# Lexmark MS622 Single Function Printer Security Target

Version 1.5

February 27, 2019

Lexmark International, Inc.
740 New Circle Road
Lexington, KY 40550

## DOCUMENT INTRODUCTION

Prepared By:

Common Criteria Consulting LLC
15804 Laughlin Lane
Silver Spring, MD 20906
http://www.consulting-cc.com

Prepared For:

Lexmark International, Inc.
740 New Circle Road
Lexington, KY 40550
http://www.lexmark.com

## REVISION HISTORY

| Rev | Description |
|---|---|
| 1.0 | July 16, 2018, Initial release |
| 1.1 | September 13, 2018, Addressed lab ORs |
| 1.2 | September 17, 2018, Added printer detail to Table 5 |
| 1.3 | November 9, 2018, Updated CAVP cert numbers |
| 1.4 | January 23, 2019, Corrected SE part number |
| 1.5 | February 27, 2019, Updated TD List |

## TABLE OF CONTENTS

## LIST OF TABLES



## ACRONYMS LIST

**AD ..... Active Directory**
**AES ..... Advanced Encryption Standard**

**BSD** ..... **Berkeley Software Distribution**
**CAC** ..... **Common Access Card**
**CAVP** ..... **Cryptographic Algorithm Validation Program**
**CBC** ..... **Cipher Block Chaining**
**CC** ..... **Common Criteria**
**CM** ..... **Configuration Management**
**DRBG** ..... **Deterministic Random Bit Generator**
**EAL** ..... **Evaluation Assurance Level**
**ESP** ..... **Encapsulating Security Payload**
**FAC** ..... **Function Access Control**
**GSSAPI** ..... **Generic Security Services Application Program Interface**
**GUI** ..... **Graphical User Interface**
**HTTP** ..... **HyperText Transfer Protocol**
**I&A** ..... **Identification & Authentication**
**IP** ..... **Internet Protocol**
**IPP** ..... **Internet Printing Protocol**
**IPsec** ..... **Internet Protocol Security**
**ISO** ..... **International Standards Orgaization**
**IT** ..... **Information Technology**
**KAT** ..... **Known Answer Test**
**KDC** ..... **Key Distribution Center**
**LAN** ..... **Local Area Network**
**LDAP** ..... **Lightweight Directory Access Protocol**
**MB** ..... **MegaByte**
**SFP** ..... **Multi-Function Printer**
**NIAP** ..... **National Information Assurance Partnership**
**NTP** ..... **Network Time Protocol**
**OSP** ..... **Organizational Security Policy**
**PIV** ..... **Personal Identity Verification**
**PJL** ..... **Printer Job Language**
**PP** ..... **Protection Profile**
**PSK** ..... **Pre-Shared Key**
**PSTN** ..... **Public Switched Telephone Network**
**RBG** ..... **Random Bit Generator**
**RFC** ..... **Request For Comments**
**SFP** ..... **Security Function Policy**
**SFP** ..... **Single Function Printer**
**SFR** ..... **Security Functional Requirement**
**SHA** ..... **Secure Hash Algorithm**
**ST** ..... **Security Target**
**TD** ..... **Technical Decision**
**TOE** ..... **Target of Evaluation**
**TRNG** ..... **True Random Number Generator**
**TSF** ..... **TOE Security Function**
**URL** ..... **Uniform Resource Locator**
**USB** ..... **Universal Serial Bus**

# 1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the Lexmark MS622 with firmware version MSTGM.050.023 with Lexmark Secure Element (P/N 57X0185) TOE. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5*. As such, the spelling of terms is presented using the internationally accepted English.

## 1.1 Security Target Reference

Lexmark MS622 Single Function Printer Security Target, version 1.5, February 27, 2019.

## 1.2 TOE Reference

Lexmark MS622 with firmware version MSTGM.052.025 with Lexmark Secure Element (P/N 57X0185).

## 1.3 Keywords

Hardcopy, Paper, Document, Printer, Residual data, Temporary data, Network interface, Single Function Device, SFP

## 1.4 TOE Overview

### 1.4.1 Usage and Major Security Features

The SFPs are single function printer systems with networked capabilities. Their capabilities extend to servicing print jobs through the network. The SFPs feature an integrated touch-sensitive operator panel.

The Lexmark Secure Element (Part Number 57X0185) is an optional component that must be installed in the SFP in the evaluated configuration. The Secure Element incorporates an Infineon Smart Card IC M9900 (Release A22, Infineon Part Number SLE97CSFX1M00PE). The M9900 provides a True Random Number Generator (TRNG) used by the TOE to supply entropy to the DRBG functionality provided on the mother board. The Secure Element also incorporates Lexmark application firmware enabling communication between the SFP firmware on the mother board and the M9900.

The major security features of the TOE are:

1. All Users are identified and authenticated as well as authorized before being granted permission to perform any restricted TOE functions.
2. Administrators authorize Users to use the functions of the TOE.
3. User Document Data are protected from unauthorized disclosure or alteration.
4. TSF Data, of which unauthorized disclosure threatens operational security, are protected from unauthorized disclosure.
5. TSF Data, of which unauthorized alteration threatens operational security, are protected from unauthorized alteration.
6. Document processing and security-relevant system events are recorded, and such records are protected from disclosure to anyone except for authorized personnel. Records may not be altered.

#### 1.4.1.1 User Definitions

There are two categories of Users defined in this Security Target:

**Table 1 - User Categories**

| Designation | Category name | Definition |
|---|---|---|
| U.NORMAL | Normal User | A User who has been identified and authenticated and does not have an administrative role |
| U.ADMIN | Administrator | A User who has been identified and authenticated and has an administrative role |

#### 1.4.1.2 Asset Definitions

Assets are passive entities in the TOE that contain or receive information. Assets are Objects (as defined by the CC). There are two categories of Assets:

**Table 2 - Asset categories**

| Designation | Asset category | Definition |
|---|---|---|
| D.USER | User Data | Data created by and for Users that do not affect the operation of the TSF |
| D.TSF | TSF Data | Data created by and for the TOE that might affect the operation of the TSF |

#### 1.4.1.3 User Data

User Data are composed of two types:

**Table 3 - User Data types**

| Designation | User Data type | Definition |
|---|---|---|
| D.USER.DOC | User Document Data | Information contained in a User's Document, in electronic or hardcopy form |

| Designation | User Data type | Definition |
|---|---|---|
| D.USER.JOB | User Job Data | Information related to a User's Document or Document Processing Job |

#### 1.4.1.4 TSF Data

TSF Data are composed of two types:

**Table 4 - TSF Data types**

| Designation | TSF Data type | Definition |
|---|---|---|
| D.TSF.PROT | Protected TSF Data | TSF Data for which alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE, but for which disclosure is acceptable |
| D.TSF.CONF | Confidential TSF Data | TSF Data for which either disclosure or alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE |

### 1.4.2 TOE type

Single Function Device (Printer)

### 1.4.3 Required Non-TOE Hardware/Software/Firmware

To be fully operational, the following items may be connected to the SFP:

1. A LAN for network connectivity. The TOE supports IPv4 and IPv6.
2. IT systems that submit print jobs to the SFP via the network using standard print protocols.
3. An IT system acting as the remote syslog recipient of audit event records sent from the TOE.
4. LDAP server to support Identification and Authentication (I&A). This component is optional depending on the type(s) of I&A mechanisms used.

5. Card reader and cards to support Personal Identity Verification (PIV) cards. This component is optional depending on the type(s) of I&A mechanisms used. The supported card reader is the Identiv uTrust 2700 F Contact Smart Card Reader.

## 1.5 TOE Description

The TOE provides the following functions related to SFPs:

1. Printing
2. Network Communication
3. Administration
4. Internal Audit Log Storage
5. Purge Data

All of the SFP models referenced in the evaluation are complete SFPs in a single unit.

All of the SFP models included in this evaluation provide the same security functionality. There are no security-relevant differences between the models included in the evaluation. Their differences are limited to minor differences in processors, color or black & white printing, and the speed of printing. The differences in the processors accommodate differences in the speed of printing and support for color operations. The following tables summarize the technical characteristics of the SFP models.

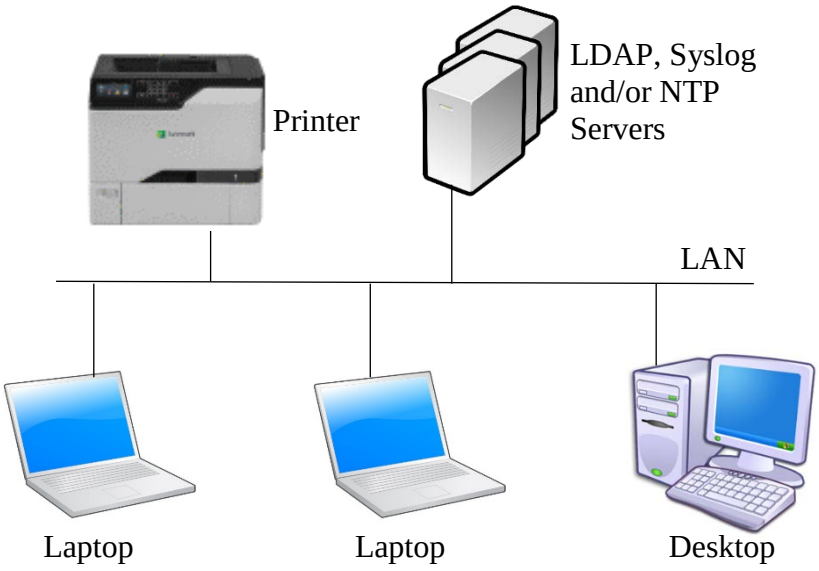
**Table 5 - Technical Characteristics of the SFP Models**

| Model | Processor | Word Size | Color/Mono | Pages Per Minute |
|---|---|---|---|---|
| MS622 | Marvell 88PA6220 (Gem) | 32-bit | Mono | 50 |

### 1.5.1 Physical Boundary

The physical boundary of the TOE is the SFP, including the Lexmark Secure Element.

**Figure 1 - Representative TOE Deployment**




The physical scope of the TOE also includes the following guidance documentation:

1. *Lexmark Common Criteria Installation Supplement and Administrator Guide*
2. *Lexmark Embedded Web Server Administrator's Guide*
3. *Lexmark M3250, MS622 User's Guide*

### 1.5.2 Logical Boundary

The TOE supports the security functions documented in the following sections.

#### 1.5.2.1 Identification, Authentication and Authorization

When a touch panel or web session is initiated, the user is implicitly assumed to be the Guest (default) user. Per the evaluated configuration, the permissions for this user must be configured such that no access to TSF data or functions is allowed other than print job submission (job submission is authorized regardless of what user is logged in). Therefore, the user must successfully log in as a different user before any TSF data or functions other than print job submission may be accessed.

The TOE supports I&A with a per-user selection of Username/Password Accounts (processed by the TOE) or integration with an external LDAP server (in the operational environment) using GSSAPI/Kerberos. Smart Card authentication may also be specified for users of the touch panel.

#### 1.5.2.2 Access Control

Access controls configured for functions and menu access are enforced by the TOE.

