# Kemp LoadMaster Security Target

Document Version: 0.8

intertek acumen security

2400 Research Blvd
Suite 395
Rockville, MD 20850

**Revision History**

| Version | Date | Changes |
|---|---|---|
| Version 0.1 | 7/13/2020 | Initial Version |
| Version 0.2 | 9/9/2020 | Updated based on Kemp input |
| Version 0.3 | 10/2/2020 | Updated based on additional Kemp review |
| Version 0.4 | 12/8/2021 | Updated based on Kemp input and updated to new template |
| Version 0.5 | 12/14/2021 | Updated based on QA feedback |
| Version 0.6 | 4/1/2022 | Updates based on ECRs |
| Version 0.7 | 12/15/2022 | Updates based on review |
| Version 0.8 | 01/19/2023 | Updated based on ECRs |

# Contents

# 1 Introduction

The Security Target (ST) serves as the basis for the Common Criteria (CC) evaluation and identifies the Target of Evaluation (TOE), the scope of the evaluation, and the assumptions made throughout. This document will also describe the intended operational environment of the TOE, and the functional and assurance requirements that the TOE meets.

## 1.1 Security Target and TOE Reference

This section provides the information needed to identify and control the TOE and the ST.

**Table 1 – TOE/ST Identification**

| Category | Identifier |
|---|---|
| ST Title | Kemp LoadMaster Security Target |
| ST Version | 0.8 |
| ST Date | 01/19/23 |
| ST Author | Acumen Security, LLC. |
| TOE Identifier | Kemp LoadMaster |
| TOE Version | Loadmaster OS 7.2.48.8 |
| TOE Developer | Progress Software Corporation |
| Key Words | Network Device, Load Balancer |

## 1.2 TOE Overview

The TOE is Kemp LoadMaster X15, X25 and X40 and Virtual LoadMaster running on OS 7.2.48.8. The LoadMaster simplifies the management of networked resources, and optimizes and accelerates user access to diverse servers, content, and transaction-based systems. The TOE is comprised of hardware and software and represents a complete network device providing load balancing functionality. The evaluated functionality is described in Section 1.3.2 below.

## 1.3 TOE Description

Kemp LoadMaster is a load balancer and application delivery controller (ADC) appliance. It is designed to increase the availability, scalability, and security of applications and data centers. The TOE delivers unparalleled performance for organizations of all sizes with integrated hardware acceleration and support for up to 35 million concurrent connections. The TOE is a network device.

### 1.3.1 Physical Boundaries

The TOE boundary consists of one of the appliances listed below. The LoadMaster X15, X25 and X40 are physical devices while the Virtual LoadMaster is a virtual machine which runs on ESXi. The virtual TOE is conformant with Case 1 as described in the NDcPP:

**Table 2 – TOE Models**

| Model | LoadMaster X15 | LoadMaster X25 | LoadMaster X40 | Virtual LoadMaster |
|---|---|---|---|---|
| Processor | Intel Xeon E3-1275v6 (Kaby Lake) | Intel Xeon Silver 4116T (Skylake) | Intel Xeon Gold 6136 (Skylake) | Intel Xeon E5 4620 v4 (Broadwell) |

| Model | LoadMaster X15 | LoadMaster X25 | LoadMaster X40 | Virtual LoadMaster |
|---|---|---|---|---|
| RAM | 32 GB RAM | 64 GB RAM | 64 GB RAM | 2GB (evaluated) |
| Network | 16 1Gb Ethernet<br>4 10Gb Ethernet Fiber | 2 1Gb Ethernet<br>12 10Gb Ethernet Fiber | 2 1Gb Ethernet<br>12 10Gb Ethernet Fiber | 3 1Gb virtual NIC (evaluated) |
| Platform | Loadmaster OS 7.2.48.8 | Loadmaster OS 7.2.48.8 | Loadmaster OS 7.2.48.8 | Loadmaster OS 7.2.48.8 on ESXi v6.7 |

### 1.3.2 Security Functions Provided by the TOE

The TOE provides the security functions required by the Collaborative Protection Profile for Network Devices version 2.2e, hereafter referred to as NDcPP v2.2e or NDcPP.

