

The entropy rate may be affected by conditions outside the control of the entropy source itself. For example, voltage, frequency, temperature, and elapsed time after power-on are just a few of the factors that may affect the operation of the entropy source. As such, documentation will also include the range of operating conditions under which the entropy source is expected to generate random data. Similarly, documentation shall describe the conditions under which the entropy source is no longer guaranteed to provide sufficient entropy. Methods used to detect failure or degradation of the source shall be included.

D.4. Health Testing

More specifically, all entropy source health tests and their rationale will be documented. This will include a description of the health tests, the rate and conditions under which each health test is performed (e.g., at start up, continuously, or on-demand), the expected results for each health test, TOE behaviour upon entropy source failure, and rationale indicating why each test is believed to be appropriate for detecting one or more failures in the entropy source.

Appendix E: Key Management Document

> This section can be included to cover information that should not be publically released but which needs to be included in the documentation that is evaluated. In some cases this has been handled by public and proprietary versions of the ST (specifically the TSS), but this information can also be covered in a separate document.
>
> This is not always necessary and depends on the product type. The name of the document can be edited to be appropriate for the iTC, but the purpose is to cover information that would normally be marked as proprietary by a vendor.
>
> The following section has been copied from the current File Encryption PP-Module by NIAP.

The documentation of the product's encryption key management should be detailed enough that, after reading, the evaluator will thoroughly understand the product's key management and how it meets the requirements to ensure the keys are adequately protected. This documentation should include an essay and diagram(s). This documentation is not required to be part of the TSS - it can be submitted as a separate document and marked as developer proprietary.

E.1. Key Management Description

The description will provide the following information for all keys in the key chain:

- The purpose of the key
- If the key is stored in non-volatile memory
- How and when the key is protected
- How and when the key is derived
- The strength of the key
- When or if the key would be no longer needed, along with a justification
- How and when the key may be shared

The description will also describe the following topics:

- A description of all authorization factors that are supported by the product and how each factor is handled, including any conditioning and combining performed.
- If validation is implemented, the process for validation shall be described, noting what value is used for validation and the process used to perform the validation. It shall describe how this process ensures no keys in the key chain are weakened or exposed by this process.
- The authorization process that leads to the decryption of the FEK(s). This section shall detail the

key chain used by the product. It shall describe which keys are used in the protection of the FEK(s) and how they meet the encryption or derivation requirements including the direct chain from the initial authorization to the FEK(s). It shall also include any values that add into that key chain or interact with the key chain and the protections that ensure those values do not weaken or expose the overall strength of the key chain.

- The diagram and essay will clearly illustrate the key hierarchy to ensure that at no point the chain could be broken without a cryptographic exhaust or all of the initial authorization values and the effective strength of the FEK(s) is maintained throughout the key chain.
- A description of the data encryption engine, its components, and details about its implementation (e.g. initialization of the product, drivers, libraries (if applicable), logical interfaces for encryption/decryption, and how resources to be encrypted are identified. The description should also include the data flow from the device's host interface to the device's persistent media storing the data, information on those conditions in which the data bypasses the data encryption engine. The description should be detailed enough to verify all platforms ensure that when the user enables encryption, the product encrypts all selected resources.
- The process for destroying keys when they are no longer needed by describing the storage location of all keys and the protection of all keys stored in non-volatile memory.

E.2. Key Management Diagram:

- The diagram will include all keys from the initial authorization factor(s) to the FEK(s) and any keys or values that contribute into the chain. It must list the cryptographic strength of each key and indicate how each key along the chain is protected with either options from key chaining requirement. The diagram should indicate the input used to derive or decrypt each key in the chain.
- A functional (block) diagram showing the main components (such as memories and processors) the initial steps needed for the activities the TOE performs to ensure it encrypts the targeted resources when a user or administrator first provisions the product.

Appendix F: Consistency Rationale

These tables need to be completed to show mapping and justification that the threats and assumptions map to the requirements.