#### 1.5.2.3 Data Encryption

The TOE protects the confidentiality and integrity of all information exchanged over the attached network by using IPSec with ESP for all network communication.

#### 1.5.2.4 Trusted Communications

The TOE ensures communication is performed with known endpoints by using IPSec with pre-shared keys or by validating supplied certificates.

#### 1.5.2.5 Administrative Roles

Through web browser and touch panel sessions, authorized administrators may configure access controls and perform other TOE management functions.

#### 1.5.2.6 Auditing

The TOE generates audit event records for security-relevant events. Audit records are stored internally and securely transmitted to a remote IT system using the syslog protocol over IPsec.

#### 1.5.2.7 Trusted Operation

Software updates are verified to ensure the authenticity of the software before being applied. During initial start-up, the TOE performs self tests on its cryptographic components and the integrity of the executable code.

### 1.6 TOE Data

### 1.6.1 TSF Data

**Table 6 - TSF Data**

| Item | Description |
|---|---|
| Account Status | Login status information is associated with all accounts used to authenticate internally against a Username/Password. For each Username/Password account, the TOE tracks the number of login failures, time of the earliest login failure, and lock status. |
| Active Directory Configuration | Configuration information used to join an Active Directory Domain. Once joined, machine credentials are generated and the LDAP+GSSAPI Login Method parameters for communication with the Domain Controller are automatically populated. |
| Date and Time Parameters | Controls whether the time is tracked internally or from a remote NTP server. If an NTP server is used, it specifies the parameters for communication with the server. |
| Enable Audit | Determines if the device records events in the secure audit log and (if enabled) in the remote syslog. |
| Enable HTTP Server | Enables HTTP(S) server on the TOE. |
| Enable Remote Syslog | Determines if the device transmits logged events to a remote server. |
| Groups | The set of Groups may be used to configure permissions for users. Each Group has a configured set of permissions. Users may belong to any number of Groups, and any User's permissions are the union of the permissions for each Group it is a member of. |
| Held Print Job Expiration Timer | Specifies the amount of time a received print job is saved for a user to release before it is automatically deleted. |
| IPSec Settings | The configuration parameters for IPSec that require IPSec with ESP for all network communication (IPv4 and/or IPv6) with certificate validation or pre-shared keys. |
| Job Waiting | Specifies whether a print job may be placed in the Held Jobs queue if the required resources (e.g. paper type) are not currently available, enabling subsequent print jobs to be processed immediately |

| Item | Description |
|---|---|
| Kerberos Setup | Defines the KDC Address, KDC Port, and Realm for communication with the KDC. KDC communication is required if the TOE is using the LDAP+GSSAPI login mechanism. |
| LDAP Certificate Required | Specifies whether a valid certificate is required to be sent by an LDAP server. Yes specifies that the server certificate is requested; if no certificate is provided or if a bad certificate is provided, the session is terminated immediately. No indicates that a certificate is not required; if a certificate is supplied and it is invalid, the session is terminated immediately. |
| LDAP+GSSAPI – SFP Credentials | Specifies the Username and password to be used when performing LDAP queries. |
| LDAP+GSSAPI Configuration | Specifies the configuration options for communicating and exchanging information with an LDAP server using GSSAPI. |
| LES Applications | Specifies whether enhanced service Java applications may be executed on the TOE. This parameter must be set to "Enable" during installation and is not accessible to administrators during operation. |
| Login Restrictions | Determines how many failed authentications are allowed within the "Failure time frame" value before the offending Username/Password account is prevented from logging in for the duration of the "Lockout time" value. The "Web Login Timeout" determines how long the web sessions can remain idle before the user is logged off automatically. |
| Network Port | Defines the parameters required for the TOE to communicate via the standard network port |
| Permissions | Permissions specify the Function Access Control (FAC) authorizations, which grant access to menus or functions. Permissions are separately configurable for the default Guest account (Public) and for each defined Group. Users other than Guest inherent the union of permissions for all Groups that they are a member of. |
| Remote Syslog Parameters | Defines the communication to the remote syslog system |
| Security Reset Jumper | Specifies the behavior of the TOE when a position change of the Security Reset Jumper is detected. No Effect indicates the jumper should be ignored. "Enable Guest Access" changes the permissions for the Guest account to provide access to all functions and menus. |
| Smart Card Authentication Client Configuration | Specifies parameters for validating the certificate from the card and retrieving information from Active Directory. |
| USB Buffer | Disables all activity via the USB device ports (with the exception of a Smart Card reader if Smart Card usage is configured). |
| Username/Password Accounts | Specify a list of accounts that are internally validated by username and password. For each account, a list of Group memberships are configured. |
| Visible Home Screen Icons | Specifies what icons should be displayed on the touch panel home screen. |

## 1.7 Evaluated Configuration

The following configuration options apply to the evaluated configuration of the TOE:

1. The B/W Print and Color Print permissions must be configured for the Public permissions, which apply to all users including the Guest user. These permissions authorize the SFP to accept print jobs from remote IT systems. No other permissions may be configured for the Public permissions.

2. No optional network interfaces are installed on the SFPs. Note that one physical LAN interface is standard on all SFPs.
3. No optional parallel or serial interfaces are installed on the SFPs. These are for legacy connections to specific IT systems only.
4. All USB ports on the SFPs that perform document processing functions (print) are disabled via configuration. In the operational environments in which the Common Criteria evaluated configuration is of interest, the users typically require that all USB ports are disabled. If Smart Card authentication is used, the card reader is physically connected to a specific USB port during TOE installation; in the evaluated configuration this USB port is limited in functionality to acting as the interface to the card reader. A reader is shipped with the SFP. If Smart Card authentication is not used, the card reader may be left unconnected.
5. Operational management functions are performed via browser sessions to the embedded web server or via the management menus available through the touch panel.
6. Access controls are configured for all TSF data so that only authorized administrators are permitted to manage those parameters.
7. All network communication is required to use IPSec with ESP to protect the confidentiality and integrity of the information exchanged, including management sessions that exchange D.TSF.CONF and D.TSF.PROT. Certificates presented by remote IT systems are validated.
8. Because all network traffic is required to use IPSec with ESP, syslog records sent to a remote IT system also are protected by IPSec with ESP.
9. I&A may use Username/Password Accounts and/or the LDAP+GSSAPI login method on a per-user basis. Smart Card authentication may be used for touch panel users. No other I&A mechanisms are included in the evaluation because they provide significantly lower strength than the supported mechanisms.
10. LDAP+GSSAPI and Smart Card authentication require integration with an external LDAP server such as Active Directory. This communication uses default certificates; the LDAP server must provide a valid certificate to the TOE. Binds to LDAP servers for LDAP+GSSAPI use device credentials (not anonymous bind) so that the information retrieved from Active Directory can be restricted to a specific SFP. Binds to LDAP servers for Smart Card authentication use user credentials from the card (not anonymous bind) so that the information retrieved from Active Directory can be restricted to a specific user.
11. Audit event records are transmitted to a remote IT system as they are generated using the syslog protocol.
12. The severity level of audit events to log must be set to 5 (Notice).
13. No Java applications other than those stated in this section are loaded into the SFP by Administrators. These applications are referred to as eSF applications in end user documentation. The following eSF applications are installed by an administrator during TOE installation and must be enabled: “Smart Card Authentication”.

14. The following eSF applications are installed by an administrator during TOE installation and must be enabled if PIV smart card authentication is used: “Smart Card Authentication Client”, “PIV Smart Card Driver”, and “Background and Idle Screen”.
15. All other eSF applications installed by Lexmark before the TOE is shipped must be disabled.
16. No option card for downloadable emulators is installed in the TOE.
17. NPAP, PJL and Postscript have the ability to modify system settings. The capabilities specific to modifying system settings via these protocols are disabled.
18. All administrators must be authorized for print fucntions.
19. All network print jobs are held until released via the touch panel. Every network print job must include a PJL SET USERNAME statement to identify the userid of the owner of the print job. Held print jobs may only be released by an authenticated user with the same userid as specified in the print job.
20. Administrators are directed (through operational guidance) to specify passwords adhering to the following composition rules for Username/Password Accounts:
    - A minimum of 8 characters (note that the minimum size is configurable and can be set to a minimum of 15 characters)
    - At least one lower case letter, one upper case letter, and one non-alphabetic character
    - No dictionary words or permutations of the user name
21. Simple Network Management Protocol (SNMP) support is disabled.
22. Internet Printing Protocol (IPP) support is disabled.
23. All unnecessary network ports are disabled.
24. The supported Diffie-Hellman groups for IKE are Group 14 (2048-bit MODP) and Group 24 (2048-bit MODP with 256-bit POS).

The print function may be disabled or restricted, indicating that the functionality is included in the evaluation and may be disabled or restricted to an authorized set of users at the discretion of an administrator

### 1.8 Functionality Supported But Not Evaluated

The following functionality is supported in the product but is not included in the evaluation.

1. In addition to Personal Identity Verification (PIV) cards, Common Access Card (CAC) and Secret Internet Protocol Router Network (SIPRNet) cards are also supported.
2. In addition to the Identiv uTrust 2700 F Contact Smart Card Reader, the following card readers are also supported:
    a. Identiv uTrust 2700 R Contact Smart Card Reader,
    b. Omnikey 3121 SmartCard Reader,

c. Any other Omnikey SmartCard Readers that share the same USB Vendor IDs and Product IDs with the Omnikey 3121 (example Omnikey 3021),

d. SCM SCR 331,

e. SCM SCR 3310v2.

# 2. Conformance Claims

## 2.1 Common Criteria Conformance

Common Criteria version: Version 3.1 Revision 5

Common Criteria conformance: Part 2 extended and Part 3 conformant

## 2.2 Protection Profile Conformance

This Security Target claims exact conformance to the Protection Profile for Hardcopy Devices [HCD], version 1.0, dated September 10, 2015 as modified by Errata #1 dated June 2017.

The following table states whether each of the NIAP Technical Decisions (TDs) issued to date that are applicable to [HCD] are applicable to this TOE.

**Table 7 - Technical Decision Applicability**

| TD | Applicable | Exclusion Rationale |
|---|---|---|
| TD0074 - FCS_CKM.1(a) Requirement in HCD PP v1.0 | Yes | |
| TD0157 - FCS_IPSEC_EXT.1.1 - Testing SPDs | Yes | |
| TD0176: FDP_DSK_EXT.1.2 - SED Testing | No | The TD is associated with FDP_DSK_EXT.1. The TOE does not include FDP_DSK_EXT.1 functionality. |
| TD0219 - NIAP Endorsement of Errata for HCD PP v1.0 | Yes | |
| TD0253: Assurance Activities for Key Transport | No | The TD is associated with FCS_COP.1(i). The TOE does not include FCS_COP.1(i) functionality. |
| TD0261 - Destruction of CSPs in flash | Yes | |
| TD0299: Update to FCS_CKM.4 Assurance Activities | Yes | |
| TD0393 - Require FTP_TRP.1(b) only for printing | Yes | |

# 3. Security Problem Definition

The following Security Problem Definition is reproduced from [HCD], with minor changes made to account for the TOE being a single function device.