#### 1.3.2.1 Security Audit

The TOE generates audit records for security relevant events. The audit events are associated with the administrator or processes. The audit records are transmitted over TLS to an external audit server.

#### 1.3.2.2 Cryptographic Support

The TOE provides following cryptographic services described below.

**Table 3 – Cryptographic Services**

| Service | Use |
|---|---|
| TLS Client | Secure connection to remote syslog servers. |
| TLS Client | Secure connection to remote LDAP server. |
| TLS/HTTPS Server | Secures connections with remote administrators. |
| Verification of Updates | Digital signature verification prior to installing an update. |

Each of these cryptographic algorithms have been validated for conformance to the requirements specified in their respective standards, as identified below.

#### 1.3.2.3 Identification and Authentication

The TOE supports a password-based authentication mechanism which automatically locks users after a pre-configured number of failed attempts. The TOE also validates X.509 certificates in support of TLS.

#### 1.3.2.4 Security Management

The TOE provides management capabilities via Console and a Web-based GUI, accessed over HTTPS. Management functions allow the administrators to configure the system, install updates, and manage users.

#### 1.3.2.5 Protection of the TSF

The TOE prevents the reading of plaintext passwords and keys. The TOE provides a reliable timestamp for its own use. The reliable timestamp can be set by a security administrator or authenticated NTP. To protect the integrity of its security functions, the TOE implements a suite of self-tests at startup and

halts or disables affected functionality if a self-test fails. The TOE ensures that updates to the TOE are authenticated by verifying a digital signature prior to installing any update.

#### 1.3.2.6 TOE Access

The TOE monitors local and remote administrative sessions for inactivity and either locks or terminates the session when a threshold time period is reached. An advisory notice is displayed at the start of each session.

#### 1.3.2.7 Trusted Path/Channels

The TOE initiates a TLS trusted channel with a syslog server and LDAP authentication server (as configured).

The TOE is a TLS/HTTPS server that allows remote administrators to establish a trusted path with the TOE.

### 1.3.3 TOE Documentation

The following documents are essential to understanding and controlling the TOE in the evaluated configuration:

- Configuring LoadMaster for Common Criteria Conformance v0.2
- LoadMaster CLI Interface description 20 September 2022
- Web User Interface (WUI) Configuration Guide 04 October 2022

### 1.3.4 References

In additional to TOE documentation, the following reference may also be valuable when understanding and controlling the TOE:

- Kemp LoadMaster Security Target Version 0.8

## 1.4 TOE Environment

The following environmental components are required to operate the TOE in the evaluated configuration:

**Table 4 – Required Environmental Components**

| Component | Required | Usage/Purpose Description |
|---|---|---|
| Management Workstation | Yes | Workstation providing local console access to the TOE.<br>Workstation providing a browser to connected to the Web User Interface (WUI) over TLSv1.2 or TLSv1.1. |
| Audit Server | Yes | Syslog server that receives audit logs from the TOE over TLSv1.2 or TLSv1.1. |
| ESXi Server | Yes (for Virtual LoadMaster) | ESXi v6.7 acting as the hypervisor for Virtual LoadMaster. |
| LDAP Server | No | Optional authentication server supporting LDAP over TLSv1.2 or TLSv1.1. |
| NTP Server | No | Optional NTP server supporting SHA-1 integrity verification. |

## 1.5 Product Functionality not Included in the Scope of the Evaluation

The following product functionality is not included in the CC evaluation:

- SSH
- Management API
- Administrative Trusted Channels
- IPv6

# 2 Conformance Claims

## 2.1 CC Conformance Claims

The TOE is conformant to the following:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017 (Extended)
- Common Criteria for Information Technology Security Evaluations Part 3, Version 3.1, Revision 5, April 2017 Conformant

## 2.2 Protection Profile Conformance

This ST claims exact conformance to the following:

- collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [PP-ND]

## 2.3 Conformance Rationale

This ST provides exact conformance to the items listed in the previous section. The security problem definition, security objectives, and security requirements in this ST are all taken from the Protection Profile (PP), performing only the operations defined there.

