# Security Target

# API Technologies ION SA5600 v2.0.0 with PRIISMS v3.0

Document Version 1.19

June 14, 2016

Prepared For:

API Technologies
120 Corporate Boulevard
South Plainfield, NJ 07080
www.apitech.com

Prepared By:

Apex Assurance Group, LLC
530 Lytton Avenue, Ste. 200
Palo Alto, CA 94301
www.apexassurance.com

## Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), API Technologies ION SA5600 v2.0.0 with PRIISMS v3.0. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

## Revision History

| Revision | Date | Description |
|---|---|---|
| 1.0 | February 2, 2013 | Initial draft |
| 1.1 | February 18, 2013 | Updates to respond to evaluator comments |
| 1.2 | February 24, 2013 | Updates to address evaluator comments |
| 1.3 | February 28, 2013 | Removed reference to info flow control |
| 1.4 | March 19, 2013 | Hardware/Software TOE |
| 1.5 | March 25, 2013 | Address ORs |
| 1.6 | April 18, 2013 | Address ORs.  Add PRIISMS appliance |
| 1.7 | April 19, 2013 | Appended extended components definitions |
| 1.8 | May 30, 2013 | Respond to ORs |
| 1.9 | June 7, 2013 | Address June 7 ORs |
| 1.10 | June 12, 2013 | Corrections |
| 1.11 | June 28, 2013 | Response to certifier comments |
| 1.12 | October 9, 2013 | Response to certifier comments |
| 1.13 | October 18, 2013 | Address additional evaluator comments |
| 1.14 | October 28, 2013 | Remove NDPP conformance claim |
| 1.15 | October 28, 2013 | Added dependency rationale |
| 1.16 | May 13, 2014 | Address evaluator testing comments |
| 1.17 | May 22, 2014 | Address evaluator testing comments |
| 1.18 | May 22, 2016 | Updated version |
| 1.19 | June 14, 2016 | Addressed evaluator comments |

## Table of Contents

## List of Tables

## List of Figures

# 1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

## 1.1 ST Reference

| | |
|---|---|
| **ST Title** | Security Target: API Technologies ION SA5600 v2.0.0 with PRIISMS v3.0 |
| **ST Revision** | 1.19 |
| **ST Publication Date** | June 14, 2016 |
| **Author** | Apex Assurance Group, LLC |

## 1.2 TOE Reference

| | |
|---|---|
| **TOE Reference** | API Technologies ION SA5600 v2.0.0 with PRIISMS v3.0 |

## 1.3 Document Organization

This Security Target follows the following format:

| SECTION | TITLE | DESCRIPTION |
|---|---|---|
| 1 | Introduction | Provides an overview of the TOE  and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE |
| 2 | Conformance Claims | Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable |
| 3 | Security Problem Definition | Specifies the threats, assumptions and organizational security policies that affect the TOE |
| 4 | Security Objectives | Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats |
| 5 | Extended Components Definition | Describes extended components of the evaluation (if any) |
| 6 | Security Requirements | Contains the functional and assurance requirements for this TOE |
| 7 | TOE Summary Specification | Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements. |

**Table 1-1 – ST Organization and Section Descriptions**

## 1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets, i.e. [assignment_value(s)].

The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).

The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *italicized* text.

Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

When not embedded in a Security Functional Requirement, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

## 1.5 Document Terminology

The following table describes the acronyms used in this document:

| TERM | DEFINITION |
|---|---|
| CC | Common Criteria version 3.1 |
| CSP | Cryptographic security parameter |
| DES | Data Encryption Standard |
| DH | Diffie Hellman |
| EAL | Evaluation Assurance Level |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| FIPS | Federal Information Processing Standard |
| FIPS-PUB 140-2 | Federal Information Processing Standard Publication 140-2 |
| GUI | Graphical User Interface |
| HMAC | Keyed-Hash Message Authentication Code |
| HTTP | Hypertext Transfer Protocol |
| I&A | Identification and Authentication |
| IETF | Internet Engineering Task Force |

| TERM | DEFINITION |
|---|---|
| NDPP | Network Devices Protection Profile |
| NIST | National Institute of Standards and Technology |
| PP | Protection Profile |
| RNG | Random Number Generator |
| RSA | Rivest, Shamir, Adleman |
| SFR | Security Functional Requirement |
| SHA | Secure Hash Algorithm |
| ST | Security Target |
| TBD | To Be Determined |
| TOE | Target of Evaluation |

**Table 1-2 – Acronyms Used in Security Target**

## 1.6 TOE Overview

The TOE is API Technologies ION SA5600 v2.0.0 with PRIISMS v3.0 provide secure administrative access to virtually any device, using virtually any type of connectivity (e.g., IP, dial-up). ION appliances provide a highly-scalable, easily compatible platform for remote services delivery that satisfies service providers' need for access, monitoring and management, and enterprise companies' need for security. Built-in alarm management and filtering technology helps dramatically improve service levels.

The ION SA5600 v2.0.0 with PRIISMS v3.0 may also be referred to as the TOE in this document.

## 1.7 TOE Description

### 1.7.1 Overview

The TOE is composed of the following components:

- ION SA5600 appliance running ION SA5600 appliance firmware v2.0.0
- PRIISMS v3.0 software running on PRIISMS appliance hardware
- PRIISMS Routing Device running PRIISMS Routing Device firmware v2.0.0

**ION PRIISMS** (Proactive Remote Integrated Intelligent Secure Management Solution) is a central management system used to remotely access, manage, and monitor IT and voice equipment. PRIISMS is a tool for service providers, equipment vendors, and large IT organizations that must manage and centrally control technicians' access to hundreds or thousands of devices worldwide. PRIISMS is a hardware/software solution that contains the PRIISMS Routing Device and a software/user interface. When combined with ION's suite of Secure Appliances, PRIISMS offers a comprehensive remote services delivery and vendor access and control solution.

PRIISMS forms a secure and auditable gateway for all administrator channel access, ensuring protection of critical business data. PRIISMS serves as a single portal for administrative access by IT staff and third-party contractors, businesses can complement existing application security policies and address threats from supposedly trusted users with access to core business infrastructure.

Supporting this new application requires the **PRIISMS Routing Device** appliance, a new component of the PRIISMS application. This PRIISMS Routing Device is the concentration point for all Services. TLS is the communication channel from SA5600 secure appliance into the PRIISMS environment. The PRIISMS Routing Device enables a more powerful application proxy that supports multiple TCP/UDP ports, ION Networks has developed a second generation Application Proxy Layer (APL2). With APL2, PRIISMS with the PRIISMS Routing Device can secure virtually any TCP/IP application (e.g., Web, FTP, VNC, RDP, or a proprietary GUI management application). This is accomplished using several security applications (e.g., Encryption, Strong Authentication, and Firewall technologies).

The ION **SA5600 Secure Appliance** is easily deployable and delivers next generation remote services, such as: patch management, proactive device monitoring, and VoIP Quality of Service (QoS) monitoring, while meeting enterprise customers' diverse security, compliance, and connectivity requirement. The ION SA5600 extends secure remote access to trusted vendors and IT staff without losing control or visibility. Its built-in audit trails, AES encryption, two-factor authentication, and individual user profiles/permissions help meet or exceed compliance requirements for most enterprise and government security standards.

ION Secure Appliances may be accessed from ION PRIISMS – a single signon, multi-factor authentication portal providing encrypted dial-up or secure IP tunnel connectivity from a local or remote workstation - connecting to a wide range of devices, delivering a scalable and auditable gateway for all administrative-class users.

### 1.7.2 Physical Boundary

The TOE is a combined hardware/software TOE and is defined as the ION SA5600 v2.0.0 with PRIISMS v3.0 and the PRIISMS Routing Device v2.0.0. The TOE and its deployed environment are shown below.