> The Security Problem Definition (SPD) is divided into two parts. This first part describes Assets, Threats, and Organizational Security Policies, in narrative form. [Brackets] indicate a reference to the second part, formal definitions of Users, Assets, Threats, Organizational Security Policies, and Assumptions, which appear in Appendix A of [HCD].
>
> Note: From this point in the document, the Target of Evaluation will be referred to by the acronym "TOE" (Target of Evaluation) instead of by the product category "HCD" (Hardcopy Device).

## 3.1 Users

A conforming TOE must define at least the following two User roles:

1. Normal Users [U.NORMAL] who are identified and authenticated and do not have an administrative role.
2. Administrators [U.ADMIN] who are identified and authenticated and have an administrative role.

A conforming TOE may allow additional roles, sub-roles, or groups. In particular, a conforming TOE may allow several administrative roles that have authority to administer different aspects of the TOE.

Note that a User can be a human user or an external IT entity.

Additional details about Users are in Appendix A.1 of [HCD].

## 3.2 Assets

From a User's perspective, the primary Asset to be protected in a TOE is User Document Data [D.USER.DOC]. A User's job instructions, User Job Data [D.USER.JOB] (information related to a User's Document or Document Processing Job), may also be protected if their compromise impacts the protection of User Document Data. Together, User Document Data and User Job Data are considered to be User Data.

As an illustrative example, data sent by a Network User for printing contains a User's Document [D.USER.DOC] which must not be accessed by anyone else, and job instructions [D.USER.JOB] which must not be altered by anyone else.

From an Administrator's perspective, the primary Asset to be protected in a TOE is data that is used to configure and monitor the secure operation of the TOE. This kind of data is considered to be TOE Security Functionality (TSF) Data.

There are two broad categories for this kind of data:

1. Protected TSF Data, which may be read by any User but must be protected from unauthorized modification and deletion [D.TSF.PROT]; and,
2. Confidential TSF Data, which may neither be read nor modified or deleted except by authorized Users [D.TSF.CONF].

An illustrative example is data that is used by the TOE to identify and authenticate authorized Users. Typically, a username that is used for identification may be read by anyone but must be protected from unauthorized modification and deletion [D.TSF.PROT]. In contrast, a User's password that is used for authentication must be confidential, prohibiting any Unauthorized Access [D.TSF.CONF].

If TSF Data is compromised, it can be used for a variety of malicious purposes that include elevation of privileges, accessing stored Documents, redirecting the destination of processed Documents, masquerading as an authorized User or Administrator, altering the operating software of the TOE, and attacking External IT Entities.

In a conforming TOE, TSF Data is clearly identified and categorized as either Protected TSF Data or Confidential TSF Data.

From a network security perspective, it is important to ensure the secure operation of the TOE and other IT entities in its Operational Environment. Since the Operational Environment is outside of the TOE, Organizational Security Policies are employed to address protection of the Operational Environment.

Additional details about assets are in Appendix A.2 of [HCD].

## 3.3 Threats

The following are Threats against the TOE that are countered by conforming products.

Additional details about threats are in Appendix A.3 of [HCD].

### 3.3.1 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.

### 3.3.2 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.

### 3.3.3 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 record the transmission of system Credentials, or to send malicious data to the TOE.

### 3.3.4 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.

## 3.4 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 of [HCD].

### 3.4.1 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.

### 3.4.2 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.

### 3.4.3 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.

### 3.4.4 Purge Data

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.

## 3.5 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 of [HCD].

### 3.5.1 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.

### 3.5.2 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.

### 3.5.3 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.

### 3.5.4 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.

# 4. Security Objectives

The following Security Objectives are reproduced from [HCD]. Note that paragraph numbering shown in this chapter corresponds to paragraph numbers in [HCD].

## 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 of [HCD].

### 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.

### 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:

- User Document Data [D.USER.DOC] can be accessed only by the

Document owner or an Administrator.

- User Job Data [D.USER.JOB] can be read by any User but can be modified only by the Job Owner or an Administrator.
- 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.
- 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:

- Sensitive data or Credentials are obtained by monitoring LAN data outside of the TOE.
- A successfully authenticated session is captured and replayed on the LAN, permitting the attacker to masquerade as the authenticated User.
- 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 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 of [HCD].

### 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 rationale is reproduced from [HCD].

**Table 8 - Security Objectives rationale**

| Threat/Policy/Assumption | Rationale |
|---|---|
| T.UNAUTHORIZED_ACCESS<br><br>*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.* | O.ACCESS_CONTROL restricts access to User Data in the TOE to authorized Users.<br><br>O.USER_I&A provides the basis for access control.<br><br>O.ADMIN_ROLES restricts the ability to authorize Users and set access controls to authorized Administrators. |
| T.TSF_COMPROMISE<br><br>*An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.* | O.ACCESS_ CONTROL restricts access to TSF Data in the TOE to authorized Users.<br><br>O.USER_I&A provides the basis for access control.<br><br>O.ADMIN_ROLES restricts the ability to authorize Users and set access controls to authorized Administrators. |
| T.TSF_FAILURE<br><br>*A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.* | O.TSF_SELF_TEST prevents the TOE from operating if a malfunction is detected. |
| T.UNAUTHORIZED_UPDATE<br><br>*An attacker may cause the installation of unauthorized software on the TOE.* | O.UPDATE_VERIFICATION verifies the authenticity of software updates. |

| Threat/Policy/Assumption | Rationale |
|---|---|
| T.NET_COMPROMISE<br><br>*An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.* | O.COMMS_PROTECTION protects LAN communications from sniffing, replay, and man-in- the-middle attacks. |
| P.AUTHORIZATION<br><br>*Users must be authorized before performing Document Processing and administrative functions.* | O.USER_AUTHORIZATION restricts the ability to perform Document Processing and administrative functions to authorized Users.<br><br>O.USER_I&A provides the basis for authorization.<br><br>O.ADMIN_ROLES restricts the ability to authorize Users to authorized Administrators. |
| P.AUDIT<br><br>*Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.* | O.AUDIT requires the generation of audit data.<br><br>O.ACCESS_CONTROL restricts access to audit data in the TOE to authorized Users.<br><br>O.USER_AUTHORIZATION provides the basis for authorization. |
| P.COMMS_PROTECTION<br><br>*The TOE* must be able to identify itself to other devices *on the LAN.* | O.COMMS_PROTECTION protects LAN communications from man-in-the-middle attacks. |
| P.PURGE_DATA<br><br>*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.* | O.PURGE_DATA provides a function that makes all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices when invoked by an authorized administrator. |

| Threat/Policy/Assumption | Rationale |
|---|---|
| A.PHYSICAL<br><br>*Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.* | OE.PHYSICAL_PROTECTION establishes a protected physical environment for the TOE. |
| A.NETWORK<br><br>*The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.* | OE.NETWORK_PROTECTION establishes a protected LAN environment for the TOE. |
| A.TRUSTED_ADMIN<br><br>*TOE Administrators are trusted to administer the TOE according to site security policies.* | OE.ADMIN_TRUST establishes responsibility of the TOE Owner to have a trusted relationship with Administrators. |
| A.TRAINED_USERS<br><br>*Authorized Users are trained to use the TOE according to site security policies.* | OE.ADMIN_TRAINING establishes responsibility of the TOE Owner to provide appropriate training for Administrators.<br><br>OE.USER_TRAINING establishes responsibility of the TOE Owner to provide appropriate training for Users. |

# 5. Extended Components Definition

The following extended components defined in [HCD] are used in this Security Target. The following information is copied from [HCD]; note that paragraph numbering shown in this chapter corresponds to paragraph numbers in [HCD].

## 5.1 Extended SFR Component Definitions

### 5.1.1 FAU_STG_EXT Extended: External Audit Trail Storage

**Family Behavior:**

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

**Component leveling:**

| | |
|---|---|
| FAU_STG_EXT.1: Extended: 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.

**Management:**

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

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

**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.

**FAU_STG_EXT.1 Extended: 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.

**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.

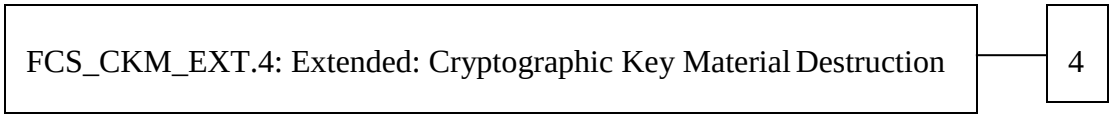
This extended component protects the audit records, and it is therefore placed in the FAU class with a single component.

### 5.1.2 FCS_CKM_EXT Extended: Cryptographic Key Management

**Family Behavior:**

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

**Component leveling:**




**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.

**Management:**

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

- There are no management actions foreseen.

**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.

**FCS_CKM_EXT.4 Extended: 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.

**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.

### 5.1.3 FCS_IPSEC_EXT Extended: IPsec selected

**Family Behavior:**

This family addresses requirements for protecting communications using IPsec.

**Component leveling:**


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

**Management:**

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

- There are no management actions foreseen.

**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

**FCS_IPSEC_EXT.1 Extended: 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.

**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.

### 5.1.4 FCS_RBG_EXT Extended: Cryptographic Operation (Random Bit Generation)

**Family Behavior:**

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.

**Component leveling:**


**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.

**Management:**

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

- There are no management actions foreseen.

**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.

**FCS_RBG_EXT.1 Extended: 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.

**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.

### 5.1.5 FIA_PMG_EXT Extended: Password Management

**Family Behavior:**

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.

**Component leveling:**


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

**Management:**

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

- There are no management actions foreseen.

**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.

**FIA_PMG _EXT.1 Extended: 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.

**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.

### 5.1.6 FIA_PSK_EXT Extended: Pre-Shared Key Composition

**Family Behavior:**

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

**Component leveling:**

| | |
|---|---|
| FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition | 1 |

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

**Management:**

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

- There are no management actions foreseen.

**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.

**FIA_PSK_EXT.1 Extended: 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*].

**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.

### 5.1.7 FPT_SKP_EXT Extended: Protection of TSF Data

**Family Behavior:**

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.

**Component leveling:**


**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.

**Management:**

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

- There are no management actions foreseen.

**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.

**FPT_SKP_EXT.1 Extended: 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.

**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.

### 5.1.8 FPT_TST_EXT Extended: TSF testing

**Family Behavior:**

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

**Component leveling:**


**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.

**Management:**

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

- There are no management actions foreseen.

**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.

**FPT_TST_EXT.1 Extended: 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.

**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.

### 5.1.9 FPT_TUD_EXT Extended: Trusted Update

**Family Behavior:**

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.

**Component leveling:**


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

**Management:**

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

- There are no management actions foreseen.

**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.

**FPT_TUD_EXT.1** Trusted 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.

**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.

# 6. Security Requirements

This section contains the functional requirements that are provided by the TOE.

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in underlined text

*Selection: indicated in italics*

*Assignments within selections: indicated in italics and underlined text*

**SFR operation completed or partially completed in the PP: Bold**

**Refinement: indicated with bold text**

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by letters in parentheses following the component or element (e.g., FAU_ARP.1(A)).