### 2.3.1 Technical Decisions

**Table 5 – Relevant Technical Decisions**

| Technical Decision | Applicable (Y/N) | Exclusion Rationale (if applicable) |
|---|---|---|
| TD0527: NIT Technical Decision for Updates to Certificate Revocation Testing (FIA_X509_EXT.1) | Yes | |
| TD0528: NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4 | Yes | |
| TD0536: NIT Technical Decision for Update Verification Inconsistency | Yes | |
| TD0537: NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3 | No | FCS_TLSC_EXT.2.3 is not claimed |
| TD0538: NIT Technical Decision for Outdated link to allowed-with list | Yes | |
| TD0546: NIT Technical Decision for DTLS – clarification of Application Note 63 | No | DTLS is not claimed |
| TD0547: NIT Technical Decision for Clarification on developer disclosure of AVA_VAN | Yes | |
| TD0555: NIT Technical Decision for RFC Reference incorrect in TLSS Test | Yes | |
| TD0556: NIT Technical Decisions for RFC 5077 question | No | Session tickets are not claimed |

| Technical Decision | Applicable (Y/N) | Exclusion Rationale (if applicable) |
|---|---|---|
| TD0563: NIT Technical Decision for Clarification of audit date information | Yes | |
| TD0564: NIT Technical Decision for Vulnerability Analysis Search Criteria | Yes | |
| TD0569: NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7 | NO | DTLSS is not claimed |
| TD0570: NIT Technical Decision for Clarification about FIA_AFL.1 | Yes | |
| TD0571: NIT Technical Decision for Guidance on how to handle FIA_AFL.1 | Yes | |
| TD0572: NIT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers | Yes | |
| TD0580: NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e | No | Diffie Helman Group 14 is not claimed |
| TD0581: NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3 | Yes | |
| TD0591: NIT Technical Decision for Virtual TOEs and hypervisors | Yes | |
| TD0592: NIT Technical Decision for Local Storage of Audit Records | Yes | |
| TD0631: NIT Technical Decision for Clarification of public key authentication for SSH Server | No | SSH is not claimed |
| TD0632: NIT Technical Decision for Consistency with Time Data for vNDs | Yes | |
| TD0633: NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance | No | IPsec is not claimed |
| TD0634: NIT Technical Decision for Clarification required for testing IPv6 | No | IPv6 is not claimed |
| TD0635: NIT Technical Decision for TLS Server and Key Agreement Parameters | Yes | |

| Technical Decision | Applicable (Y/N) | Exclusion Rationale (if applicable) |
|---|---|---|
| TD0636: NIT Technical Decision for Clarification of Public Key User Authentication for SSH | No | SSH is not claimed |
| TD0638: NIT Technical Decision for Key Pair Generation for Authentication | Yes | |
| TD0639 : NIT Technical Decision for Clarification for NTP MAC Keys | Yes | |
| TD0670: NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing | Yes | |

# 3 Security Problem Definition

The security problem definition has been taken directly from the claimed PP and any relevant EPs/Modules/Packages specified in Section 2.2 and is reproduced here for the convenience of the reader. The security problem is described in terms of the threats that the TOE is expected to address, assumptions about the operational environment, and any Organizational Security Policies (OSPs) that the TOE is expected to enforce.

## 3.1 Threats

The threats included in Table below are drawn directly from the PP and any EPs/Modules/Packages specified in Section 2.2.

**Table 6 – Threats**

| ID | Threat |
|---|---|
| T.UNAUTHORIZED_ADMINISTRATOR_ACCESS | Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides. |
| T.WEAK_CRYPTOGRAPHY | Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort. |
| T.UNTRUSTED_COMMUNICATION_CHANNELS | Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself. |
| T.WEAK_AUTHENTICATION_ENDPOINTS | Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of |

| ID | Threat |
|---|---|
| | confidentiality and integrity, and potentially the Network Device itself could be compromised. |
| T.UPDATE_COMPROMISE | Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration. |
| T.UNDETECTED_ACTIVITY | Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised. |
| T.SECURITY_FUNCTIONALITY_COMPROMISE | Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker. |
| T.PASSWORD_CRACKING | Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other Network Devices. |
| T.SECURITY_FUNCTIONALITY_FAILURE | An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device. |

## 3.2 Assumptions

The assumptions included in Table 7are drawn directly from PP and any relevant EPs/Modules/Packages.