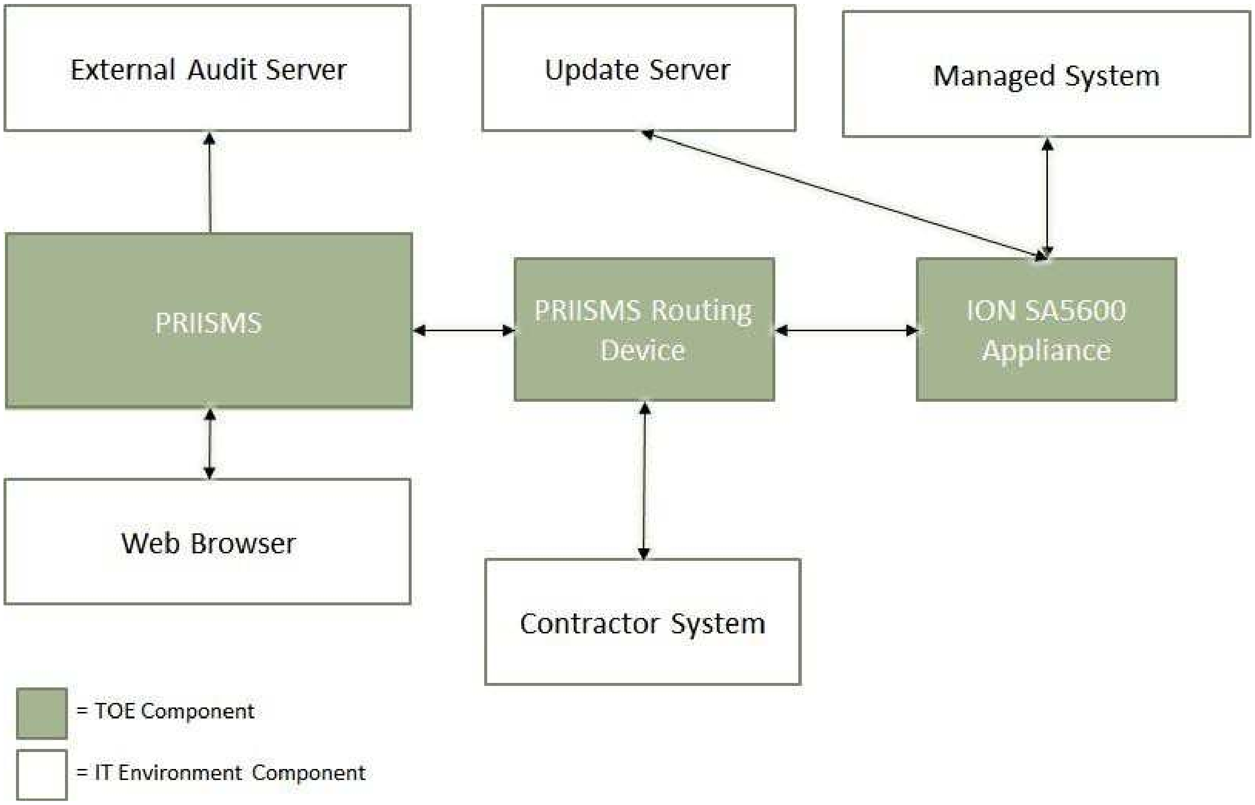


**Figure 1 –Deployed TOE**

The physical boundary is defined as the entire router chassis. In order to comply with the evaluated configuration, the following hardware and software components should be used:

| TOE COMPONENT | SOFTWARE REQUIREMENTS | HADWARE REQUIREMENTS |
|---|---|---|
| ION SA5600 appliance | SA5600 firmware v2.0.0-B07 | ION SA5600 appliance hardware part numbers:<br>• SA5610-IA<br>• SA5620-IA<br>• SA5630-IA |
| PRIISMS v3.0 | PRIISMS software v3.0.1 (B1619.5)<br>See Table 1-4 - Software Supplied by the PRIISMS System | PRIISMS Appliances part numbers:<br>• PR-5CS-V-IA2<br>• PR-10CS-V-IA2<br>• PR-15CS-V-IA2<br>• PR-25CS-V-IA2<br>• PR-50CS-V-IA2<br>• PR-100CS-V-IA2<br>• PR-200CS-V-IA2 |
| PRIISMS Routing Device v2.0 | PRIISMS Routing Device firmware v2.0.0-B08 | PRIISMS Routing Device hardware |

**Table 1-3 - TOE Components**

#### 1.7.2.1 *PRIISMS Platform*

The PRIISMS component of the TOE is a software application running on top of the PRIISMS appliance hardware. The PRIISMS software includes third-party software. The table below describes the software contained in the PRIISMS component.

| OPERATING SYSTEM | WEB SERVER | DATABASE | WEB BROWSER |
|---|---|---|---|
| Windows Server 2012 R2 (32-bit) | Internet Information Services (IIS) v8.0[1] | Microsoft SQL Server 2012 | Internet Explorer 6 or later for local administrator console access. |

**Table 1-4 - Software Supplied by the PRIISMS System**

PRIISMS implements stunnel for secure (TLS) communications with the external audit server.

### 1.7.3 Operational Environment Requirements

#### 1.7.3.1 *Audit Server*

An external audit server will be connected to the TOE using TLS. The audit server is part of the Operational Environment and will run on a general purpose computer. The only requirement is that the system upon which the audit server will run must support stunnel usingTLS.

| HARDWARE | OPERATING SYSTEM | SOFTWARE |
|---|---|---|
| General-Purpose Computer | Operating systems that support syslog server. | • Syslog Server<br>• stunnel |

**Table 1-5 – Operational Environment Requirements for Audit Server**

#### 1.7.3.2 *Web Browser*

A web browser is sued for remote administrator access to the management console functionality.

| HARDWARE | OPERATING SYSTEM | SOFTWARE |
|---|---|---|
| General-Purpose Computer | Operating systems that support web browser. | Internet Explorer 6 or later |

**Table 1-6 - Operational Environment Requirements for Web Browser**

#### 1.7.3.3 *Managed System and Contractor Systems*

Contractor Systems are external systems that want to gain access to Managed Systems. Managed Systems are corporate network elements (a router, server, voice switch, data processing equipment) that are protected by ION security appliances.

[1] Required for HTTPS/TLS support

Contractor Systems can gain access to Managed Systems by physically connecting through the PRIISMS Routing Device to enable contractor users to access managed system applications with complex GUI clients such as RDP, Web or proprietary fat clients. Contractor Systems can also access through the ION SA5600 appliance's Ethernet or serial interfaces.

#### 1.7.3.4 *Update Server*

The update server in the Operational Environment provides software updates to the TOE. The updates are protected using SHA-256 and 512 for cryptographic hashing to verify the updates.

### 1.7.4 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following table:

| TSF | DESCRIPTION |
|---|---|
| Security Audit | The TOE's auditable events are stored in the system log files, and can be sent to an external log server over HTTPS/TLS. Auditable events include start-up of the audit functions, authentication events, service requests, as well as the events listed in Table 6-2 - Audit Events and Details. Audit records include the date and time, event category, event type, username, and the outcome of the event (success or failure). |
| Cryptographic Support | The TOE includes a baseline cryptographic module that provides confidentiality and integrity services for authentication and for protecting communications with adjacent systems. The TOE uses TLS and HTTPS/TLS for secure communications with the external log server and remote administrator consoles. |
| User Data Protection | The TOE will provide residual information protection by ensuring that user data is not persistent when memory resources are released. |
| Identification and Authentication | The TOE requires users to provide unique identification and authentication data before any administrative access to the system is granted. |
| Security Management | The TOE provides an authorized Administrator role that is responsible for:<br>• the configuration and maintenance of cryptographic elements related to the establishment of secure connections to and from the evaluated product<br>• the regular review of all audit data;<br>• all administrative tasks (e.g., creating the security policy).<br>The TOE is managed through a web-based GUI. |
| Protection of the TSF | The TOE provides protection mechanisms for its security functions. One of the protection mechanisms is to protect TSF data (e.g. cryptographic keys, administrator passwords). Another protection mechanism is to ensure the integrity of any software/firmware updates are can be verified prior to installation. The TOE provides for both cryptographic and non-cryptographic self-tests, and is capable of automated recovery from failure states. Also, reliable timestamps are made available by the TOE. |
| TOE Access | The TOE can be configured to terminate interactive user sessions, and to present an access banner with warning messages prior to authentication. |

| TSF | DESCRIPTION |
|---|---|
| Trusted Path/Channel | The TOE creates trusted channels between itself and remote trusted authorized audit server that protect the confidentiality and integrity of communications using TLS.<br>The TOE creates trusted paths between itself and remote administrators and users that protect the confidentiality and integrity of communications using HTTPS/TLS. |

**Table 1-7 – Logical Boundary Descriptions**

### 1.7.5 Excluded Functionality

The following functions are excluded from this evaluation:

- Firewall technologies
- Proactive device monitoring
- VoIP QOS monitoring
- Built-in audit trails[3]
- Two-factor authentication. [4]
- Single signon / multi-factor authentication
- FTP service[5]

### 1.7.6 TOE Product Documentation

The TOE includes the following product documentation:

- *ION Security Appliance Administrator Guide*
- *ION PRIISMS Administrator Guide*
- *ION PRIISMS & ION SA5600 Secure Appliance Military Unique Deployment Guide*

[3] Audit logs that are in scope are the server logs and syslogs. Out of scope are the audit trails for managed system activity.

[4] Out of scope authentication relate to two-factor, single signon and multi-factor authentication used by managed systems. In scope, is password authentication for administrator login.

[5] In the evaluated configuration, FTP shall be disabled.

# 2 Conformance Claims

## 2.1 CC Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 4 (September 2012) Part 2 extended and Part 3 conformant.

## 2.2 Protection Profile Conformance Claim

The TOE does not claim conformance to any protection profiles but the ST is based on requirements from:

- Security Requirements for Network Devices, Version 1.1, 08 June 2012 (NDPP)

References are made to the NDPP throughout this document where statements have been leveraged from the NDPP.

## 2.3 Package Claim

The TOE claims conformance to:

- Evaluation Assurance Level 1
- No other assurance or functional packages.

# 3 Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
- Any organizational security policy statements or rules with which the TOE must comply
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

## 3.1 Threats

The following are threats identified for the TOE and the IT Systems the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all threats is unsophisticated.