## 6.1 TOE Security Functional Requirements

**Table 9 - TOE Security Functional Requirements**

| SFR | Description |
|---|---|
| FAU_GEN.1 | Audit Data Generation |
| FAU_GEN.2 | User Identity Association |
| FAU_SAR.1 | Audit review |
| FAU_SAR.2 | Restricted audit review |
| FAU_STG.1 | Protected audit trail storage |
| FAU_STG.4 | Prevention of audit data loss |
| FAU_STG_EXT.1 | Extended: External Audit Trail Storage |
| FCS_CKM.1(a) | Cryptographic Key Generation (for asymmetric keys) |
| FCS_CKM_EXT.4 | Extended: Cryptographic Key Material Destruction |
| FCS_CKM.4 | Cryptographic key destruction |
| 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_IPSEC_EXT.1 | Extended: IPsec selected |
| FCS_RBG_EXT.1 | Extended: Cryptographic Operation (Random Bit Generation) |
| FDP_ACC.1 | Subset access control |
| FDP_ACF.1 | Security attribute based access control |
| FDP_RIP.1(b) | Subset residual information protection |
| FIA_AFL.1 | Authentication failure handling |
| FIA_ATD.1 | User attribute definition |
| FIA_PMG_EXT.1 | Extended: Password Management |
| FIA_PSK_EXT.1 | Extended: Pre-Shared Key Composition |
| FIA_UAU.1 | Timing of authentication |
| FIA_UAU.7 | Protected authentication feedback |
| FIA_UID.1 | Timing of identification |
| FIA_USB.1 | User-subject binding |
| FMT_MOF.1 | Management of security functions behavior |
| FMT_MSA.1 | Management of security attributes |
| FMT_MSA.3 | Static attribute initialization |

| SFR | Description |
|---|---|
| FMT_MTD.1 | Management of TSF data |
| FMT_SMF.1 | Specification of Management Functions |
| FMT_SMR.1 | Security roles |
| FPT_SKP_EXT.1 | Extended: Protection of TSF Data |
| FPT_STM.1 | Reliable time stamps |
| FPT_TST_EXT.1 | Extended: TSF testing |
| FPT_TUD_EXT.1 | Extended: Trusted Update |
| FTA_SSL.3 | TSF-initiated termination |
| FTP_ITC.1 | Inter-TSF trusted channel |
| FTP_TRP.1(a) | Trusted path (for Administrators) |
| FTP_TRP.1(b) | Trusted path (for Non-administrators) |

Note that paragraph numbering shown in this chapter corresponds to paragraph numbers in [HCD].

### 6.1.1 Security Audit (FAU)

#### 6.1.1.1 FAU_GEN.1 Audit 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 10,** [no other auditable events].

*Refinement Rationale: The table reference is changed to reflect the contents of the ST.*

**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 10**, [no other information].

*Refinement Rationale: The table reference is changed to reflect the contents of the ST.*

**Table 10 - Auditable Events**

| Auditable event | Relevant SFR | Additional information |
|---|---|---|
| Job completion | FDP_ACF.1 | Type of job, JobID |
| Job started | FDP_ACF.1 | Type of job, JobID, Source IP address for print jobs |
| Successful User identification and authentication | FIA_UAU.1, FIA_UID.1 | SessionID, Source IP address for remote users |
| Unsuccessful User authentication | FIA_UAU.1 | UserID supplied, Source IP address for remote users |
| Unsuccessful User identification | FIA_UID.1 | UserID supplied, Source IP address for remote users |
| Use of management functions | FMT_SMF.1 | Parameter ID, old and new values |
| 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 |
| Audit log cleared by authorized administrator | FAU_STG.1 | None |

#### 6.1.1.2 FAU_GEN.2 User 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.

#### 6.1.1.3 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 [U.ADMIN] 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.

#### 6.1.1.4 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.

#### 6.1.1.5 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.

#### 6.1.1.6 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 [*overwrite the oldest stored audit records*] and [take no other actions] if the audit trail is full.

#### 6.1.1.7 FAU_STG_EXT.1 Extended: 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.

### 6.1.2 Cryptographic Support (FCS)

#### 6.1.2.1 FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)

(for O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: [~~FCS_CKM.2 Cryptographic key distribution, or~~

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

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 [**

- ***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.**

#### 6.1.2.2 FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

(for O.COMMS_PROTECTION, 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.

#### 6.1.2.3 FCS_CKM.4 Cryptographic key destruction

(for O.COMMS_PROTECTION, 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(a) Refinement:** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [

**For volatile memory, the destruction shall be executed by a [*single overwrite consisting of [zeroes], removal of power to the memory*].**

**For nonvolatile memory the destruction shall be executed by a [*single overwrite consisting of [zeroes], block erase]*;**

] that meets the following: ***No Standard***.

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

(for O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: [~~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(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 [CBC mode]** and cryptographic key sizes **128-bits and 256-bits** that meets the following:

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

*Application Note: For this TOE, this SFR addresses AES for IPsec only.*

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

(for O.UPDATE_VERIFICATION, O.COMMS_PROTECTION)

Hierarchical to: No other components.

Dependencies: [~~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(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 **[**

- ***RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [2048 bits]]***

that meets the following **[**

- ***FIPS PUB 186-4, "Digital Signature Standard"***

].

#### 6.1.2.6 FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)

(selected in FPT_TUD_EXT.1.3)

Hierarchical to: No other components.

Dependencies: No dependencies.

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

#### 6.1.2.7 FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)

(selected with FCS_IPSEC_EXT.1.4)

Hierarchical to: No other components.

Dependencies: [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(b) Cryptographic key generation (Symmetric Keys)]

FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

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

#### 6.1.2.8 FCS_IPSEC_EXT.1 Extended: IPsec selected

(selected in FTP_ITC.1.1, FTP_TRP.1.1)

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 [*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 [*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*].

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

**FCS_IPSEC_EXT.1.6** The TSF shall ensure the encrypted payload in the [*IKEv1, IKEv2*] protocol uses the cryptographic algorithms AES-CBC-128, AES-CBC- 256 as specified in RFC 3602 and [*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 [*IKEv2 SA lifetimes can be established based on* [*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 [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 [*24 (2048-bit MODP with 256-bit POS)*].

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

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

(for 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 [*NIST SP 800-90A*] using [*CTR_DRBG (AES)*].

**FCS_RBG_EXT.1.2** The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [[*1*] *hardware-based noise source(s)*] with a minimum of [*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.

### 6.1.3 User Data Protection (FDP)

#### 6.1.3.1 FDP_ACC.1 Subset 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 11 - and Table 12 -.**

#### 6.1.3.2 FDP_ACF.1 Security 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 11 - and Table 12 -.**

**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 11 - and Table 12 -**.

**FDP_ACF.1.3 Refinement:** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [no additional rules].

**FDP_ACF.1.4 Refinement:** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [

1. The Job Owner of submitted print jobs is determined by a Userid included in the embedded PJL. Print jobs received without a Userid, or with an unknown Userid, or with a Userid of a user that does not have the Held Jobs Access permission, are deleted after the specified timeout period for releasing held print jobs. During this time, no access to the print jobs is possible since access is restricted to the job owner.].

**Table 11 - D.USER.DOC Access Control SFP**

| | | "Create" | "Read" | "Modify" | "Delete" |
|---|---|---|---|---|---|
| **Print** | ***Operation:*** | ***Submit a document to be printed*** | ***View image or Release printed output*** | ***Modify stored document*** | ***Delete stored document*** |
| | **Job owner (with Held Jobs Access)** | Yes | Release | No | Yes |
| | **Job owner (without Held Jobs Access)** | Yes, but deleted | denied | denied | denied |
| | **Unknown user** | Yes, but deleted | denied | denied | denied |
| | **No userid specified** | Yes, but deleted | denied | denied | denied |
| | **U.ADMIN** | U.ADMIN has no inherent privileges; rather this role can only create/access his/her own jobs and will fall into one of the categories listed above | | | |

| | | "Create" | "Read" | "Modify" | "Delete" |
|---|---|---|---|---|---|
| | **U.NORMAL** | U.NORMAL has no inherent privileges; rather this role can only create/access his/her own jobs and will fall into one of the categories listed above | | | |
| | **Unauthenticated** | See above categories | denied | denied | denied |

**Table 12 - D.USER.JOB Access Control SFP**

| | | "Create" | "Read" | "Modify" | "Delete" |
|---|---|---|---|---|---|
| **Print** | ***Operation:*** | ***Create print job*** | ***View print queue / log*** | ***Modify print job*** | ***Cancel print job*** |
| | **Job owner (with Held Jobs Access)** | Yes | Yes for itself | Modify # of copies | Yes for itself |
| | **Job owner (without Held Jobs Access)** | Yes, but deleted | denied | denied | denied |
| | **Unknown user** | Yes, but deleted | denied | denied | denied |
| | **No userid specified** | Yes, but deleted | denied | denied | denied |
| | **U.ADMIN** | U.ADMIN has no inherent privileges; rather this role can only create/access his/her own jobs and will fall into one of the categories listed above | | | |
| | **U.NORMAL** | U.NORMAL has no inherent privileges; rather this role can only create/access his/her own jobs and will fall into one of the categories listed above | | | |
| | **Unauthenticated** | See above categories | denied | denied | denied |

#### 6.1.3.3 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**.

### 6.1.4 Identification and Authentication (FIA)

#### 6.1.4.1 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 [*an administrator configurable positive integer within [1-10]*] unsuccessful authentication attempts occur related to [consecutive login attempts via the touch panel or web interface within the configured time period].

**FIA_AFL.1.2** When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [automatically lock the user account for the configured amount of time].

#### 6.1.4.2 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: [

1. Username
2. Password
3. Associated groups
4. User permissions, as specified by associated groups
5. Number of consecutive authentication failures
6. Time of the earliest authentication failure (since the last successful login if any have occurred)
7. Account lock status].

#### 6.1.4.3 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: *[“!”,*

*“@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [other ACII characters except CR and NL]*];

- Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater;

#### 6.1.4.4 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)

**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 [*[lengths from 1 to 36 characters]*];
- 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 [*SHA-1, SHA-256*] and be able to [*use no other pre-shared keys*].

#### 6.1.4.5 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 [submit print jobs; view operational status of the device] 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.

#### 6.1.4.6 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 [only asterisks ("*") or dots ("●")] to the user while the authentication is in progress.

#### 6.1.4.7 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 [submit print jobs; view operational status of the device] 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.

#### 6.1.4.8 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: [

1. Username
2. Associated groups
3. User permissions].

**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: [

1. The username are the values supplied by the user.
2. The associated groups are the values configured for the user account.
3. User permissions are determined by combining the configured permissions for each associated group.].

**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: [the security attributes do not change during a session].

### 6.1.5 Security Management (FMT)

#### 6.1.5.1 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 [*determine the behaviour of, disable, enable, modify the behaviour of*] the functions [

- Audit
- Identification and authentication
- Authorization and access controls
- Communication with External IT Entities
- Network communications
- System or network time source
- Device functions (e.g. Print)

] to **U.ADMIN**.