**Table 7 – Assumptions**

| ID | Assumption |
|---|---|
| A.PHYSICAL_PROTECTION | The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs. |
| A.LIMITED_FUNCTIONALITY | The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).<br><br>If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform. |
| A.NO_THRU_TRAFFIC_PROTECTION | A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall). |

| ID | Assumption |
|---|---|
| A.TRUSTED_ADMINISTRATOR | The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. |
| A.REGULAR_UPDATES | The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities. |
| A.ADMIN_CREDENTIALS_SECURE | The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside. |
| A.RESIDUAL_INFORMATION | The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. |
| A.VS_TRUSTED_ADMINISTRATOR | The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device. |
| A.VS_REGULAR_UPDATES | The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities. |
| A.VS_ISOLATION | For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform. |
| A.VS_CORRECT_CONFIGURATION | For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs. |

## 3.3 Organizational Security Policies

The OSPs included in Table  are drawn directly from the PP and any relevant EPs/Modules/Packages.

**Table 8 – OSPs**

| ID | OSP |
|---|---|
| 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. |

# 4 Security Objectives

The security objectives have been taken directly from the claimed PP and any relevant EPs/Modules/Packages and are reproduced here for the convenience of the reader.

## 4.1 Security Objectives for the Operational Environment

Security objectives for the operational environment assist the TOE in correctly providing its security functionality. These objectives, which are found in the table below, track with the assumptions about the TOE operational environment.

**Table 9 – Security Objectives for the Operational Environment**

| ID | Objectives for the Operational Environment |
|---|---|
| OE.PHYSICAL | Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment. |
| 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. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS. |
| OE.NO_THRU_TRAFFIC_PROTECTION | The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment. |
| OE.TRUSTED_ADMN | Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality. |
| OE.UPDATES | The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities. |
| OE.ADMIN_CREDENTIALS_SECURE | The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside. |
| OE.RESIDUAL_INFORMATION | The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment. |

| ID | Objectives for the Operational Environment |
|---|---|
| OE.VM_CONFIGURATION | For vNDs, the Security Administrator ensures that the VS and VMs are configured to<br>• Reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and<br>• Correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting).<br>The VS should be operated in a manner that reduces the likelihood that vND operations are adversely affected by virtualisation features such as cloning, save/restore, suspend/resume, and live migration.<br>If possible, the VS should be configured to make use of features that leverage the VS's privileged position to provide additional security functionality. Such features could include malware detection through VM introspection, measured VM boot, or VM snapshot for forensic analysis |

# 5 Security Requirements

This section identifies the Security Functional Requirements (SFRs) for the TOE. The SFRs included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revisions 5, September 2017, and all international interpretations.