The TOE and Operational Environment address the following threats:

| THREAT | DESCRIPTION |
|---|---|
| T.ADMIN_ERROR | An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms. |
| T.TSF_FAILURE | Security mechanisms of the TOE may fail, leading to a compromise of the TSF. |
| T.UNDETECTED_ACTIONS | Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated. |
| T.UNAUTHORIZED_ACCESS | A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data. |
| T.UNAUTHORIZED_UPDATE | A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE. |
| T.USER_DATA_REUSE | User data may be inadvertently sent to a destination not intended by the original sender. |

**Table 3-1 – Threats addressed by the TOE**

## 3.2 Organizational Security Policies

The TOE meets the following organizational security policies:

| POLICY | DESCRIPTION |
|---|---|
| P.ACCESS_BANNER | The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE. |

**Table 3-2 – Organizational Security Policies**

## 3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

| ASSUMPTION | DESCRIPTION |
|---|---|
| A.NO_GENERAL_PURPOSE | It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. Access to the underlying operating system (e.g., Windows) functions and general purpose applications are not made available to users through the TOE TSFI. |
| A.PHYSICAL | Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment. |
| A.TRUSTED_ADMIN | TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner. |

**Table 3-3 – Assumptions**

# 4 Security Objectives

## 4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

| OBJECTIVES | DESCRIPTION |
|---|---|
| O.PROTECTED_COMMUNICATIONS | The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities. |
| O.VERIFIABLE_UPDATES | The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source. |
| O.SYSTEM_MONITORING | The TOE will provide the capability to generate audit data and send those data to an external IT entity. |
| O.DISPLAY_BANNER | The TOE will display an advisory warning regarding use of the TOE. |
| O.TOE_ADMINISTRATION | The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators. |
| O.RESIDUAL_INFORMATION_CLEARING | The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated. |
| O.SESSION_LOCK | The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked. |
| O.TSF_SELF_TEST | The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly. |

**Table 4-1 – TOE Security Objectives**

## 4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

| OBJECTIVE | DESCRIPTION |
|---|---|
| OE.NO_GENERAL_PURPOSE | There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. |
| OE.PHYSICAL | Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment. |
| OE.TRUSTED_ADMIN | TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner. |

**Table 4-2 – Operational Environment Security Objectives**

## 4.3 Security Objectives Rationale

This Security Objectives for the TOE and the Operational Environment, Assumptions, Organizational Security Policies and Threats are mapped in the table below.

| THREAT/ASSUMPTION/POLICY | O.PROTECTED_COMMUNICATIONS | O.VERIFIABLE_UPDATES | O.SYSTEM_MONITORING | O.DISPLAY_BANNER | O.TOE_ADMINISTRATION | O.RESIDUAL_INFORMATION_CLEARING | O.SESSION_LOCK | O.TSF_SELF_TEST | OE.NO_GENERAL_PURPOSE | OE.PHYSICAL | OE.TRUSTED_ADMIN |
|---|---|---|---|---|---|---|---|---|---|---|---|
| T.ADMIN_ERROR | | | | | | | | | | | X |
| T.TSF_FAILURE | | | | | | | | X | | | |
| T.UNDETECTED_ACTIONS | | | X | | | | | | | | |
| T.UNAUTHORIZED_ACCESS | X | | | | X | | X | | | | |
| T.UNAUTHORIZED_UPDATE | | X | | | | | | | | | |
| T.USER_DATA_REUSE | X | | | | | X | | X | | | |
| P.ACCESS_BANNER | | | | X | | | | | | | |
| A.NO_GENERAL_PURPOSE | | | | | | | | | X | | |
| A.PHYSICAL | | | | | | | | | | X | |
| A.TRUSTED_ADMIN | | | | | | | | | | | X |

# 5 Extended Components Definition

The following extended components are used in this ST.

- FAU_STG_EXT.1
- FCS_CKM_EXT.4
- FCS_RBG_EXT.1
- FCS_TLS_EXT.1
- FCS_HTTPS_EXT.1
- FIA_PMG_EXT.1
- FIA_UIA_EXT.1
- FIA_UAU_EXT.5
- FPT_SKP_EXT.1
- FPT_APW_EXT.1
- FPT_TUD_EXT.1
- FPT_TST_EXT.1
- FTA_SSL_EXT.1

## 5.1 Extended Components Definition

Table 5-1 - Extended Components identifies the extended components which are incorporated into this ST.

| Component | Title |
|---|---|
| FAU_STG_EXT.1 | External Audit Trail Storage |
| FCS_CKM_EXT.4 | Cryptographic Key Zeroization |
| FCS_RBG_EXT.1 | Cryptographic Operation (Random Bit Generation) |
| FCS_TLS_EXT.1 | Explicit: TLS |
| FCS_HTTPS_EXT.1 | Explicit: HTTPS |
| FIA_PMG_EXT.1 | Password Management |
| FIA_UIA_EXT.1 | User Identification and Authentication |
| FIA_UAU_EXT.2 | Password-based Authentication Mechanism |
| FPT_SKP_EXT.1 | Protection of TSF Data (for reading of passwords) |
| FPT_APW_EXT.1 | Protection of Administrator Passwords |

| Component | Title |
|---|---|
| FPT_TUD_EXT.1 | Trusted Update |
| FPT_TST_EXT.1 | TSF Testing |
| FTA_SSL_EXT.1 | TSF-initiated Session Locking |

**Table 5-1 - Extended Components**

### 5.1.1 External Audit Trail Storage (FAU_STG_EXT.1)

**Family Behavior**

This family defines the requirements for external audit trail storage functionality. This component is added to the existing family FAU_STG.

**Component Leveling**

FAU_STG_EXT
1

FAU_STG_EXT.1 External Audit Trail Storage

**Management: FAU_STG_EXT.1**

There are no management functions foreseen.

**Audit: FAU_STG_EXT.1**

There are no auditable events foreseen.

**FAU_STG_EXT.1 External Audit Trail Storage**

Hierarchical to: No other components

Dependencies: FTP_ITC_1 Inter-TSF trusted channel

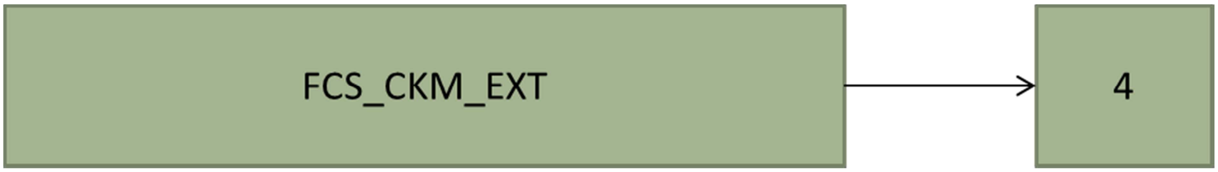
FAU_STG_EXT.1.1 The TSF shall be able to [*selection: transmit the generated audit data to an external IT entity, receive and store audit data from an external IT entity*] using a trusted channel implementing the [*selection: IPsec, SSH, TLS, TLS/HTTPS*] protocol.

### 5.1.2 Cryptographic Key Zeroization (FCS_CKM_EXT.4)

**Family Behavior**

This family defines the requirements for cryptographic key zeroization. This component is added to the existing family FCS_CKM.

**Component Leveling**



FCS_CKM_EXT.4 Cryptographic Key Zeroization

**Management: FCS_CKM_EXT.4**

There are no management functions foreseen.

**Audit: FCS_CKM_EXT.4**

There are no auditable events foreseen.

**FCS_CKM_EXT.4 Cryptographic Key Zeroization**

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 Cryptographic key generation

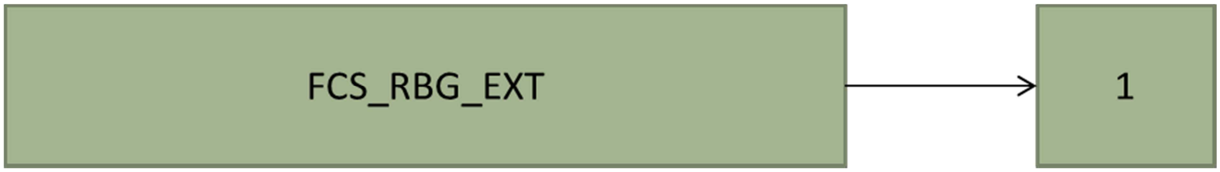
FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

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

**Family Behavior**

This family defines the requirements for cryptographic random bit generation. This family is added to the existing class FCS.

**Component Leveling**



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

**Management: FCS_RBG_EXT.1**

There are no management functions foreseen.

**Audit: FCS_RBG_EXT.1**

There are no auditable events foreseen.

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

Hierarchical to: No other components

Dependencies: No dependencies

FCS_RBG_EXT.1.1 FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with [*selection, choose one of: NIST Special Publication 800-90 using* [*selection: Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES), Dual_EC_DRBG (any)]; FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using AES*] seeded by an entropy source that accumulated entropy from [selection, one or both of: a software-based noise source; a TSF-hardware-based noise source].

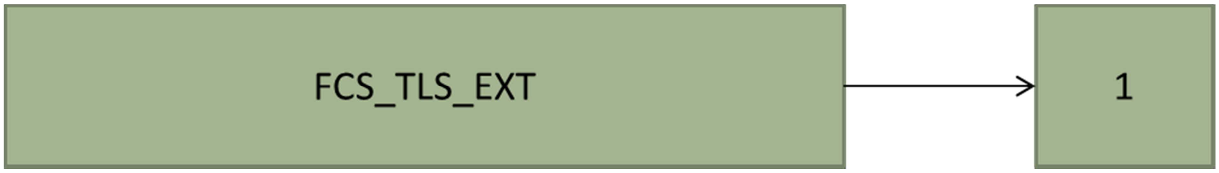
FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of [*selection, choose one of: 128 bits, 256 bits*] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

### 5.1.4 Explicit: TLS (FCS_TLS_EXT.1)

**Family Behavior**

This family defines the requirements for TLS implementation. This family is added to the existing class FCS.

**Component Leveling**



FCS_TLS_EXT.1 Explicit: TLS

**Management: FCS_TLS_EXT.1**

There are no management functions foreseen.

**Audit: FCS_TLS_EXT.1**

The following events should be auditable:

- Failure to establish a TLS Session with the reason for failure.
- Establishment/Termination of a TLS session with the non-TOE endpoint of connection (IP address) for both successes and failures.