#### 6.1.5.2 FMT_MSA.1 Management of security attributes

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, ~~or~~

~~FDP_IFC.1 Subset information flow control~~]

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 [*query, modify, delete, [create]*] the security attributes

[Username, associated groups and user permissions] to [administrators authorized for access to the Security Menu].

#### 6.1.5.3 FMT_MSA.3 Static 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 [*restrictive*] default values for security attributes that are used to enforce the SFP.

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

#### 6.1.5.4 FMT_MTD.1 Management 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 13 **-.**

*Application Note: Since U.ADMIN is represented by multiple distinct permissions, the following table identifies the associated permission rather than grouping everything under the U.ADMIN role.*

**Table 13 - Management of TSF Data**

| Data | Operation | Authorized Role(s) (Associated Permission) |
|---|---|---|
| **TSF Data owned by a U.NORMAL or associated with Documents or jobs owned by a U.NORMAL** | | |
| D.USER.JOB | *Query, Delete* | **Held Jobs Access (for the user's own jobs only)** |
| **TSF Data not owned by a U.NORMAL** | | |
| Active Directory Configuration | *Create* | **Security Menu** |

| Data | Operation | Authorized Role(s) (Associated Permission) |
|---|---|---|
| Date and Time Parameters | *Query*, *Modify* | **Device Menu** |
| Enable Audit | *Query*, *Modify* | **Security Menu** |
| Enable HTTP Server | *Query*, *Modify* | **Network/Ports Menu** |
| Enable Remote Syslog | *Query*, *Modify* | **Security Menu** |
| Groups | *Query*, *Modify*, *Delete*, *Create* | **Security Menu** |
| Held Print Job Expiration Timer | *Query*, *Modify* | **Security Menu** |
| IPSec Settings | *Query*, *Modify* | **Network/Ports Menu** |
| Job Waiting | *Query*, *Modify* | **Device Menu** |
| Kerberos Setup | *Query*, *Modify* | **Security Menu** |
| LDAP Certificate Verification | *Query*, *Modify* | **Security Menu** |
| LDAP+GSSAPI – SFP Credentials | *Query*, *Modify* | **Security Menu** |
| LDAP+GSSAPI Configuration | *Query*, *Modify*, *Delete*, *Create* | **Security Menu** |
| Login Restrictions | *Query*, *Modify* | **Security Menu** |
| Network Port | *Query*, *Modify* | **Network/Ports Menu** |
| Permissions | *Query*, *Modify* | **Security Menu** |
| Remote Syslog Parameters | *Query*, *Modify* | **Security Menu** |
| Security Reset Jumper | *Query*, *Modify* | **Security Menu** |

| Data | Operation | Authorized Role(s) (Associated Permission) |
|---|---|---|
| Smart Card Authentication Client Configuration | *Query*, *Modify* | **Security Menu** |
| USB Buffer | *Query*, *Modify* | **Network/Ports Menu** |
| Username/Password Accounts | *Query*, *Modify*, *Delete*, *Create* | **Security Menu** |
| Visible Home Screen Icons | *Query*, *Modify* | **Device Menu** |
| **Software, firmware, and related configuration data** | | |
| Firmware | *Query* | **Reports Menu** |
| | *Modify* | **Firmware Updates** |

#### 6.1.5.5 FMT_SMF.1 Specification 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: [

- 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
- Configuring network communications
- Configuring the system or network time source
- Configuring data transmission to audit server
- Configuring internal audit log storage
- Configure applications
- Perform firmware updates
- Configure device functions

- Sanitize device].

#### 6.1.5.6 FMT_SMR.1 Security 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 Refinement:** The TSF shall maintain the roles **U.ADMIN, U.NORMAL**.

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

### 6.1.6 Protection of the TSF (FPT)

#### 6.1.6.1 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.

#### 6.1.6.2 FPT_STM.1 Reliable 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.

#### 6.1.6.3 FPT_TST_EXT.1 Extended: 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.

#### 6.1.6.4 FPT_TUD_EXT.1 Extended: 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 [*no other functions*] prior to installing those updates.

### 6.1.7 TOE Access (FTA)

#### 6.1.7.1 FTA_SSL.3 TSF-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 [configurable time interval of user inactivity in the range of 1 to 120 minutes for the web interface and 10 to 300 seconds for the touch panel].

### 6.1.8 Trusted Paths/Channels (FTP)

#### 6.1.8.1 FTP_ITC.1 Inter-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 [*IPsec*] to** provide **a trusted** communication channel between itself and **authorized IT entities supporting the**

**following capabilities: [*authentication server, [remote audit server, network time server]*]** 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 [**remote authentication, sending audit records, network time synchronization**].

#### 6.1.8.2 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** [***IPsec***] **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**.

#### 6.1.8.3 FTP_TRP.1(b) Trusted path (for Non-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(b) Refinement** : The TSF shall **use** [***IPsec*] to** provide **a trusted** communication path between itself and **remote** users 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(b) Refinement**: The TSF shall permit [***the TSF, remote users***] to initiate communication via the trusted path

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

## 6.2 Security Assurance Requirements

The Security Assurance Requirements are the EAL 1 components as specified in Part 3 of the Common Criteria. Note that these components are refined by the assurance activities stated in [HCD], which are included by reference.

**Table 14 - TOE Assurance Components Summary**

| Assurance Classes | Assurance Component | Description |
|---|---|---|
| Security Target | ASE_CCL.1 | Conformance claims |
| | ASE_ECD.1 | Extended components definition |
| | ASE_INT.1 | ST introduction |
| | ASE_OBJ.1 | Security objectives for the operational environment |
| | ASE_REQ.1 | Stated security requirements |
| | ASE_SPD.1 | Security Problem Definition |
| | ASE_TSS.1 | TOE summary specification |
| Development | ADV_FSP.1 | Basic Functional Specification |
| Guidance Documents | AGD_OPE.1 | Operational User Guidance |
| | AGD_PRE.1 | Preparative Procedures |
| Lifecycle Support | ALC_CMC.1 | Labeling of the TOE |
| | ALC_CMS.1 | TOE CM Coverage |
| Test | ATE_IND.1 | Independent Testing – Conformance |
| Vulnerability Assessment | AVA_VAN.1 | Vulnerability survey |

# 7. TOE Summary Specification

## 7.1 Security Functions

### 7.1.1 Identification, Authentication and Authorization

Users are required to successfully complete the I&A process before they are permitted to access any restricted data or functionality. The set of restricted user functionality is under the control of the administrators, with the exception of submission of network print jobs which is always allowed.

A new session is established for the touch panel when the system boots and for web sessions when the connection is established. All sessions are initially bound to the Guest (default) user. In the evaluated configuration, the Guest user has no access to restricted functions or data other than allowing print jobs to be submitted.

Users must log in as a different user in order to gain access to TOE functionality. Multiple login mechanisms are supported in the evaluated configuration: Smart Card authentication, Username/Password Accounts and LDAP+GSSAPI. Note that Smart Card and LDAP+GSSAPI authentications also use Kerberos functionality when authenticating certificates or credentials. Username/Password information is stored in flash.

For Smart Card authentication, no functions at the touch panel are allowed until I&A successfully completes. The touch panel displays a message directing the user to insert a card into the attached reader. Once a card is inserted, the user is prompted for a PIN. When the PIN is entered, only asterisks ("*") or dots ("●") are displayed. Asterisks are displayed on the touch panel; dots are displayed on the web interface. Once the PIN is collected (indicated by the user touching the Next button), the TOE passes the PIN to the card for validation. If it is not valid, a message is displayed on the touch panel and the user is asked to re-enter the PIN. After the card-configured number of consecutive invalid PINs, the card will lock itself until unlocked by a card administrator.

Upon successful card validation, the TOE forwards the certificate from the card to the configured Kerberos Key Distribution Center (Windows Domain Controller) for validation. If the certificate validation is not successful, an error message is displayed on the touch panel until the current card is removed from the reader. If the certificate validation is successful, the TOE binds the username, account name, and email address (all obtained from the KDC/LDAP server) to the user session for future use. An audit record for the successful authentication is generated. All communication with the KDC and LDAP server uses IPsec.

For Username/Password Accounts and LDAP+GSSAPI, the TOE collects a username and password via the touch panel or via the browser session. When the password is entered, only asterisks ("*") are displayed. Once the username and password are collected, the next step in the process depends on the I&A mechanism being used.

For Username/Password Accounts, the TOE performs the validation of the username and password against the set of configured Username/Password Accounts. If the validation fails because of an invalid password (for a valid username), the count of failed authentication attempts is incremented for that account. If the threshold for failed attempts within a time period is reached, then the account is marked as being locked for the configured amount of time to mitigate against brute force password attacks.

For LDAP+GSSAPI, the TOE hashes the supplied password and forwards the username in an authentication request signed by the hashed password to the configured KDC for validation (using the configured machine credentials) and waits for the response. If no response is received, the validation is considered to have failed.

In the case of failed validations, an error message is displayed via the touch panel or browser session, and then the display returns to the previous screen for further user action. An audit record for the failed authentication attempt is generated.

If validation is successful, the TOE retrieves the account name and email address from the LDAP server and binds them to the user session for future use. An audit record for the successful authentication is generated.

Permissions for the user session are determined from group memberships. Authorized Administrators assign roles to user accounts by configuring permissions for each configured group and then assigning user accounts to groups. At minimum, during installation Authorized Administrators must perform the user account configuration activities in the guidance documentation to establish the evaluated configuration:

- Create new groups for Authorized Administrators and Authorized Users. The group names must correspond to names used in the LDAP server of Smart Card or LDAP+GSSAPI authentication is used.
- Configure appropriate permissions for each of those groups
- Assign all users and administrators using Username/Password Accounts to groups
- Modify the Public permissions (which are the only permissions for the Guest user account so that only B/W Print and Color Print are configured

For Username/Password accounts, the permissions for each group that the user is a member of (as specified in the account configuration) are combined. For Smart Cards and LDAP+GSSAPI, a list of group memberships are retrieved from the LDAP server. For each of those groups that match a group configured in the TOE, the permissions are combined. If the group memberships or permissions are changed, active sessions are not affected; the changes take effect at the next login.

The user session is considered to be active until the user explicitly logs off, removes the card or the administrator-configured inactivity timer for sessions expires. The timer values are separately configurable: 1 to 120 minutes for the web interface and 10 to 300 seconds for the touch panel.