**Table 10 – SFRs**

| Requirement | Description |
|---|---|
| FAU_GEN.1 | Audit Data Generation |
| FAU_GEN.2 | User Identity Association |
| FAU_STG_EXT.1 | Protected Audit Event Storage |
| FAU_STG_EXT.3/LocSpace | Action in Case of Possible Audit Data Loss |
| FCS_CKM.1 | Cryptographic Key Generation |
| FCS_CKM.2 | Cryptographic Key Establishment |
| FCS_CKM.4 | Cryptographic Key Destruction |
| FCS_COP.1/DataEncryption | Cryptographic Operation (AES Data Encryption/Decryption) |
| FCS_COP.1/SigGen | Cryptographic Operation (Signature Generation and Verification) |
| FCS_COP.1/Hash | Cryptographic Operation (Hash Algorithm) |
| FCS_COP.1/KeyedHash | Cryptographic Operation (Keyed Hash Algorithm) |
| FCS_HTTPS_EXT.1 | HTTPS Protocol |
| FCS_NTP_EXT.1 | NTP Protocol |
| FCS_RBG_EXT.1 | Random Bit Generation |
| FCS_TLSC_EXT.1 | TLS Client Protocol without Mutual Authentication |
| FCS_TLSS_EXT.1 | TLS Server Protocol without Mutual Authentication |
| FIA_AFL.1 | Authentication Failure Management |
| FIA_PMG_EXT.1 | Password Management |
| FIA_UIA_EXT.1 | User Identification and Authentication |
| FIA_UAU_EXT.2 | Password-based Authentication Mechanism |
| FIA_UAU.7 | Protected Authentication Feedback |
| FIA_X509_EXT.1/Rev | X.509 Certificate Validation |
| FIA_X509_EXT.2 | X.509 Certificate Authentication |
| FIA_X509_EXT.3 | X.509 Certificate Requests |
| FMT_MOF.1/ManualUpdate | Management of Security Functions Behaviour |
| FMT_MOF.1/Services | Management of Security Functions Behaviour |
| FMT_MTD.1/CoreData | Management of TSF Data |
| FMT_MTD.1/CryptoKeys | Management of TSF Data |
| FMT_SMF.1 | Specification of Management Functions |
| FMT_SMR.2 | Restrictions on security roles |
| FTP_APW_EXT.1 | Protection of Administrator Passwords |
| FPT_SKP_EXT.1 | Protection of TSF Data (for reading of all pre-shared, symmetric and private keys) |

| Requirement | Description |
|---|---|
| FPT_TST_EXT.1 | TSF Testing |
| FPT_STM_EXT.1 | Reliable Time Stamps |
| FPT_TUD_EXT.1 | Trusted Update |
| FTA_SSL.3 | TSF-initiated Termination |
| FTA_SSL.4 | User-initiated Termination |
| FTA_SSL_EXT.1 | TSF-initiated Session Locking |
| FTA_TAB.1 | Default TOE Access Banner |
| FTP_ITC.1 | Inter-TSF Trusted Channel |
| FTP_TRP.1/Admin | Trusted Path |

## 5.1 Conventions

The CC allows the following types of operations to be performed on the functional requirements: assignments, selections, refinements, and iterations. The following font conventions are used within this document to identify operations defined by CC:

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with underlined text;
- Iteration: Indicated by appending the iteration identifier after a slash, e.g., /SigGen.
- Where operations were completed in the PP and relevant EPs/Modules/Packages, the formatting used in the PP has been retained.
- Extended SFRs are identified by the addition of "EXT" after the requirement name.

## 5.2 Security Functional Requirements

This section includes the SFRs for this ST.

### 5.2.1 Security Audit (FAU)

#### 5.2.1.1 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:

a) Start-up and shut-down of the audit functions;
b) Auditable events for the not specified level of audit; and
c) *All administrative actions comprising:*
   - *Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).*
   - *Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
   - *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
   - *Resetting passwords (name of related user account shall be logged).*
   - [*no other actions*]*;*
d) *Specifically defined auditable events listed in Table 11*.

**FAU_GEN.1.2**

a) 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

b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, *information specified in column three of Table 11.*

**Table 11 – Security Functional Requirements and Auditable Events**

| Requirement | Auditable Events | Additional Audit Record Contents |
|---|---|---|
| FAU_GEN.1 | • Start-up and shut-down of the audit functions.<br>• Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).<br>• Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).<br>• Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).<br>• Resetting passwords (name of related user account shall be logged). | None |
| FAU_GEN.2 | None | None |
| FAU_STG_EXT.1 | None | None |
| FAU_STG_EXT.3/LocSpace | Low storage space for audit events | None |
| FCS_CKM.1 | None | None |
| FCS_CKM.2 | None | None |
| FCS_CKM.4 | None | None |
| FCS_COP.1/DataEncryption | None | None |
| FCS_COP.1/SigGen | None | None |
| FCS_COP.1/Hash | None | None |
| FCS_COP.1/KeyedHash | None | None |