**FCS_TLS_EXT.1 Explicit: TLS** Hierarchical to: No

other components Dependencies: FCS_COP.1

Cryptographic Operation

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

IIS Ciphersuites:

[assignment: list of ciphersuites];

OpenVPN Ciphersuites:

[assignment: list of ciphersuites];

*Stunnel Ciphersuites:*

[assignment: list of ciphersuites].

## 5.1.5 Explicit: HTTPS (FCS_HTTPS_EXT.1)

**Family Behavior**

This family defines the requirements for HTTPS implementation. This family is added to the existing class FCS.

**Component Leveling**

FCS_HTTPS_EXT
1

FCS_HTTPS_EXT.1 Explicit: HTTPS

**Management: FCS_HTTPS_EXT.1**

There are no management functions foreseen.

**Audit: FCS_HTTPS_EXT.1**

The following events should be auditable:

- Failure to establish a HTTPS Session with the reason for failure.
- Establishment/Termination of a HTTPS session with the non-TOE endpoint of connection (IP address) for both successes and failures.

**FCS_HTTPS_EXT.1 Explicit: HTTPS**

Hierarchical to: No other components

Dependencies: FCS_TLS_EXT.1 Explicit: TLS

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

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.The TSF shall implement the HTTPS protocol that complies with RFC 2818.

### 5.1.6 Password Management (FIA_PMG_EXT.1)

**Family Behavior**

This family defines the requirements for password management. This family is added to the existing class FIA.

**Component Leveling**

FIA_PMG_EXT
1

FIA_PMG_EXT.1 Password Management

**Management: FIA_PMG_EXT.1**

There are no management functions foreseen.

**Audit: FIA_PMG_EXT.1**

There are no auditable events foreseen.

**FIA_PMG_EXT.1 Password Management**

Hierarchical to: No other components

Dependencies: FIA_UAU_EXT.2 Password-based Authentication Mechanism

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

1. 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];

2. Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater;.

### 5.1.7 User Identification and Authentication (FIA_UIA_EXT.1)

**Family Behavior**

This family defines the requirements for user identification and authentication. This family is added to the existing class FIA.

**Component Leveling**

FIA_UIA_EXT
1

FIA_UAU_EXT.1 User Identification and Authentication

**Management: FIA_UAU_EXT.1**

There are no management functions foreseen.

**Audit: FIA_UAU_EXT.1**

There are no auditable events foreseen.

**FIA_UAU_EXT.1 User Identification and Authentication**

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;

- [*selection: no other actions,* [assignment: list of services, actions performed by the TSF in response to non-TOE requests.]]

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

### 5.1.8 Password-based Authentication Mechanism (FIA_UAU_EXT.2)

**Family Behavior**

This family defines the requirements for password-based authentication mechanism. This family is added to the existing class FIA.

**Component Leveling**

FIA_UAU_EXT
2

FIA_UAU_EXT.2 Password-based Authentication Mechanism

**Management: FIA_UAU_EXT.2**

There are no management functions foreseen.

**Audit: FIA_UAU_EXT.2**

There are no auditable events foreseen.

**FIA_UAU_EXT.2 Password-based Authentication Mechanism**

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, *[selection:* [assignment: other authentication mechanism(s)], *none*] to perform administrative user authentication.

### 5.1.9 Protection of TSF Data (for reading of passwords) (FPT_SKP_EXT.1)

**Family Behavior**

This family defines the requirements for protection of reading of passwords. This family is added to the existing class FPT.

**Component Leveling**

FPT_SKP_EXT
1

FPT_SKP_EXT.1 Protection of TSF Data (for reading of passwords)

**Management: FPT_SKP_EXT.1**

There are no management functions foreseen.

**Audit: FPT_SKP_EXT.1**

There are no auditable events foreseen.

**FPT_SKP_EXT.1 Protection of TSF Data (for reading of passwords)**

Hierarchical to: No other components

Dependencies: No dependencies

FPT_SKP_EXT.1.1 The TSF shall prevent reading of passwords.

### 5.1.10 Protection of Administrator Passwords (FPT_APW_EXT.1)

**Family Behavior**

This family defines the requirements for the protection of administrator passwords. This family is added to the existing class FPT.

**Component Leveling**

FPT_APW_EXT
1

FPT_APW_EXT.1 Protection of Administrator Passwords

**Management: FPT_APW_EXT.1**

There are no management functions foreseen.

**Audit: FPT_APW_EXT.1**

There are no auditable events foreseen.

**FPT_APW_EXT.1 Protection of Administrator Passwords**

Hierarchical to: No other components

Dependencies: No dependencies

FPT_APW_EXT.1.1 The TSF shall store passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext passwords.

### 5.1.11 Trusted Update (FPT_TUD_EXT.1)

**Family Behavior**

This family defines the requirements for trusted updates. This family is added to the existing class FPT.

**Component Leveling**

FPT_TUD_EXT
1

FPT_TUD_EXT.1 Trusted Update

**Management: FPT_TUD_EXT.1**

There are no management functions foreseen.

**Audit: FPT_TUD_EXT.1**

There are no auditable events foreseen.

**FPT_TUD_EXT.1 Trusted Update**

Hierarchical to: No other components

Dependencies: No dependencies

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

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

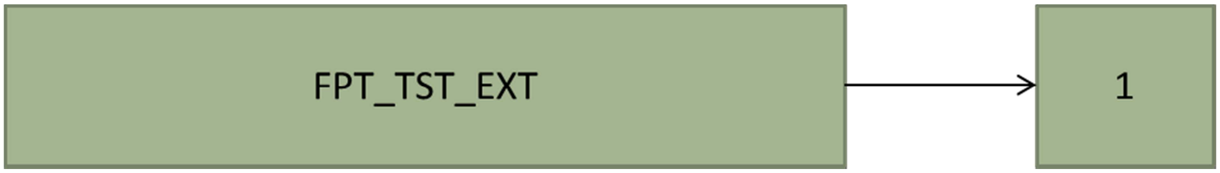
FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a [*selection: digital signature mechanism, published hash*] prior to installing those updates.

### 5.1.12 TSF Testing (FPT_TST_EXT.1)

**Family Behavior**

This family defines the requirements for TSF testing. This family is added to the existing class FPT.

**Component Leveling**



FPT_TST_EXT.1 TSF Testing

**Management: FPT_TST_EXT.1**

There are no management functions foreseen.

**Audit: FPT_TST_EXT.1**

There are no auditable events foreseen.

**FPT_TST_EXT.1 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 (on power on) to demonstrate the correct operation of the TSF.

### 5.1.13 TSF-initiated Session Locking (FTA_SSL_EXT.1)

**Family Behavior**

This family defines the requirements for TSF-initiated session locking. This family is added to the existing class FTA.

**Component Leveling**

FTA_SSL_EXT
1

FTA_SSL_EXT.1 TSF-initiated Session Locking

**Management: FTA_SSL_EXT.1**

There are no management functions foreseen.

**Audit: FTA_SSL_EXT.1**

There are no auditable events foreseen.

**FTA_SSL_EXT.1 TSF-initiated Session Locking**

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [*selection:*

- *lock the session - disable any activity of the user's data access/display devices other than unlocking the session, and requiring that the administrator re-authenticate to the TSF prior to unlocking the session;*
- *terminate the session*]

after a Security Administrator-specified time period of inactivity.

## 5.2 Rationale for Extended Components

This ST includes these extended components to reflect the security capabilities of the TOE..

# 6 Security Requirements

The security requirements that are levied on the TOE and the Operational environment are specified in this section of the ST.

## 6.1 Security Functional Requirements

The functional security requirements for this Security Target are summarized in the following table:

| CLASS HEADING | CLASS_FAMILY | DESCRIPTION |
|---|---|---|
| Security Audit | FAU_GEN.1 | Audit Data Generation |
| | FAU_GEN.2 | User Identity Association |
| | FAU_STG_EXT.1 | External Audit Trail Storage |
| Cryptographic Support | FCS_CKM.1 | Cryptographic Key Generation (for asymmetric keys) |
| | FCS_CKM_EXT.4 | Cryptographic Key Zeroization |
| | FCS_COP.1(1) | Cryptographic Operation (for data encryption/decryption) |
| | FCS_COP.1(2) | Cryptographic Operation (for cryptographic signature) |
| | FCS_COP.1(3) | Cryptographic Operation (for cryptographic hashing) |
| | FCS_COP.1(4) | Cryptographic Operation (for keyed-hash message authentication) |
| | FCS_RBG_EXT.1 | Extended: Cryptographic Operation (Random Bit Generation) FCS_TLS_EXT.1 |
| | | Explicit TLS Requirements |
| | FCS_HTTPS_EXT.1 | Explicit HTTPS Requirements |
| User Data Protection | FDP_RIP.2 | Full residual information protection |
| Identification and Authentication | FIA_PMG_EXT.1 | User Identification and Authentication |
| | FIA_UIA_EXT.1 | Extended: Password-based Authentication Mechanism |
| | FIA_UAU_EXT.2 | Extended: Password-based Authentication Mechanism |
| | FIA_UAU.7 | Protected Authentication Feedback |
| Security Management | FMT_MTD.1 | Management of TSF Data (for general TSF data) |
| | FMT_SMF.1 | Specification of Management Functions |
| | FMT_SMR.2 | Security Roles |
| Protection of the TSF | FPT_ITT.1 | Basic Internal TSF Data Transfer Protection |
| | FPT_SKP_EXT.1 | Extended: Protection of TSF Data (for reading of passwords) |
| | FPT_APW_EXT.1.1 | Extended: Protection of Administrator Passwords |
| | FPT_STM.1 | Reliable Time Stamps |
| | FPT_TUD_EXT.1 | Extended: Trusted Update |
| | FPT_TST_EXT.1 | TSF Testing |
| TOE Access | FTA_ SSL_EXT.1 | TSF-initiated session locking |
| | FTA_SSL.3 | TSF-initiated termination |
| | FTA_SSL.4 | User-initiated termination |
| | FTA_TAB.1 | Default TOE access banners |

| CLASS HEADING | CLASS_FAMILY | DESCRIPTION |
|---|---|---|
| Trusted Path/Channels | FTP_ITC.1 | Inter-TSF trusted channel |
| | FTP_TRP.1 | Trusted path |

**Table 6-1 – TOE Security Functional Requirements**

## 6.1.1 Security Audit (FAU)

### 6.1.1.1 *FAU_GEN.1 Audit Data Generation*

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

- Start-up of the audit functions;
- All auditable events for the *not specified* level of audit; and
- *All Administrative actions*;
- *[Specifically defined auditable events listed in Table 6-2 - Audit Events and Details*].