Table 4. Consistency Rationale for threats and OSPs

Threats/OSPs	Consistency Rationale

Table 5. Consistency Rationale for Assumptions

Assumptions	Consistency Rationale

F.1. Consistency of Objectives

The objectives for the biometric system and its operational environment are consistent with the [MDFPP] based on the following rationale:

Table 6. Consistency Rationale for TOE Objectives

TOE Objectives	Consistency Rationale

Table 7. Consistency Rationale for Environmental Objectives

Environmental Objectives	Consistency Rationale

F.2. Consistency of Requirements

Appendix G: SFR List

> This section is to provide a full list of all SFRs and their inclusion status (mandatory, optional or selection-based) within the cPP.

This table is provided as a reference of all SFRs included in this cPP.

The Type column has the following definitions:

Mandatory [R]

The requirement is mandatory for inclusion in the ST.

Conditionally Mandatory [C]

The requirement is conditionally mandatory for inclusion in the ST.

Optional [O]

The requirement is optional for inclusion in the ST.

Selection [S]

The requirement inclusion is determined by selections in other requirements in the ST.

[U]

The SFR plays a supporting role to other SFRs.

Table 8. Security Functional Requirements

Objective/SFR	O.ACCESS_CONTROL	O.ADMIN_ROLES	O.AUDIT	O.COMMS_PROTECTION	O.FAX_NET_SEPARATION	O.IMAGE_OVERWRITE	O.KEY_MATERIAL	O.PURGE_DATA	O.STORAGE_ENCRYPTION	O.TSF_SELF_TEST	O.UPDATE_VERIFICATION	O.USER_AUTHORIZATION	O.USER_I&A

FAU_GEN.1			R										
FAU_GEN.2			R										
FAU_SAR.1			O										
FAU_SAR.2			O										
FAU_STG.1			O										
FAU_STG.4			O										
FAU_STG_EXT.1			R										
FCS_CKM.1(a)				R									
FCS_CKM.1(b)				R					S				
FCS_CKM.4				U				O	U				
FCS_CKM_EXT.4				U				O	U				
FCS_COP.1(a)				R									
FCS_COP.1(b)				S							S		
FCS_COP.1(c)									U		S		
FCS_COP.1(d)									U				
FCS_COP.1(e)									U				

FCS_COP.1(f)									U				
FCS_COP.1(g)				S									
FCS_COP.1(h)									O				
FCS_COP.1(i)									U				
FCS_HTTPS_EXT.1				S									
FCS_IPSEC_EXT.1				S									
FCS_KDF_EXT.1									O				
FCS_KYC_EXT.1									C				
FCS_PCC_EXT.1									O				
FCS_RBG_EXT.1				U					U				
FCS_SMC_EXT.1									S				
FCS_SNI_EXT.1									S				
FCS_SSH_EXT.1				S									

FCS_TLS_EXT.1				S									
FDP_ACC.1	R										R		
FDP_ACF.1	R										R		
FDP_DSK_EXT.1								C					
FDP_FXS_EXT.1					C								
FDP_RIP.1(a)						O							
FDP_RIP.1(b)								O					
FIA_AFL.1												U	
FIA_ATD.1											U		
FIA_PMG_EXT.1												R	
FIA_PSK_EXT.1				S									
FIA_UAU.1												R	
FIA_UAU.7												R	
FIA_UID.1												R	
FIA_USB.1												R	
FMT_MOF.1		R											

FMT_MSA.1	U										R		
FMT_MSA.3	U										R		
FMT_MTD.1	U												
FMT_SMF.1	U	R									R		
FMT_SMR.1	U	R									R		
FPT_KYP_EXT.1							C						
FPT_SKP_EXT.1				R									
FPT_STM.1			U										
FPT_TST_EXT.1									R				
FPT_TUD_EXT.1										R			
FTA_SSL.3												R	
FTP_ITC.1			U	R									
FTP_TRP.1(a)				R									
FTP_TRP.1(b)				R									

Appendix H: Glossary

This should be completed to define all the terms needed to fully understand the content of the cPP.

For the purpose of this cPP, the following terms and definitions given in *some specific references* apply. If the same terms and definitions are given in those references, terms and definitions that fit the context of this cPP take precedence.

Data Encryption Key (DEK)

A key used to encrypt data at rest.

Appendix I: Acronyms

Table 9. Acronyms

Acronym	Meaning
AES	Advanced Encryption Standard
ITSEF	IT Security Evaluation Facility