| Requirement | Auditable Events | Additional Audit Record Contents |
|---|---|---|
| FCS_HTTPS_EXT.1 | Failure to establish a HTTPS Session | Reason for failure |
| FCS_NTP_EXT.1 | • Configuration of a new time server<br>• Removal of configured time server | • Identity if new/removed time server |
| FCS_RBG_EXT.1 | None | None |
| FCS_TLSC_EXT.1 | Failure to establish a TLS Session | Reason for failure |
| FCS_TLSS_EXT.1 | Failure to establish a TLS Session | Reason for failure |
| FIA_AFL.1 | Unsuccessful login attempts limit is met or exceeded | Origin of the attempt (e.g., IP address) |
| FIA_PMG_EXT.1 | None | None |
| FIA_UIA_EXT.1 | All use of identification and authentication mechanism | Origin of the attempt (e.g., IP address) |
| FIA_UAU_EXT.2 | All use of identification and authentication mechanism | Origin of the attempt (e.g., IP address) |
| FIA_UAU.7 | None | None |
| FIA_X509_EXT.1/Rev | • Unsuccessful attempt to validate a certificate<br>• Any addition, replacement or removal of trust anchors in the TOE's trust store | • Reason for failure of certificate validation<br>• Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store |
| FIA_X509_EXT.2 | None | None |
| FIA_X509_EXT.3 | None | None |
| FMT_MOF.1/ManualUpdate | Any attempt to initiate a manual update | None |
| FMT_MTD.1/CoreData | All management activities of TSF data | None |
| FMT_MTD.1/CryptoKeys | None | None |
| FMT_SMF.1 | None | None |
| FMT_SMR.2 | None | None |
| FPT_SKP_EXT.1 | None | None |
| FPT_APW_EXT.1 | None | None |
| FPT_TST_EXT.1 | None. | None. |

| Requirement | Auditable Events | Additional Audit Record Contents |
|---|---|---|
| FPT_STM_EXT.1 | Discontinuous changes to time - either Administrator actuated or changed via an automated process<br>(Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1) | For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address). |
| FPT_TUD_EXT.1 | Initiation of update; result of the update attempt (success or failure) | None |
| FTA_SSL.3 | The termination of a remote session by the session locking mechanism | None |
| FTA_SSL.4 | The termination of an interactive session | None |
| FTA_SSL_EXT.1 (if "lock the session" is selected) | Any attempts at unlocking of an interactive session | None |
| FTA_SSL_EXT.1 (if "terminate the session" is selected) | The termination of a local session by the session locking mechanism | None |
| FTA_TAB.1 | None | 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/Admin | • Initiation of the trusted path<br>• Termination of the trusted path.<br>• Failure of the trusted path functions. | None |

#### 5.2.1.2 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.

#### 5.2.1.3 FAU_STG_EXT.1 Protected Audit Event 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 according to FTP_ITC.1.

**FAU_STG_EXT.1.2**
The TSF Shall be able to store generated audit data on the TOE itself. In addition [selection:

- *The TOE shall consist of a single standalone component that stores audit data locally,*

].

**FAU_STG_EXT.1.3**
The TSF shall [*drop new audit data*] when the local storage space for audit data is full.

#### 5.2.1.4 FAU_STG_EXT.3/LocSpace Action in Case of Possible Audit Data Loss

**FAU_STG_EXT.3.1/LocSpace**
The TSF shall *generate a warning to inform the Administrator* before the audit trail *exceeds the local audit trail storage capacity*.

### 5.2.2 Cryptographic Support (FCS)

#### 5.2.2.1 FCS_CKM.1 Cryptographic Key Generation

**FCS_CKM.1.1**
The TSF shall generate **asymmetric** cryptographic key in accordance with a specified cryptographic key generation algorithm: [selection:

- *ECC schemes using "NIST curves" [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;*

] ~~and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].~~

#### 5.2.2.2 FCS_CKM.2 Cryptographic Key Establishment

**FCS_CKM.2.1**
The TSF shall **perform** cryptographic **key establishment** in accordance with a specified cryptographic key **establishment** method: [selection:

- *Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";*

] ~~that meets the following: [assignment: list of standards].~~

**Application Note:** This SFR has been updated as per TD0580 and TD0581

#### 5.2.2.3 FCS_CKM.4 Cryptographic Key Destruction

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

- *For plaintext keys in volatile storage, the destruction shall be executed by a [single overwrite consisting of [zeroes]], destruction of reference to the key directly followed by a request for garbage collection];*
- *For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [:*
    - *logically addresses the storage location of the key and performs a [single] overwrite consisting of [zeroes];*

that meets the following: *No Standard*

#### 5.2.2.4 FCS_COP.1/DataEncryption Cryptographic Operations (AES Data Encryption/Decryption)

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

#### 5.2.2.5 FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)

**FCS_COP.1.1/SigGen**
The TSF shall perform *cryptographic signature services (generation and verification)* in accordance with a specified cryptographic algorithm [selection:

- *RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [2048 bits]*
- *Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [256 bits]*

]
that meet the following: [selection:

- *For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,*
- *For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [P-256]; ISO/IEC 14888-3, Section 6.4*

].

#### 5.2.2.6 FCS_COP.1/Hash Cryptographic Operations (Hash Algorithm)

**FCS_COP.1.1/Hash**
The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm [*SHA-1, SHA-256, SHA-384, SHA-512*] ~~and cryptographic key sizes~~ [~~*assignment: cryptographic key sizes*~~] and **message digest sizes [*160, 256, 384, 512*] bits** that meet the following: *ISO/IEC 10118-3:2004*.

#### 5.2.2.7 FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)

**FCS_COP.1.1/KeyedHash**
The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [ *HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384*] and cryptographic key sizes *[160-bits, 256-bits, 384 bits]* **and message digest sizes [*160, 256, 384*] bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*.

#### 5.2.2.8 FCS_HTTPS_EXT.1 HTTPS Protocol

**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 the HTTPS protocol using TLS.

**FCS_HTTPS_EXT.1.3**
If a peer certificate is presented, the TSF shall [*not establish the connection*] if the peer certificate is deemed invalid.

#### 5.2.2.9 FCS_NTP_EXT.1 NTP Protocol

**FCS_NTP_EXT.1.1**
The TSF shall use only the following NTP version(s) [*NTP v4 (RFC 5905)*].

**FCS_NTP_EXT.1.2**
The TSF shall update its system time using [selection:

- Authentication using [*SHA1*] as the message digest algorithm(s);

].

**FCS_NTP_EXT.1.3**
The TSF shall not update NTP timestamp from broadcast and/or multicast addresses.

**FCS_NTP_EXT.1.4**
The TSF shall support configuration of at least three (3) NTP time sources in the Operational Environment.

#### 5.2.2.10 FCS_RBG_EXT.1 Random Bit Generation

**FCS_RBG_EXT.1.1**
The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 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 [*[one] platform-based noise source*] 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.

#### 5.2.2.11 FCS_TLSC_EXT.1 TLS Client Protocol without Mutual Authentication

**FCS_TLSC_EXT.1.1**
The TSF shall implement [*TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)*] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

[selection:

- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*

*] and no other ciphersuites.*

**FCS_TLSC_EXT.1.2**
The TSF shall verify that the presented identifier matches [ *the reference identifier per RFC 6125 section 6, IPv4 address in CN or SAN*].

**FCS_TLSC_EXT.1.3**
When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [selection:

- *Not implement any administrator override mechanism*

*].*

**FCS_TLSC_EXT.1.4**
The TSF shall [*present the Supported Elliptic Curves/Supported Groups Extension with the following curves/groups:* [*secp256r1, secp384r1, secp521r1*] *and no other curves/groups*]] in the Client Hello.

#### 5.2.2.12 FCS_TLSS_EXT.1 TLS Sever Protocol Without Mutual Authentication

**FCS_TLSS_EXT.1.1**
The TSF shall implement [*TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)*] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

[selection:

- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*

*] and no other ciphersuites.*

**FCS_TLSS_EXT.1.2**
The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [*none*].

**FCS_TLSS_EXT.1.3**
The TSF shall perform key establishment for TLS using [*ECDHE curves* [*secp256r1, secp384r1, secp521r1*] *and no other curves*]].