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

- Date and time of the event, type of event, subject identity, and the outcome [success or failure] of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three of Table 6-2 - Audit Events and Details].

| REQUIREMENT | AUDITABLE EVENTS | ADDITIONAL DETAILS |
|---|---|---|
| FAU_GEN.1 | None. | |
| FAU_GEN.2 | None. | |
| FAU_STG_EXT.1 | None. | |
| FAU_STG_EXT.3 | None. | |
| FCS_CKM.1 | None. | |
| FCS_CKM_EXT.4 | None. | |
| FCS_COP.1(1) | None. | |
| FCS_COP.1(2) | None. | |
| FCS_COP.1(3) | None. | |
| FCS_COP.1(4) | None. | |
| FCS_RBG_EXT.1 | None. | |
| FCS_TLS_EXT.1 | Failure to establish a TLS Session.<br>Establishment/Termination of a TLS session. | Reason for failure.<br>Non-TOE endpoint of connection (IP address)<br>for both successes and failures. |

| REQUIREMENT | AUDITABLE EVENTS | ADDITIONAL DETAILS |
|---|---|---|
| FCS_HTTPS_EXT.1 | Failure to establish a HTTPS Session.<br>Establishment/Termination of a HTTPS session. | Reason for failure.<br>Non-TOE endpoint of connection (IP address) for both successes and failures. |
| FDP_RIP.2 | None. | |
| FIA_PMG_EXT.1 | None. | |
| FIA_UIA_EXT.1 | All use of the identification and authentication mechanism. | Provided user identity, origin of the attempt (e.g., IP address). |
| FIA_UAU_EXT.2 | All use of the authentication mechanism | Origin of the attempt (e.g., IP address). |
| FIA_UAU.7 | None. | |
| FMT_MTD.1 | None. | |
| FMT_SMF.1 | None. | |
| FMT_SMR.2 | None. | |
| FPT_SKP_EXT.1 | None. | |
| FPT_APW_EXT.1 | None. | |
| FPT_ITT.1 | None. | |
| FPT_STM.1 | Changes to the time. | The old and new values for the time.<br>Origin of the attempt (e.g., IP address). |
| FPT_TUD_EXT.1 | Initiation of update. | No additional information. |
| FPT_TST_EXT.1 | None | |
| FTA_SSL_EXT.1 | Any attempts at unlocking of an interactive session. | No additional information |
| FTA_SSL.3 | The termination of a remote session by the session locking mechanism. | No additional information. |
| FTA_SSL.4 | The termination of an interactive session. | No additional information. |
| FTA_TAB.1 | None. | |
| FTP_ITC.1 | Initiation of the trusted channel.<br>Termination of the trusted channel.<br>Failure of the trusted channel functions. | Identification of the initiator and target of failed trusted channels establishment attempt. |
| FTP_TRP.1 | Initiation of the trusted channel.<br>Termination of the trusted channel.<br>Failures of the trusted path functions. | Identification of the claimed user identity. |

**Table 6-2 - Audit Events and Details**

#### 6.1.1.2 *FAU_GEN.2 User Identity Association*

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_STG_EXT.1 External Audit Trail Storage*

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 implementing the *TLS* protocol.

### 6.1.2 Cryptographic Support (FCS)

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

FCS_CKM.1.1 **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 Cryptographic Key Zeroization*

FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

#### 6.1.2.3 *FCS_COP.1(1) Cryptographic Operation (for data encryption/decryption)*

FCS_COP.1.1(1) **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, 256-bits, and [*no other key sizes*]] that meets the following:

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

#### 6.1.2.4 *FCS_COP.1(2) Cryptographic Operation (for cryptographic signature)*

FCS_COP.1.1(2) **Refinement:** The TSF shall perform **cryptographic signature services** in accordance with a [

*RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater*]

that meets the following:

RSA Digital Signature Algorithm

- FIPS PUB 186-2, "Digital Signature Standard"

### 6.1.2.5 FCS_COP.1(3) Cryptographic Operation (for cryptographic hashing)

FCS_COP.1.1(3) **Refinement:** The TSF shall perform [cryptographic hashing services] in accordance with a specified cryptographic algorithm [SHA-256, *SHA-512*] and message digest sizes 256, *512* bits that meet the following: FIPS Pub 180-3, "Secure Hash Standard."

### 6.1.2.6 FCS_COP.1(4) Cryptographic Operation (for keyed-hash message authentication)

FCS_COP.1.1(4) **Refinement:** The TSF shall perform [keyed-hash message authentication] in accordance with a specified cryptographic algorithm HMAC-[ *SHA-1, SHA-256*], key size [160, 256 bits], and message digest sizes [*160, 256*] bits that meet the following: FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard."

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

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with *NIST Special Publication 800-90 using* [*HMAC_DRBG (SHA-256)]; FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using AES* seeded by an entropy source that accumulated entropy from [*a software-based noise source*].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of [*256 bits*] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

### 6.1.2.8 FCS_TLS_EXT.1 Explicit: TLS

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

IIS Ciphersuites: [

- TLSv1_ECDHE-RSA-AES256-SHA
- TLSv1_RSA_AES256-SHA
- TLSv1_RSA_DES-CBC3-SHA
- TLSv1_ECDHE-RSA-AES128-SHA
- TLSv1_RSA_AES128-SHA
- TLS1.1_ECDHE-RSA-AES256-SHA

- TLS1.1_RSA_AES256-SHA
- TLS1.1_RSA_DES-CBC3-SHA
- TLS1.1_ECDHE-RSA-AES128-SHA
- TLS1.1_RSA_AES128-SHA];

OpenVPN Ciphersuites: [

- DHE-RSA-AES256-SHA];

stunnel Ciphersuites:[

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES256-SHA384
- DHE-DSS-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- DHE-DSS-AES256-SHA256
- ECDH-RSA-AES256-GCM-SHA384
- ECDH-ECDSA-AES256-GCM-SHA384
- ECDH-RSA-AES256-SHA384
- ECDH-ECDSA-AES256-SHA384
- AES256-GCM-SHA384
- AES256-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-ECDSA-AES128-SHA256

- DHE-DSS-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256
- DHE-DSS-AES128-SHA256
- ECDH-RSA-AES128-GCM-SHA256
- ECDH-ECDSA-AES128-GCM-SHA256
- ECDH-RSA-AES128-SHA256
- ECDH-ECDSA-AES128-SHA256
- AES128-GCM-SHA256
- AES128-SHA256].

#### 6.1.2.9 *FCS_HTTPS_EXT.1 Explicit: HTTPS*

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

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

### 6.1.3 User Data Protection (FDP)

#### 6.1.3.1 *FDP_RIP.2 Full Residual Information Protection*

FDP_RIP.2.1 FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [*deallocation of the resource from*] all objects.

### 6.1.4 Identification and Authentication (FIA)

#### 6.1.4.1 *FIA_PMG_EXT.1 Password Management*

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

1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [*that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")"*]; [no other characters]];

2. Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater;

#### 6.1.4.2 *FIA_UIA_EXT.1 User Identification and Authentication*

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

Display the warning banner in accordance with FTA_TAB.1;

*no other actions.*

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

#### 6.1.4.3 *FIA_UAU_EXT.2 Extended: Password-based Authentication Mechanism*

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, *none* to perform administrative user authentication.

#### 6.1.4.4 *FIA_UAU.7 Protected Authentication Feedback*

FIA_UAU.7.1 The TSF shall provide only obscured feedback to the administrative user while the authentication is in progress at the local console.

### 6.1.5 Security Management (FMT)

#### 6.1.5.1 *FMT_MTD.1 Management of TSF Data (for general TSF data)*

FMT_MTD.1.1 The TSF shall restrict the ability to <u>manage</u> the TSF data to the Security Administrators.

#### 6.1.5.2 *FMT_SMF.1 Specification of Management Functions*

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

- Ability to administer the TOE locally and remotely;
- Ability to update the TOE, and to verify the updates using *published hash* capability prior to installing those updates;
- *No other capabilities*.

Application Note: Software updates are available for the Routing Device and SA appliance only.

#### 6.1.5.3 *FMT_SMR.2 Restrictions on Security Roles*

FMT_SMR.2.1 The TSF shall maintain the roles:

- Authorized Administrator.

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

FMT_SMR.2.3 The TSF shall ensure that the conditions

- Authorized Administrator role shall be able to administer the TOE locally;
- Authorized Administrator role shall be able to administer the TOE remotely;

are satisfied.

### 6.1.6 Protection of the TSF (FPT)

#### 6.1.6.1 *Extended: Protection of TSF Data (for reading of passwords)*

FPT_SKP_EXT.1.1 The TSF shall prevent reading of passwords.