Users of the TOE, whether accessing the TOE via the touch panel or web interface, are considered to be in one or more of the following categories:

- Authorized Users – permitted to perform one or more of the user functions defined in FDP_ACC.1 and FDP_ACF.1.
- Authorized Administrators – permitted to access administrative functionality for control and monitoring of the SFP operation.
- Any Users – Authorized Users and Authorized Administrators

The following Permissions may be configured for groups:

**Table 15 - Permissions**

| Item | Description | Comment |
|---|---|---|
| Address Book | Controls the ability to manage the Address Book contents. | Permission may only be granted to authorized administrators in the evaluated configuration |
| Apps Configuration | Controls access to the configuration of any installed applications | Permission may only be granted to authorized administrators in the evaluated configuration. |
| B/W Print | Controls the ability to accept black and white print jobs. | Permission must be granted to the Public permissions |
| Cancel Jobs at the device | Controls access to the functionality to cancel jobs via the touch panel. | Permission may only be granted to authorized users in the evaluated configuration |
| Change Language from Home Screen | Controls access to the Change Language button on the Home screen (when displayed); this button is NOT displayed by default but a user can activate it via the “General Settings Menu” | Permission may be granted to any users |
| Color Dropout | Controls a user’s ability to activate the Color Dropout functionality as part of a job; if protected and the user fails to authenticate, then the device DOES NOT use the color dropout functionality in the job | Permission may only be granted to authorized users in the evaluated configuration |
| Color Print | Controls the ability to print color jobs. | Permission must be granted to the Public permissions |
| Device Menu | Controls access to the Device administrative menu | Permission may only be granted to authorized administrators in the evaluated configuration |
| Firmware Updates | Controls a user’s ability to update the device’s firmware code via the network | Permission may only be granted to authorized administrators in the evaluated configuration |
| Flash Drive Color Printing | Controls whether USB interfaces may be used for color print operations | Permission must not be specified for any user |
| Flash Drive Print | Controls whether USB interfaces may be used for black and white print operations | Permission must not be specified for any user |
| Function Configuration Menus | Controls access to the configuration menus for the print functions. | Permission may only be granted to authorized administrators in the evaluated configuration |
| Held Jobs Access | Controls access to the Held Jobs function | Permission may only be granted to authorized users in the evaluated configuration |
| Import/Export Settings | Controls the ability to import and export configuration files | Permission may only be granted to authorized administrators in the evaluated configuration |
| Internet Printing Protocol (IPP) | Controls access to print job submission via IPP | Permission must not be specified for any user |
| Manage Bookmarks | Controls access to the Delete Bookmark, Create Bookmark, and Create Folder buttons from both the bookmark list screen and from the individual bookmark screen | Permission must not be specified for any user |

| Item | Description | Comment |
|---|---|---|
| Manage Shortcuts | Controls access to the Manage Shortcuts Menu | Permission must not be specified for any user |
| Network/Ports Menu | Controls access to the Network/ Ports Menu | Permission may only be granted to authorized administrators in the evaluated configuration |
| New Apps | Controls access to configuration parameters for apps subsequently added to the device. | Permission may only be granted to authorized administrators in the evaluated configuration |
| Option Card Menu | Controls a user's ability to access the "Option Card Menu" that displays menu nodes associated with installed DLEs | Permission may only be granted to authorized administrators in the evaluated configuration |
| Out of Service Erase | Controls the ability to wipe the storage of the SFP when it is being taken out of service. | Permission may only be granted to authorized administrators in the evaluated configuration |
| Paper Menu | Controls access to the Paper Menu | Permission may be granted to any users |
| Remote Management | Controls whether or not management functions may be invoked from remote IT systems | Permission must not be specified for any user |
| Reports Menu | Controls access to the Reports Menu. This includes information about user jobs, which can't be disclosed to non-administrators. | Permission may only be granted to authorized administrators in the evaluated configuration |
| Search Address Book | Controls access to the Search Address Book button | Permission may be granted to any users |
| Security Menus | Controls access to the Security Menu | Permission may only be granted to authorized administrators in the evaluated configuration |
| Supplies Menus | Controls access to the Security Menu | Permission may only be granted to authorized administrators in the evaluated configuration |
| Use Profiles | Controls a user's ability to execute any profile | Permission must not be specified for any user |

**Table 16 - Identification, Authentication and Authorization SFR Details**

| SFR | Description |
|---|---|
| FCS_CKM_EXT.4 | When Username/Password accounts are deleted, the associated password is destroyed in flash. Passwords in memory are destroyed as soon as login validation is completed. |
| FCS_CKM.4 | When Username/Password accounts are deleted, the associated password in flash is overwritten with zeros. Passwords in memory are zeroized as soon as login validation is completed. |
| FIA_AFL.1 | Consecutive login failures for each user account within a configured time period are tracked, and if the configured limit is reached the user account is automatically locked for the configured amount of time. |

| SFR | Description |
|---|---|
| FIA_ATD.1 | The TSF maintains the following security attributes for users:<br>• Username (configured for internal account, acquired from LDAP server AD and Smartcards)<br>• Password (internal accounts)<br>• Associated groups (configured for internal account, acquired from LDAP server AD and Smartcards)<br>• Permissions (dynamically determined by group memberships)<br>• Number of consecutive login failures<br>• Time of earliest login failure (since last successful login)<br>• Account lock status |
| FIA_PMG_EXT.1 | Passwords for internal accounts are configured by administrators. The minimum password length is configurable from 1-32 characters. Passwords may contain any ASCII characters other than NL and CR. |
| FIA_UAU.1 | User interaction through the touch panel and web interface prior to successful authentication is limited to viewing the operational status of the device (e.g. low paper). Users may submit print jobs without authenticating, but the jobs are not printed until released by the authenticated user. |
| FIA_UAU.7 | When a password or PIN is entered for authentication, only asterisks ("*") or dots ("●") are displayed. |
| FIA_UID.1 | User interaction through the touch panel and web interface prior to successful identification is limited to viewing the operational status of the device. Users may submit print jobs and supply identification via embedded PJL, but the jobs are not printed until released by the authenticated user. Invalid and missing identification in print jobs results in those print jobs being deleted. |
| FIA_USB.1 | Upon successful login, the username, associated groups and permissions are bound to the session. The username is the value specified during login or the username associated with the certificate from a smartcard. The groups are those configured internally or on the LDAP server. The permissions are the union of the permissions for each associated group. These bindings do not change during an active session. |
| FTA_SSL.1 | Upon expiration of an inactivity timer, the corresponding session is automatically terminated. |

#### 7.1.1.1 Active Directory Additional Information

If Active Directory parameters are supplied and Join is selected, the parameter values are used to join the Active Directory Domain. If successful, machine credentials are generated and the LDAP+GSSAPI configuration parameters are automatically updated with the Domain and machine information.

Once the Domain has been joined, subsequent I&A attempts may use the LDAP+GSSAPI configuration to validate user credentials using the newly-created machine credentials as described above. The credentials specified for Active Directory by an authorized administrator are not saved.

Communication with the Active Directory server uses IPsec.

### 7.1.2 Access Control

Access control validates a user access request against the session's permissions.

Authorization is restricted by not associating a permission with a function.

When the FAC is a menu, access is also restricted to all submenus (a menu that is normally reached by navigating through the listed item). This is necessary for instances where a shortcut could bypass the listed menu. If a shortcut is used to access a sub-menu, the access control check for the applicable menu item is still performed (as if normal menu traversal was being performed).

When a function is restricted, the access control function determines if the user has permission to access the function. Normally the icons for the functions the user is not permitted to access are not displayed in the GUI.

The following table summarizes the access controls and configuration parameters used by the TOE to control user access to the SFP functions provided by the TOE. Additional details for each function are provided in subsequent sections.

**Table 17 - TOE User Function Access Control**

| Function | Access Control Rules | Configuration Parameter Rules |
|---|---|---|
| Print | Network print jobs can always be submitted. The job is held until released by a user who is authorized for the Held Jobs Access function and has the same userid as was specified in the SET USERNAME PJL statement. Network print jobs without a PJL SET USERNAME statement are automatically deleted after the expiry period for held jobs. | Allowed |

**Table 18 - User Functions Access Control SFR Details**

| SFR | Description |
|---|---|
| FDP_ACC.1/FDP_ACF.1 | Access to user functions is controlled as specified in these SFRs. |

**Printing**

Submission of print jobs from users on the network is always permitted. Jobs that do not contain a PJL SET USERNAME statement are discarded after the configured held jobs expiry period. Submitted jobs are always held on the TOE until released or deleted by a user authorized for the appropriate access control and whose userid matches the username specified when the job was submitted. Users are able to display the queue of their pending print jobs. If a held job is not released within the configured expiration time, the job is automatically deleted.

In the evaluated configuration, the setdevparams, setsysparams and setuserparams Postscript operators are made non-operational so that the Postscript DataStream can not modify configuration settings in the TOE.

### 7.1.3 Trusted Communications

During TOE installation, a 2048-bit self-signed certificate for the device is generated in accordance with NIST SP 800-56B Revision 1 (“Recommendation for Pair-Wise Key

Establishment Schemes Using Integer Factorization Cryptography" for RSA- based key establishment schemes).

IPSec with ESP operating in transport mode is required for all network datagram exchanges of any type with remote IT systems. This includes the following IT systems:

- Workstations submitting print jobs
- Workstations initiating connections to the web interface
- Remote Syslog server
- KDC
- LDAP server (including Active Directory)

IPSec provide confidentiality, integrity and authentication of the endpoints. Supported encryption options for ESP are AES-CBC-128 and AES-CBC-256. SHA-256 and SHA-384 are supported for HMACs.

ISAKMP and IKEv1/v2 are used to establish the Security Association (SA) and session keys for the IPSec exchanges. For IKEv1, Main Mode is always used for Phase 1 exchanges (Aggressive Mode is never used). Diffie-Hellman is used for the IKE Key Derivation Function as specified in RFC2409, using Oakley Groups 14 or 24. SA lifetimes for both IKEv1 and IKEv2 can be limited to separately configurable times for each phase: 1 to 24 hours for Phase 1, and 1 to 8 hours for Phase 2.

When the TOE receives an IKE proposal, it selects the first proposed DH group that matches a DH group configured in the TOE (DH Groups 14 or 24) and the negotiation will fail if there is no match. Similarly, when the TOE initiates the IKE protocol, a proposal is sent with all of the DH groups that are configured. The peer will select the first match from the IKE proposal against its configured DH groups; the negotiation fails if no match is found.

Peer authentication is performed using the RSA algorithm and certificates and/or pre-shared keys.

During the ISAKMP exchange, the TOE requires the remote IT system to provide a certificate and the RSA signature for it is validated, or text-based Pre-Shared Keys (PSKs) may be configured by administrators and validated between endpoints. PSKs configured in the system may be 1 to 36 characters in length, composed of the characters specified in FIA_PSK_EXT.1.2, and are conditioned using SHA-1, SHA-256, or SHA-384. The key size specified in the SA exchange may be 128 or 256 bits, the encryption algorithm is AES-CBC, and the Hash Authentication Algorithm is SHA-1, SHA-256, or SHA-384.

If an incoming IP datagram does not use IPSec with ESP, the datagram is discarded. The Security Policy Database is dynamically built with an accept/protect rule for each of the configured pre-shared keys and certificates, permitting packets from the addresses associated with them, and a default "final rule" to discard all other traffic. Incoming packets are validated against the SPD. Essentially incoming IP datagrams from authorized addresses (with PSKs or certificates) are accepted, and all other IP datagrams are discarded per the default final rule.

If external accounts are defined, LDAP+GSSAPI is used for the exchanges with the LDAP server. Kerberos v5 is supported for exchanges with the LDAP server.