Application Note: This applies to administrator passwords.

#### 6.1.6.2 *Extended: Protection of Administrator Passwords*

FPT_APW_EXT.1.1 The TSF shall store passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext passwords.

#### 6.1.6.3 *FPT_ITT.1 Basic Internal TSF Data Transfer Protection*

FPT_ITT.1.1 **Refinement:** The TSF shall protect TSF data from disclosure and detect its modification when it is transmitted between separate parts of the TOE through the use [TLS].

Application Note: The TOE uses OpenVPN which employs TLS to protect communications between TOE components.

#### 6.1.6.4 *FPT_STM.1 Reliable Time Stamps*

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

#### 6.1.6.5 *FPT_TUD_EXT.1 Extended: Trusted Update*

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

FPT_TUD_EXT.1.2 The TSF shall provide security 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 [*published hash*] prior to installing those updates.

Application Note: Software updates are only available on the Routing Device and SA appliance.

### 6.1.6.6 *FPT_TST_EXT.1: TSF Testing*

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

## 6.1.7 TOE Access

### 6.1.7.1 *FTA_SSL_EXT.1 TSF-initiated Session Locking*

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, *terminate the session* after a Security Administrator-specified time period of inactivity.

### 6.1.7.2 *FTA_SSL.3 TSF-initiated Termination*

FTA_SSL.3.1 **Refinement:** The TSF shall terminate a remote interactive session after a [**Security Administrator-configurable time interval of session inactivity**].

### 6.1.7.3 *FTA_SSL.4 User-initiated Termination*

FTA_SSL_EXT.4.1 The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

### 6.1.7.4 *FTA_TAB.1 Default TOE Access Banners*

FTA_TAB.1.1 **Refinement:** Before establishing an administrative user session the TSF shall display a **Security Administrator**-specified advisory **notice and consent** warning message regarding use of the TOE.

## 6.1.8 Trusted Path/Channel (FTP)

### 6.1.8.1 *FTP_ITC.1 Inter-TSF Trusted Channel*

FTP_ITC.1.1 **Refinement:** The TSF shall use **[*TLS/HTTPS*]** to provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [no other capabilities]]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data **from disclosure and detection of modification of the channel data.**

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

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [remote audit log storage].

#### 6.1.8.2 *FTP_TRP.1 Trusted Path*

FTP_TRP.1.1 **Refinement:** The TSF shall use ***TLS/HTTPS*** 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 **Refinement:** The TSF shall permit **remote administrators** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial administrator authentication and all remote administration actions.

## 6.2 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies.

## 6.3 Security Assurance Requirements

The Security Assurance Requirements for this evaluation are listed in Section 6.4.3 – Security Assurance Requirements.

## 6.4 Security Requirements Rationale

### 6.4.1 Sufficiency of Security Requirements

The following table presents a mapping of the rationale of TOE Security Requirements to Objectives.

| OBJECTIVE | SFR |
|---|---|

| OBJECTIVE | SFR |
|---|---|
| Protected Communications<br>O.PROTECTED_COMMUNICATIONS | FCS_CKM.1<br>FCS_CKM_EXT.4<br>FCS_COP.1(1)<br>FCS_COP.1(2)<br>FCS_COP.1(3)<br>FCS_COP.1(4)<br>FCS_RBG_EXT.1<br>FCS_TLS_EXT.1<br>FCS_HTTPS_EXT.1<br>FPY_ITT.1<br>FPT_PTD.1(2)<br>FPT_RPL.1<br>FTP_ITC.1<br>FTP_TRP.1 |
| Verifiable Updates<br>O.VERIFIABLE_UPDATES | FPT_TUD_EXT.1<br>FCS_COP.1(2)<br>FCS_COP.1(3) |
| System Monitoring<br>O.SYSTEM_MONITORING | FAU_GEN.1<br>FAU_GEN.2<br>FAU_STG_EXT.1<br>FPT_STM.1 |
| TOE Administration<br>O.TOE_ADMINISTRATION<br>O.DISPLAY_BANNER<br>O.SESSION_LOCK | FIA_UIA_EXT.1<br>FIA_PMG_EXT.1<br>FIA_UAU_EXT.2<br>FIA_UAU.7<br>FMT_MTD.1<br>FMT_SMF.1<br>FMT_SFR.1<br>FTA_SSL_EXT.1<br>FTA_SSL.3<br>FTA_SSL.4 |
| Residual Information Clearing<br>O.RESIDUAL_INFORMATION_CLEARING | FDP_RIP.2 |
| TSF Self Test<br>O.TSF_SELF_TEST | FPT_TST_EXT.1 |

**Table 6-3 – Rationale for TOE SFRs to Objectives**

### 6.4.2 Rationale for IT Security functional Requirement Dependencies

This section includes a table of all the security functional requirements and their dependencies and a rationale for any dependencies.

| Functional Component | Dependency | Rationale |
|---|---|---|
| FAU_GEN.1 | FPT_STM.1 | Satisfied |

| Functional Component | Dependency | Rationale |
|---|---|---|
| FAU_GEN.2 | FAU_GEN.1, FIA_UID.1 | FAU_GEN.1 is included. Dependency on FIA_UID.1 met by FIA_UIA_EXT.1, which includes that functionality. |
| FAU_STG_EXT.1 | FTP_ITC.1 | Satisfied |
| FCS_CKM.1 | FCS_CKM.2 or FCS_COP.1, FCS_CKM.4 | Satisfied through FCS_COP.1 and FCS_CKM_EXT.4 |
| FCS_CKM_EXT.4 | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 | Satisfied using FCS_CKM.1 |
| FCS_COP.1(1) | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4 | Satisfied using FCS_CKM.1 and FCS_CKM_EXT.4 (which provides equivalent functionality to FCS_CKM.4) |
| FCS_COP.1(2) | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4 | Satisfied using FCS_CKM.1 and FCS_CKM_EXT.4 (which provides equivalent functionality to FCS_CKM.4) |
| FCS_COP.1(3) | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4 | Satisfied using FCS_CKM.1 and FCS_CKM_EXT.4 (although dependencies are not relevant as this component relates to hashing only) |
| FCS_COP.1(4) | FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4 | Satisfied using FCS_CKM.1 and FCS_CKM_EXT.4 (which provides equivalent functionality to FCS_CKM.4) |
| FCS_RBG_EXT.1 | None. | Satisfied |
| FCS_HTTPS_EXT.1 | FCS_TLS_EXT.1 | Satisfied |
| FCS_SSH_EXT.1 | None. | Satisfied |
| FCS_TLS_EXT.1 | None. | Satisfied |
| FDP_RIP.2 | None. | Satisfied |
| FIA_PMG_EXT.1 | FIA_UAU_EXT.2 | Satisfied |
| FIA_UIA_EXT.1 | None. | Satisfied |
| FIA_UAU_EXT.2 | FIA_PMG_EXT.1 | Satisfied |
| FIA_UAU.7 | FIA_UAU.1 | Satisfied using FIA_UIA_EXT.1 |
| FMT_MTD.1 | FMT_SMR.2, FMT_SMF.1 | Satisfied |
| FMT_SMF.1 | None. | Satisfied |
| FMT_SMR.2 | FIA_UID.1 | Satisfied using FIA_UIA_EXT.1 |
| FPT_ITT.1 | None. | Satisfied |
| FPT_APW_EXT.1 | FIA_UAU_EXT.2 | Satisfied |
| FPT_SKP_EXT.1 | None. | Satisfied |
| FPT_STM.1 | None. | Satisfied |
| FPT_TUD_EXT.1 | None. | Satisfied |
| FPT_TST_EXT.1 | None. | Satisfied |
| FTA_SSL_EXT.1 | FIA_UIA_EXT.1 | Satisfied |

| Functional Component | Dependency | Rationale |
|---|---|---|
| FTA_SSL.3 | None. | Satisfied |
| FTA_SSL.4 | None. | Satisfied |
| FTA_TAB.1 | None. | Satisfied |
| FTP_ITC.1 | None. | Satisfied |
| FTP_TRP.1 | None. | Satisfied |

### 6.4.3 Security Assurance Requirements

The assurance security requirements for this Security Target are from EAL 1. The assurance components are summarized in the following table:

| CLASS HEADING | CLASS_FAMILY | DESCRIPTION |
|---|---|---|
| ADV: Development | ADV_FSP.1 | Basic Functional Specification |
| AGD: Guidance Documents | AGD_OPE.1 | Operational User Guidance |
| | AGD_PRE.1 | Preparative Procedures |
| ALC: Lifecycle Support | ALC_CMC.1 | Labeling of the TOE |
| | ALC_CMS.1 | TOE CM coverage |
| ATE: Tests | ATE_IND.1 | Independent Testing - Conformance |
| AVA: Vulnerability Assessment | AVA_VAN.1 | Vulnerability Analysis |

**Table 6-4 – Security Assurance Requirements**

### 6.4.4 Security Assurance Requirements Rationale

The ST specifies assurance activities specified in EAL 1.

# 7 TOE Summary Specification

This section presents the Security Functions implemented by the TOE.

## 7.1 TOE Security Functions

The security functions performed by the TOE are as follows:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channel

## 7.2 Security Audit

The TOE generates audit log entries for security events.

The Security Audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1
- FAU_GEN.2
- FAU_STG_EXT.1

### 7.2.1 FAU_GEN.1 and FAU_GEN.2 Audit Date Generation and User Identify Association

The following events are logged in PRIISMS system logs with the date and time of the event, type of event, user/subject identity, and success/failure of the event.

System logs are described in ION PRIISMS Administrator Guide Chapter 10: Managing System Logs.

| REQUIREMENT | AUDITABLE EVENTS | ADDITIONAL DETAILS | REFERENCES |
|---|---|---|---|
| FAU_GEN.1 | Start up auditing function | | System start up is logged. |

| REQUIREMENT | AUDITABLE EVENTS | ADDITIONAL DETAILS | REFERENCES |
|---|---|---|---|
| FAU_GEN.1 | All Administrative actions | | See FCS_TLS_EXT.1, FCS_HTTPS_EXT.1, FIA_UIA_EXT.1, FIA_UAU_EXT.2, FPT_STM.1, FPT_TUD_EXT.1, FTA_SSL_EXT.1, and FTP_TRP.1 |
| FCS_TLS_EXT.1 | Failure to establish a TLS Session.<br>Establishment/Termination of a TLS session. | Reason for failure.<br>Non-TOE endpoint of connection (IP address) for both successes and failures. | See FCS_HTTPS_EXT.<br>TLS is used with HTTPS to establish administrative user console access. |
| FCS_HTTPS_EXT.1 | Failure to establish a HTTPS Session.<br>Establishment/Termination of a HTTPS session. | Reason for failure.<br>Non-TOE endpoint of connection (IP address) for both successes and failures. | HTTPS is used to establish administrative user console access. |
| FIA_UIA_EXT.1 | All use of the identification and authentication mechanism. | Provided user identity, origin of the attempt (e.g., IP address). | System logs record administrator user login including identification, authentication, and IP address. |
| FIA_UAU_EXT.2 | All use of the authentication mechanism | Origin of the attempt (e.g., IP address). | System logs record administrator user login including identification, authentication, and IP address. |
| FPT_STM.1 | Changes to the time. | The old and new values for the time.<br>Origin of the attempt (e.g., IP address). | Appliance logs time changes through the appliance interface. |
| FPT_TUD_EXT.1 | Initiation of update. | No additional information. | Appliance firmware updates are logged. |
| FPT_TST_EXT.1 | Indication that TSF self-test was completed. | Any additional information generated by the tests beyond “success” or “failure”. | Self-tests are incorporated with the FIPS crypto module. |
| FTA_SSL_EXT.1 | Any attempts at unlocking of an interactive session. | No additional information | The TOE terminates sessions that exceed timeouts. There are no administrator capabilities to unlock user sessions. |

| REQUIREMENT | AUDITABLE EVENTS | ADDITIONAL DETAILS | REFERENCES |
|---|---|---|---|
| FTA_SSL.3 | The termination of a remote session by the session locking mechanism. | No additional information. | Idle administrator session terminations are logged |
| FTA_SSL.4 | The termination of an interactive session. | No additional information. | Administrator logout is logged in the system log. |
| FTP_ITC.1 | Initiation of the trusted channel.<br>Termination of the trusted channel.<br>Failure of the trusted channel functions. | Identification of the initiator and target of failed trusted channels establishment attempt. | Starting, ending, and failures connections to audit server are logged. |
| FTP_TRP.1 | Initiation of the trusted channel.<br>Termination of the trusted channel.<br>Failures of the trusted path functions. | Identification of the claimed user identity. | Administrator logins, logouts, and failures are logged in the system log. |

### 7.2.2 FAU_STG_EXT.1 External Audit Trail Storage

The TOE sends audit logs to an external log server using Stunnel using TLS to secure the transfer of the audit records. Locally, the TOE stores audit records and overwrites the records when the log capacity is exceeded. The SA5600 supports up to 128 Mbytes. The log files are not accessible from outside the TOE. The TOE does not provide any capability for deleting log records.

## 7.3 Cryptographic Support

The TOE implements uses a cryptographic module which has a FIPS 140-2 validation  (Certificate # 2070) to provide the TOE with cryptographic functions in support of secure communications between TOE components and trusted external IT entities. The cryptographic module has the following cryptographic algorithm validation program (CAVP) certificates:

| ALGORITHM | CAVP CERTIFICATE NUMBER |
|---|---|
| AES | 2273 |
| RSA | 1166 |
| Triple- DES | 1420 |
| SHA | 1954 |
| RNG | 1132 |
| DRBG | 281 |
| HMAC | 1391 |

The TOE also uses the Microsoft IIS web server which provides HTTPS/TLS for remote administrator console access. The FIPS 140-2 CMVP certificate number is 2356. The cryptographic module used by IIS has the following cryptographic algorithm validation program (CAVP) certificates:

| ALGORITHM | CAVP CERTIFICATE NUMBER |
|---|---|
| AES | 2832 |
| SHS | 2373 |
| DRBG | 489 |
| HMAC | 1773 |
| RSA | 1487, 1493, 1519 |
| KAS | 47 |

**Table 7-1 - IIS CAVP Certificates**

The Open-VPN and stunnel implementations under FIPS cert #2070 have the ECCDH Primative tested under CVL certificate #44.

The Cryptographic Support function is designed to satisfy the following security functional requirements:

- FCS_CKM.1
- FCS_CKM_EXT.4
- FCS_COP.1(1)
- FCS_COP.1(2)
- FCS_COP.1(3)
- FCS_COP.1(4)
- FCS_RBG_EXT.1
- FCS_TLS_EXT.1
- FCS_HTTPS_EXT.1

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

The relevant sections of 800-56B for asymmetric cryptographic keys is section 6 - RSA Key Pairs.

All “SHALL” statements within the listed sections are implemented in the TOE and all “SHALL NOT” statements are adhered to within the TOE and the described functionality/behavior is not present. The implemented option associated with each “SHOULD” and “SHOULD NOT” statement in a referenced section is detailed.

There are no TOE-specific extensions, processing that is not included in the documents, or alternative implementations that impact the security requirements the TOE.

The TOE implements FFC Domain Parameter Generation that conforms to FIPS 186-3.

### 7.3.2 FCS_CKM_EXT.4 Cryptographic Key Zeroization

The following table describes the keys used by the TOE and the zeroization mechanism.

| Keys and CSPs | Zeroization |
|---|---|
| AES Key | overwrite with zeroes when no longer needed |
| RSA Public Key | overwrite with zeroes when no longer needed |
| RSA Private Key | overwrite with zeroes when no longer needed |
| HMAC Key | overwrite with zeroes when no longer needed |
| Integrity Key | overwrite with zeroes when no longer needed |
| HMAC DRBG Entropy | overwrite with zeroes when no longer needed |
| HMAC DRBG Key | overwrite with zeroes when no longer needed |
| HMAC DRBG init_seed | overwrite with zeroes when no longer needed |

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

The TOE uses a random bit generation (RBG) service in accordance with NIST Special Publication 800-90 using HMAC_DRBG (SHA-256); FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using AES seeded by an entropy source from a software-based noise source.

The PRIISMS component uses the Windows[6] CryptGenRandom() API to get random numbers. CryptGenRandom main entropy sources are:

- Time (time since boot)
- System performance and CPU counter data
- Timings of context switches and interrupts

The resulting byte stream (called system entropy) is hashed with SHA-1 to produce a 20-byte seed. This seed is used to generate random numbers in accordance with FIPS 186-2. The system entropy pool produced is 3584 bytes.[7]

The SA5600 appliance uses the X9.31 compliant Linux kernel Random Number Generator. The SA5600 runs on a Linux Kernel version 2.6.33.11. The Linux /dev/random[8] device driver is provides random numbers to the crypto module and obtains its entropy from system timings in milliseconds from:

- Key events
- Mouse events
- Completion of disk I/O events
- IRQ events

[6] From *Writing Secure Code, Second Edition* by Howard and LeBlanc

[7] From *Cryptanalysis of the Random Number Generator of the Windows Operating System* by Dorrendorf, Gutterman, and Pinkas. While this document references older versions of Windows, the entropy mechanism has nto changes for the Windows operating systems used in this TOE's evaluated configuration.

[8] From *Analysis of the Linux Random Number Generator* by Gutterman, Pinkas, and Reinmann.

Each event generates a 32-bit value representing timing and another 32-bit value representing the attribute (e.g., keystroke). These sources are batched a few times per minute and are sent to fill a 512 byte primary entropy pool. If the primary entry pool is full, a secondary pool is filled. These pools are the source of random data for /dev/random.

### 7.3.4 FCS_TLS_EXT.1 Extended: TLS

The TOE uses IIS v8.0 which supports TLS v1.1 and v1.2 on Windows Server 2012 R2.

The TOE supports the following TLS cipersuites:

- TLSv1_ECDHE-RSA-AES256-SHA
- TLSv1_RSA_AES256-SHA
- TLSv1_RSA_DES-CBC3-SHA
- TLSv1_ECDHE-RSA-AES128-SHA
- TLSv1_RSA_AES128-SHA
- TLS1.1_ECDHE-RSA-AES256-SHA
- TLS1.1_RSA_AES256-SHA
- TLS1.1_RSA_DES-CBC3-SHA
- TLS1.1_ECDHE-RSA-AES128-SHA
- TLS1.1_RSA_AES128-SHA];

Here are the steps to enable TLS 1.1 and TLS 1.2 on the Windows Server 2012 R2 server in the PRIISMS appliance:

1. Please backup your registry.
2. Start the registry editor (`regedit`)
3. Browse to the following registry key: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols`
4. Add the following keys:
   `TLS 1.1` and `TLS 1.2`
5. Within each of the `TLS 1.1` and `TLS 1.2` keys (they look like folders), add these keys: `Client` and `Server`
6. Within each of the `Client` and `Server` keys, create the following DWORD values:
   - `DisabledByDefault` with a value of `0`
   - `Enabled` with a value of `1`
7. Reboot the server.