All session keys are stored in dynamic RAM. The TOE zeroizes the session keys by overwriting once with zeros when the sessions are terminated. Any copy of an RSA private key or PSK in

RAM is destroyed when power is turned off or by overwriting with zeroes when the buffer holding it is released. Section in 7.1.8 provides information concerning destruction of keys stored in flash memory.

**Table 19 - Trusted Communications SFR Details**

| SFR | Description |
|---|---|
| FCS_CKM.1(a) | A 2048-bit asymmetric key pair is generated in accordance with NIST SP 800-56B during installation. |
| FCS_CKM_EXT.4 | Session keys are destroyed when sessions terminate. PSKs are destroyed when the PSKs are deleted from the configuration by an authorized administrator. |
| FCS_CKM.4 | Session keys are overwritten with zeros when sessions terminate. |
| FCS_COP.1(a) | IPsec traffic is encrypted using AES-CBC-128 or AES-CBC-256. |
| FCS_COP.1(c) | IPsec keyed-hash message authentication codes use hash algorithms supplied by the TOE. |
| FCS_COP.1(g) | IPsec uses keyed-hash message authentication codes that are authenticated by the TOE. |
| FCS_IPSEC_EXT.1 | IPsec is implemented as described in the text preceding this table. |
| FCS_RBG_EXT.1 | An RBG function conforming to NIST SP 800-90A using CTR_DRBG(AES) is used to generate the asymmetric key pair. Entropy is provided by a hardware source that is described in more detail in the ancillary Entropy document. |
| FIA_PSK_EXT.1 | Text-based PSKs are supported and conditioned using SHA-1 or SHA-256. |
| FTP_ITC.1 | Trusted channels using IPsec are supported for authentication servers, remote audit servers, and network time servers. |
| FTP_TRP.1(a) | Trusted paths using IPsec are supported for administrators using the web interface. |
| FTP_TRP.1(b) | Trusted paths using IPsec are supported for users submitting print jobs. |

**Table 20 - NIST SP800-56B Conformance**

| Section # | “should”, “should not”, or “shall not” | Implemented accordingly? | Rationale for deviation |
|---|---|---|---|
| 5.6 | should | Yes | n/a |
| 5.8 | shall not | Yes | n/a |
| 5.9 | shall not (first occurrence) | Yes | n/a |
| 5.9 | shall not (second occurrence) | Yes | n/a |
| 6.1 | should not | Yes | n/a |
| 6.1 | should (first occurrence) | Yes | n/a |
| 6.1 | should (second occurrence) | Yes | n/a |
| 6.1 | should (third occurrence) | Yes | n/a |
| 6.1 | should (fourth occurrence) | Yes | n/a |
| 6.1 | shall not (first occurrence) | Yes | n/a |
| 6.1 | shall not (second occurrence) | Yes | n/a |
| 6.2.3 | should | Yes | n/a |
| 6.5.1 | should | Yes | n/a |
| 6.5.2 | should | Yes | n/a |

| Section # | "should", "should not", or "shall not" | Implemented accordingly? | Rationale for deviation |
|---|---|---|---|
| 6.5.2.1 | should | Yes | n/a |
| 6.6 | shall not | Yes | n/a |
| 7.1.2 | should | Yes | n/a |
| 7.2.1.3 | should | Yes | n/a |
| 7.2.1.3 | should not | Yes | n/a |
| 7.2.2.3 | should (first occurrence) | Yes | n/a |
| 7.2.2.3 | should (second occurrence) | Yes | n/a |
| 7.2.2.3 | should (third occurrence) | Yes | n/a |
| 7.2.2.3 | should (fourth occurrence) | Yes | n/a |
| 7.2.2.3 | should not | Yes | n/a |
| 7.2.2.3 | shall not | Yes | n/a |
| 7.2.3.3 | should (first occurrence) | Yes | n/a |
| 7.2.3.3 | should (second occurrence) | Yes | n/a |
| 7.2.3.3 | should (third occurrence) | Yes | n/a |
| 7.2.3.3 | should (fourth occurrence) | Yes | n/a |
| 7.2.3.3 | should (fifth occurrence) | Yes | n/a |
| 7.2.3.3 | should not | Yes | n/a |
| 8 | should | Yes | n/a |
| 8.3.2 | should not | Yes | n/a |

### 7.1.4 Administrative Roles

The TOE provides the ability for authorized administrators to manage TSF data from remote IT systems via a browser session or locally via the touch panel. Authorization is granular, enabling different administrators to be granted access to different TSF data.

Authorized administrators (U.ADMIN) have one or more permissions to access management menus and/or functions. The individual permissions that administrators have determine what management functions (as defined in FMT_SMF.1) they may perform. The following table provides a correlation between functions and the required permission.

**Table 21 - Function Correspondence to Permissions**

| Management Function | Required Permission |
|---|---|
| User management | Security Menus |
| Role management | Security Menus |
| Configuring identification and authentication | Security Menus |
| Configuring authorization and access controls | Security Menus |
| Configuring communication with External IT Entities | Network/Ports Menu |
| Configuring network communications | Network/Ports Menu |
| Configuring the system or network time source | Network/Ports Menu |
| Configuring data transmission to audit server | Security Menus |
| Configuring internal audit log storage | Security Menus |
| Configure applications | Apps Configuration |

| Management Function | Required Permission |
|---|---|
| Perform firmware updates | Firmware Updates |
| Configure device functions | Function Configuration Menus |
| Sanitize device | Out of Service Erase |

If defined users have no management permissions, they are considered to have the U.NORMAL role and have no access to management functions or data.

When new users are defined, by default they have no associated groups, and therefore no access to management functions or job functions (restrictive default attributes).

Neither the web interface nor the touch panel provide the ability to view the values of PSKs, symmetric keys or private keys for any administrator or user.

**Table 22 - Administrative Roles SFR Details**

| SFR | Description |
|---|---|
| FMT_MOF.1 | Administrators with the appropriate permissions have the ability to disable, enable and control the behavior of the specified functions. |
| FMT_MSA.1 | Only administrators with the Security Menus permission may query, modify, delete or create user accounts or groups. |
| FMT_MSA.3 | By default, new users have no group memberships and therefore restrictive permissions. |
| FMT_MTD.1 | Administrator operations on specific TSF data is determined by their permissions as described in Table 13 -. Users have no access to TSF data. |
| FMT_SMF.1 | Management functionality for the listed functions is provided to administrators as described in Table 21 -. |
| FMT_SMR.1 | Administrators have one or more permission related to management functionality. Users have job function permissions only. |
| FPT_SKP_EXT.1 | PSKs, symmetric keys and private keys are stored in flash. No mechanism is provided to read PSKs, symmetric keys or private keys. |

### 7.1.5 Auditing

The TOE generates audit event records for security-relevant events. The events that cause audit records to be generated are specified in section 6.1.1.1 . A time stamp is inserted into each record; reliable time is maintained via internal hardware or NTP. When NTP is used, it must be transmitted over IPsec (all communication with the TOE must use IPsec). A severity level is associated with each type of auditable event; only events at or below the severity level configured by an administrator are generated. Per the evaluated configuration, the severity level must be set to 5 (Notice).

Audit records are stored internally as well as being sent to a configured remote syslog server. Communication with the remote syslog server uses the Syslog protocol with IPsec.

Audit records for Successful Login events include the userid of the user as well as a session identifier. Other audit records include the session identifier, enabling the userid associated with other audit records to be determined via the corresponding Successful Login record. The time field in audit records is supplied by the TOE if internal time is configured by an administrator or by an NTP server if external time is configured.

Audit records sent to the remote syslog server follow the syslog format defined in the Berkeley Software Distribution (BSD) Syslog Protocol (RFC 3164). The TOE supplies the PRI, HEADER, MSG/TAG, and MSG/CONTENT fields for all messages. The CONTENT portion may contain the following fields (in order, separated by commas):

- Event Number
- ISO 8601 time ([YYYY-MM-DD]T[hh:mm:ss])
- Severity
- Process (same as TAG)
- Remote IPv4 address
- Remote IPv6 address
- Remote Hostname
- Remote Port
- Local Port
- Authentication/Authorization method
- Username
- Setting ID
- Setting's old and new values
- Event name
- Event data

Fields in the CONTENT section that are not relevant for specific events are blank. The remote IPv4 address, remote IPv6 address, remote hostname, remote port, and local port fields are always blank for events resulting from actions at the SFP (e.g. usage of the touch panel).

Audit records are stored in the internal log as they are generated. If the internal audit log storage space usage reaches 98% of capacity, the oldest records are purged until used space is lowered to 80%.

Using the web interface, administrator with the Security Menu permission may upload the audit log in syslog or CSV format to their remote system via the browser connection. The audit log is saved as a local file and may be reviewed by the administrator. These administrators may also clear (empty) the audit log. When this action is performed, an Audit Log Cleared record is generated to note this action. Audit records may not be modified.

No users, or administrators without the Security Menu permission, may view, modify or delete audit records.

**Table 23 - Auditing SFR Details**

| SFR | Description |
|---|---|
| FAU_GEN.1 | Audit records are generated for the events and with the content specified in Table 10 -. Audit records are stored in an internal log and transmitted to a remote syslog server. Storage space allocated for internal audit log storage is 1 MB. |
| FAU_GEN.2 | Users can be associated with audit events performed by identified users. |
| FAU_SAR.1 | Administrators with the Security Menu permission may view the internal audit log via the web interface. |
| FAU_SAR.2 | Only Administrators with the Security Menu permission may view the internal audit log. |
| FAU_STG.1 | Only Administrators with the Security Menu permission may clear the internal audit log. No functionality is provided to modify audit records. |
| FAU_STG.4 | When internal audit log space is exhausted, the oldest records in the log are discarded. |
| FAU_STG_EXT.1 | Audit records are transmitted to a remote audit server via the syslog protocol over IPsec. |
| FPT_STM.1 | The TOE maintains a reliable time stamp via internal hardware or NTP. |

### 7.1.6 Trusted Operation

During initial start-up, the TOE performs self tests on the cryptographic components.

The following tests are performed during start-up:

- Executable code integrity testing – A digital signature (RSA 2048, SHA256) of the executable code is calculated and compared to a saved value in flash.
- Memory testing – Fixed values are written to memory and read back to ensure memory is functioning properly.
- Processor testing – Basic arithmetic functions of the processor are verified.
- Cryptographic algorithm testing – Uses Known Answer Tests (KATs) to verify proper operation of cryptographic functions.

Executable code is distributed as Flash files (.FLS). A digital signature of the FLS file is calculated (RSA 2048 key and SHA256) by Lexmark when it is built and the signature is inserted into the FLS file. The signature of the file is verified before an update is applied. On each boot, the signature is also verified.

During operation, a SHA256 hash is maintained for each executable page. Before any page is loaded into memory, the hash is verified to ensure the code has not been modified since boot.

If any problems are detected with the hardware or stored TSF executable code, an appropriate error message is posted on the touch screen and operation is suspended.

Administrators may use the web interface to query the current firmware version or supply firmware updates. Firmware updates must be digitally signed, and the TOE verifies the signature before applying the update.

**Table 24 - Trusted Operation SFR Details**

| SFR | Description |
|---|---|
| FCS_COP.1(b) | Digital signatures of update files are authenticated before being applied. |
| FCS_COP.1(c) | Digital signatures verification relies on hash algorithms supplied by the TOE. |
| FPT_TST_EXT.1 | A set of self-tests are executed at start-up to verify correct operation of the TOE. |
| FPT_TUD_EXT.1 | Administrators may use the web interface to query the current firmware version and supply signed updates. |

### 7.1.7 Data Clearing and Purging

The TOE overwrites RAM with a fixed pattern upon deallocation of any buffer used to hold user data or sensitive TSF data such as keying material.

An administrator may command the TOE to be sanitized (e.g. prepared for decommissioning). For this operation, all flash data is zeroized.

**Table 25 - Data Clearing and Purging SFR Details**

| SFR | Description |
|---|---|
| FDP_RIP.1(b) | When purging is commanded by an administrator, flash storage is zeroized. |

### 7.1.8 Common Functionality Regarding Key Destruction in Flash Memory

Multiple types of keys are stored in flash memory: RSA private keys, PSKs, and the disk encryption key. The flash component performs wear leveling/garbage collection; therefore, physical copies of these keys may continue to exist inside the flash component for some period of time after they have been “overwritten” by the software.

When any of these keys are destroyed, they are first overwritten in flash memory with zeroes. Therefore, the visible storage locations for these items from the flash component reflect the overwrites.

The flash component supports the TRIM command and implements garbage collection to destroy the persistent copies of the old storage locations when not actively engaged in other tasks. The file system that maps to the flash component, and on which these keys are stored, also supports the TRIM command and the file system is configured to use it.

### 7.1.9 CAVP Certificates

The following CAVP certificates apply to this evaluation.

**Table 26 - CAVP Certificates**

| Crypto Function | Certificate #s | Associated SFRs |
|---|---|---|
| AES (CBC) | 5892/5932 (Gem-32bit) | FCS_COP.1(a)<br>FCS_IPSEC_EXT.1 |
| DRBG (CTR_DRBG (AES)) | 2485 (Gem-32bit) | FCS_RBG_EXT.1 |

| Crypto Function | Certificate #s | Associated SFRs |
|---|---|---|
| HMAC | 3867/3910 (Gem-32bit) | FCS_COP.1(g)<br>FCS_IPSEC_EXT.1 |
| RSA | 3113 (Gem-32bit) | FCS_CKM.1(a)<br>FCS_COP.1(b) |
| SHA | 4643/4687 (Gem-32bit) | FCS_COP.1(c)<br>FCS_IPSEC_EXT.1 |
| CVL (IKEv1, IKEv2) | 2161 (Gem-32bit) | FCS_IPSEC_EXT.1 |

# 8. Rationale

## 8.1 Security Requirements Rationale

### 8.1.1 Rationale for Security Functional Requirements of the TOE Objectives

The following information is copied from [HCD].

**Table 27 - Security Functional Requirements Rationale**

| Objective / SFR | Relationship | Rationale |
|---|---|---|
| **O.ACCESS_CONTROL** - ***The TOE shall enforce access controls to protect User Data and TSF Data in accordance with security policies***. | | |
| FDP_ACC.1 | Satisfies | This SFR defines the access control policy that is used to protect access to User Data and TSF Data. |
| FDP_ACF.1 | Satisfies | This SFR defines the specific rule-set that constitutes the access control policy, identifying the conditions under which access to resources, functions, and data are authorized or denied." |
| FMT_MSA.1 | Supports | The management of the product configuration, security settings, and user attributes and authorizations is critical to maintaining operational security. These management functions, as a group, provide for the ability of authorized administrators to configure the system, add and delete users, grant user-specific authorizations to system data, resources, and functions, introduce code (e.g., updates) into the system, and assign users to roles. Additionally, the SFRs also require that management functions be limited to users who have been explicitly authorized to perform management functions. |
| FMT_MSA.3 | Supports | |
| FMT_MTD.1 | Supports | |
| FMT_SMF.1 | Supports | |
| FMT_SMR.1 | Supports | |
| **O.ADMIN_ROLES** - ***The TOE shall ensure that only authorized Administrators are permitted to perform administrator functions***. | | |
| FIA_UID.1 | Supports | This SFR defines the TOE management functions that can be accessed without requiring Administrator authorization. |
| FMT_MOF.1 | Satisfies | This SFR defines the authorizations that are required for Administrators to access TOE functions. |
| FMT_SMF.1 | Satisfies | This SFR defines the administrative functions that are provided by the TSF. |
| FMT_SMR.1 | Satisfies | This SFR defines the different roles that can be assigned to Administrators for the purposes of determining authentication and authorization. |
| **O.COMMS_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***. | | |
| FCS_CKM.1(a) | Satisfies | This SFR defines the use of secure algorithms for key pair generation that can be used for key transport during protected communications. |
| FCS_CKM.4 | Supports | This SFR defines the method of data erasure used by FCS_CKM_EXT.4 that provides assurance that cryptographic keys that need to be erased cannot be recovered. |
| FCS_CKM_EXT.4 | Supports | This SFR ensures that residual cryptographic data cannot be used to compromise protected communications. |

| Objective / SFR | Relationship | Rationale |
|---|---|---|
| FCS_COP.1(a) | Satisfies | This SFR defines the use of a secure symmetric key algorithm that can be used for protected communications. |
| FCS_COP.1(g) | Selection | This SFR defines the use of a secure HMAC algorithm that can be used for protected communications. |
| FCS_IPSEC_EXT.1 | Selection | This SFR defines secure communications protocols that can be used to protect the transmission of security- relevant data. |
| FCS_RBG_EXT.1 | Supports | This SFR supports protected communications by defining a secure method of random bit generation that allows cryptographic functions to operate with their theoretical maximum strengths. |
| FIA_PSK_EXT.1 | Selection | This SFR defines the use of pre-shared keys in IPsec which allows for the secure implementation of that protocol. |
| FPT_SKP_EXT.1 | Satisfies | This SFR prevents the compromise of protected communications by ensuring that secret cryptographic data is protected against unauthorized access. |
| FTP_ITC.1 | Satisfies | This SFR defines the interfaces over which protected communications are required and the methods used to protect the communications used to transit those interfaces. |
| FTP_TRP.1(a) | Satisfies | This SFR defines the protected communications path that is used to secure Administrator interaction with the TOE. |
| FTP_TRP.1(b) | Satisfies | This SFR defines the protected communications path that is used to secure user interaction with the TOE. |
| **O.PURGE_DATA** - ***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***. | | |
| FCS_CKM.4 | Satisfies | This SFR defines the physical mechanism used to accomplish the data purge defined by FCS_CKM_EXT.4. |
| FCS_CKM_EXT.4 | Satisfies | This SFR defines the ability of the TSF to purge data from storage. |
| FDP_RIP.1(b) | Satisfies | This SFR requires the TSF to purge all User Data and TSF Data as part of the decommissioning process. |
| **O.AUDIT** - ***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***. | | |
| FAU_GEN.1 | Satisfies | This SFR defines the auditable events for which the TOE generates audit data and the fields that are included in each audit record. |
| FAU_GEN.2 | Satisfies | This SFR defines the ability of the TOE to apply attribution to all activities performed by a user or Administrator. |
| FAU_SAR.1 | Option | This SFR defines the ability of Administrators to read audit data that is stored on the TOE. |
| FAU_SAR.2 | Option | This SFR protects stored audit data from unauthorized access. |
| FAU_STG.1 | Option | This SFR ensures that audit data cannot be modified by untrusted subjects. |

| Objective / SFR | Relationship | Rationale |
|---|---|---|
| FAU_STG.4 | Option | This SFR ensures the availability of audit data by taking automatic action in the event the audit storage space is exhausted. |
| FAU_STG_EXT.1 | Satisfies | This SFR defines the ability of the TSF to transmit generated audit data to an external entity using a protected channel |
| FPT_STM.1 | Supports | This SFR ensures that audit data is labeled with accurate timestamps. |
| FTP_ITC.1 | Supports | This SFR defines the protected communications channel(s) over which audit data can be transmitted. |
| **O.TSF_SELF_TEST** - ***The TOE shall test some subset of its security functionality to help ensure that subset is operating properly***. | | |
| FPT_TST_EXT.1 | Satisfies | This SFR defines the ability of the TSF to perform self- tests which assert the security properties of the TOE. |
| **O.UPDATE_VERIFICATION** - ***The TOE shall provide mechanisms to verify the authenticity of software updates***. | | |
| FCS_COP.1(b) | Selection | This SFR defines the digital signature service(s) used to verify the authenticity TOE updates. |
| FCS_COP.1(c) | Selection | This SFR defines the hashing algorithm(s) used to verify the integrity of TOE updates. |
| FPT_TUD_EXT.1 | Satisfies | This SFR defines the ability of the TOE to be updated and the method(s) by which the updates are known to be trusted. |
| **O.USER_AUTHORIZATION** - ***The TOE shall perform authorization of Users in accordance with security policies***. | | |
| FDP_ACC.1 | Supports | This SFR enforces User Access Control SFP on subjects, objects, and operations in accordance with user authorization. |
| FDP_ACF.1 | Supports | This SFR enforces the User Access Control SFP to objects based on attributes in accordance with user authorization. |
| FIA_ATD.1 | Supports | This SFR defines the attributes that are associated with Users that can be used to define their authorizations. |
| FMT_MSA.1 | Satisfies | This SFR defines the authorizations that are required to access data that is protected by the TSF. |
| FMT_MSA.3 | Satisfies | This SFR defines the default security posture for enforcement of the access control policy that governs access to data that is protected by the TSF. |
| FMT_SMF.1 | Satisfies | This SFR defines the management functions provided by the TOE that can be used to define User authorizations. |
| FMT_SMR.1 | Satisfies | This SFR defines administrative roles that can be used to define authorizations to groups of Users. |
| **O.USER_I&A** - ***The TOE shall perform identification and authentication of Users for operations that require access control, User authorization, or Administrator roles***. | | |
| FIA_AFL.1 | Supports | This SFR protects the authentication function by limiting the number of unauthorized authentication attempts that can be made, thereby reducing the likelihood of impersonation. |

| Objective / SFR | Relationship | Rationale |
|---|---|---|
| FIA_PMG_EXT.1 | Satisfies | This SFR protects the authentication function by providing for strong credentials that are difficult to guess or derive. |
| FIA_UAU.1 | Satisfies | This SFR defines the TOE functions that can be performed without authentication and the functions that require authentication for use. |
| FIA_UAU.7 | Satisfies | This SFR protects the authentication function by hiding the authentication credential as it is being input. |
| FIA_UID.1 | Satisfies | This SFR defines the TOE functions that can be performed without identification and the functions that require identification for use. |
| FIA_USB.1 | Satisfies | This requirement provides assurance that an identified user is associated with attributes that govern their authorizations to the TSF upon successful authentication to the TOE. |
| FTA_SSL.3 | Satisfies | This SFR helps prevent User or Administrator impersonation by terminating unattended sessions. |