The TOE also uses TLS for secure communications to the syslog server using Stunnel v4.55. Refer to FAU_STG_EXT.1.

The TOE uses OpenVPN v2.3_rc1 to secure communications between TOE components. Refer to FPT_ITT.1.

The TOE uses TLS for secure communications between PRIISMS and the SA5600 over the TLS connection.

### 7.3.5 FCS_HTTPS_EXT.1 Extended: HTTPS

The TOE uses IIS v8.0 on Windows Server 2012 R2 to provide HTTPS using TLS v1.1 and v1.2. HTTPS is used for administrator console access via web browser. Enabling HTTPS is a requirement in the evaluated configuration.

## 7.4 User Data Protection

The TOE clears memory resources before reuse. Memory allocation/deallocation mechanisms are used to ensure that user data is protected.

The User Data Protection function is designed to satisfy the following security functional requirements:

- FDP_RIP.2

### 7.4.1 FDP_RIP.2 Full Residual Information Protection

The only resource made available to information flowing through a TOE is the temporary storage of packet information when access is requested and when information is being routed. User data is not persistent when resources are released by one user/process and allocated to another user/process. Temporary storage (memory) used to build network packets is erased when the resource is called into use by the next user/process.

The TOE knows, and keeps track of, the length of the packet. This means that when memory allocated from a previous user/process arrives to build the next network packet, The TOE is aware of when the end of the packet is reached and pads a short packet with zeros accordingly using a function called skb_pad. Therefore, no residual information from packets in a previous information stream can traverse through the TOE.

## 7.5 Identification and Authentication

Administrators are required to login to the PRIISMS console before gaining access to the TOE functions and data.

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_PMG_EXT.1
- FIA_UIA_EXT.1
- FIA_UAU_EXT.2
- FIA_UAU.7

### 7.5.1 FIA_PMG_EXT.1 Password Management

User passwords can be composed of any combination of upper and lower case letters, numbers, and the following special characters: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”. See Section 8.1.6 of PRIISMS Administrator Guide 3.0 (MinimumPasswordLength).

### 7.5.2 FIA_UIA_EXT.1, FIA_UAU_EXT.2, and FIA UAU.7 User Identification and Authentication, Extended: Password-based Authentication Mechanism, and Protected Authentication Feedback.

Local and remote users are required to successfully identify and authenticate locally with the TOE through the PRIISMS console using a valid administrator name and password before gaining access to the TOE functions or data. The identification and authentication process takes place over a communications channel secured by HTTPS/TLS. Only the login banner is displayed along with the login screen to the user. The user is successfully logged in when the user name and password credentials have been validate by the TOE and the main console screen is presented to the user. A system log record is written when the user has successfully logged in.

Passwords are obscured during the authentication process. Failed login attempts return obscured feedback to the user (i.e., failed login attempts are returned feedback that do not specify whether the user name or the password were incorrect). Failed login attempts are also recorded in the system log.

## 7.6 Security Management

The TOE restricts local and remote access to management functions to Authorized Administrators only. No functions are available prior to user authentication.

The Security Management function is designed to satisfy the following security functional requirements:

- FMT_MTD.1
- FMT_SMF.1
- FMT_SMR.2

### 7.6.1 FMT_MTD.1, FMT_SMF.1, and FMT_SMR.2 Management of TSF Data (for general TSF data), Specification of Management Functions, and Restrictions of Security Roles

Only authorized administrators have access to perform the following local and remote management functions:

- Ability to update the TOE, and to verify the updates prior to installing those updates with published hash.
- Configure the warning banner. See the PRIISMS Administrator Guide 3.0
- Set minimum user password lengths. See the PRIISMS Administrator Guide 3.0 (MinimumPasswordLength).
- Set user idle session timeouts. See the PRIISMS Administrator Guide 3.0 (WebInactivityMinutes).
- No functions are available to users prior to successful login.

The TOE maintains only one user role:

- Authorized Administrator

## 7.7 Protection of the TSF

The TOE implements several self-protection mechanisms to protect TSF data. The appliance provides a reliable time source for use by the TOE.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_SKP_EXT.1
- FPT_APW_EXT.1
- FPY_ITT.1
- FPT_STM.1
- FPT_TUD_EXT.1
- FPT_TST_EXT.1

### 7.7.1 FPT_SKP_EXT.1 Extended: Protection of TSF Data (for reading of passwords) and FPT_APW_EXT.1 Extended: Protection of Administrator Passwords

The TOE prevents the reading of administrator passwords by storing them in persistent storage in non-plaintext form.  These are stored within the SQL server database using SHA-256 hashing. The SQL Server is locked down with the SQL Server STIG including the restriction of only one application account, and only one SQL Admin account.

### 7.7.2 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

The communications between PRIISMS and the SA5600 components uses OpenVPN v2.3_rc1 which employs TLS to protect communications between TOE components. The PRIISMS component and SA5600 appliance component communicate via TLS. See FCS_TLS_EXT.1 Extended: TLS  for details.

### 7.7.3 FPT_STM.1 Reliable Time Stamps

The SA5600 appliance keeps its own system time and has the provision to change the system time.

### 7.7.4 FPT_TUD_EXT.1 Extended: Trusted Update

Updates to the appliance firmware use a published hash using SHA-512 to ensure that the updates can be trusted. Refer to the ION Security Appliance Administrator Guide - Upgrade, Version, and Boot Commands and the ION PRIISMS & ION SA5600 Secure Appliance Military Unique Deployment Guide – Software Upgrades for further information on firmware updates for the appliance.

### 7.7.5 FPT_TST_EXT.1 TSF Testing

The TOE performs the following cryptographic module known answer self-tests upon power-up.  These test ensure that the critical cryptographic functions are operating properly.  Any self-test failure results in the failure of the cryptographic module startup.

| TYPE | DETAIL |
|---|---|
| Software Integrity Check | HMAC SHA-256 |
| Known Answer Tests[9] | • AES encrypt/decrypt<br>• HMAC SHA-1<br>• RSA<br>• SHA-256<br>• SHA-512<br>• X9.31 RNG |
| Pair-wise Consistency Tests | • RSA |

In addition, PRIISMS appliance has a Windows scheduled task that runs daily to verify that the current set of binaries and application pages match the published set of SHA-256 hashes. If the daily test fails, an Administrative alert is generated per mismatched file including the name/path of the failed file. If the daily test succeeds a Confirmation alert is generated. At Windows bootup time, the BIOS performs the necessary hardware checks to ensure that the operating system loads properly. The operating system also performs hardware driver checks.

The SA5600  has a file integrity checking mechanism (through the FIC command) using AIDE (Advanced Intrusion Detection Environment). AIDE creates a database from the regular expression rules that it finds from its configuration files. Once this database is initialized it is used to verify the integrity of the files. It

[9] Note that all SHA-X KATs are tested as part of the respective HMAC SHA-X KAT.

uses a message digest algorithm (SHA 512) to check the integrity of the file. All of the usual file attributes are checked for inconsistencies. It reads databases from older or newer versions. The database for all executables, scripts, and libraries is created at boot time. The file Integrity is then checked daily or can be invoked on demand using the FIC command. At Linux bootup time, the BIOS performs the necessary hardware checks to ensure that the operating system loads properly. The operating system also performs hardware driver checks.

These power-on and bootup checks ensure that the TOE hardware and software are operating properly.

## 7.8 TOE Access

Local and remote access to the TOE is controlled by the TOE.

The TOE Access function is designed to satisfy the following security functional requirements:

- FTA_SSL_EXT.1
- FTA_SSL.3
- FTA_SSL.4
- FTA_TAB.1

### 7.8.1 FTA_SSL_EXT.1, FTA_SSL.3, and FTA_SSL.4 TSF-Initiated Session Locking, TSF-Initiated Termination, and User-Initiated Termination

The TOE terminates local and remote administrator user sessions after an Administrator-specified idle period. See Section 8.1.7 of PRIISMS Administrator Guide 3.0 (WebInactivityMinutes) to set the idle timeout period.

Users can terminate their own sessions by logging out of the console by clicking the “Log Out” link on any PRIISMS web page. Logouts are logged in the system log.

### 7.8.2 FTA_TAB.1 Default TOE Access Banners

An Administrator-defined banner will be displayed to users prior to logging in. See Section 3.2.5 in the ION PRIISMS & ION SA5600 Secure Appliance Military Unique Deployment Guide to define the login banner contents.

## 7.9 Trusted Path/Channel

The TOE provides trusted channel communications with external audit server using stunnel using TLS.

The TOE protects communication paths to administrator consoles via web browser using HTTPS with TLS.

The TOE protects communications paths between the SA5600 to PRIISMS using TLS.

The Protection of the TSF and Trusted Path/Channel function is designed to satisfy the following security functional requirements:

- FTP_ITC.1
- FTP_TRP.1

### 7.9.1 FTP_ITC.1 Inter-TSF trusted channel

The TOE communicates with the external audit log server using TLS. See FCS_TLS_EXT.1 Extended: TLS for more information about the use of TLS.

### 7.9.2 FTP_TRP.1 Trusted Path

The TOE uses HTTPS/TLS for communications between PRIISMS and the remote administrator console. See FCS_HTTPS_EXT.1 Extended: HTTPS for more information about the use of HTTPS.

PRIISMS and the SA5600 appliance use TLS to communicate securely. See FCS_TLS_EXT.1 Extended: TLS for more information about the use of TLS.