**FCS_TLSS_EXT.1.4**
The TSF shall support [*no session resumption or session tickets*].

### 5.2.3 Identification and Authentication (FIA)

#### 5.2.3.1 FIA_AFL.1 Authentication Failure Management

**FIA_AFL.1.1**
The TSF shall detect when an Administrator configurable positive integer within *[1-999]* unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely using a password*.

**FIA_AFL.1.2**
When the defined number of unsuccessful authentication attempts has been met, the TSF shall [*prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until [account unlock] is taken by an Administrator]*.

#### 5.2.3.2 FIA_PMG_EXT.1 Password Management

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

*a)* Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [*"!", "@", "#", "$", "%", "^", "&", "*", "(", ")", [" ", "\"", "'", "+", ",", "-", ".", "/", ":", ";", "<", "=", ">", "?", "@", "[", "\", "]", "_", "`", "{", "|", "}", "~"]*]

*b)* Minimum password length shall be configurable to between [*8*] and [*16*] characters.

#### 5.2.3.3 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;
- [*automated generation of cryptographic keys*].

**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.

#### 5.2.3.4 FIA_UAU_EXT.1 Password-based Authentication Mechanism

**FIA_UAU_EXT.2.1**
The TSF shall provide a local [*password-based*] authentication mechanism to perform local administrative user authentication.

#### 5.2.3.5 FIA_UAU.7.1 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**.

#### 5.2.3.6 FIA_X509_EXT.1/Rev X.509 Certificate Validation

**FIA_X509_EXT.1.1/Rev**
The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation **supporting a minimum path length of three certificates** .
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [*the Online Certificate Status Protocol (OCSP) as specified in RFC 6960*].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.*
  - *Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
  - *Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*
  - *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

**FIA_X509_EXT.1.2/Rev**
The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

#### 5.2.3.7 FIA_X509_EXT.2 X.509 Certificate Authentication

**FIA_X509_EXT.2.1**
The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [*HTTPS, TLS*] and [no *additional uses*].

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

**Application Note:** This SFR has been updated as per TD0537.

#### 5.2.3.8 FIA_X509_EXT.3 X.509 Certificate Requests

**FIA_X509_EXT.3.1**
The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [*device-specific information, Common Name, Organization, Organizational Unit, Country*].

**FIA_X509_EXT.3.2**
The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

### 5.2.4 Security Management (FMT)

#### 5.2.4.1 FMT_MOF.1/ManualUpdate Management of Security Functions Behavior

**FMT_MOF.1.1/ManualUpdate**
The TSF shall restrict the ability to enable the function *to perform manual updates to Security Administrators*.

#### 5.2.4.2 FMT_MOF.1/Services Management of Security Functions Behaviour

**FMT_MOF.1.1/Services**
The TSF shall restrict the ability to **start and stop** ~~the functions~~ **services** to *Security Administrators*.

#### 5.2.4.3 FMT_MTD.1/CoreData Management of TSF Data

**FMT_MTD.1.1/CoreData**
The TSF shall restrict the ability to manage the *TSF data to Security Administrators.*

#### 5.2.4.4 FMT_MTD.1/CryptoKeys Management of TSF Data

**FMT_MTD.1.1/CryptoKeys**
The TSF shall restrict the ability to *manage* the *cryptographic keys* to *Security Administrators*.

#### 5.2.4.5 FMT_SMF.1 Specification of Management Functions

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

- *Ability to administer the TOE locally and remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using [selection: digital signature, hash comparison] capability prior to installing those updates;*
- *Ability to configure the authentication failure parameters for FIA_AFL.1;*
- [
    - *Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;*
    - *Ability to manage the cryptographic keys;*
    - *Ability to configure the cryptographic functionality;*
    - *Ability to re-enable an Administrator account;*
    - *Ability to set the time which is used for time-stamps;*
    - *Ability to configure NTP;*
    - *Ability to configure the reference identifier for the peer;*
    - *Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;*
    - *Ability to import X.509v3 certificates to the TOE's trust store;*
    - ].

#### 5.2.4.6 FMT_SMR.2 Restrictions on Security Roles

**FMT_SMR.2.1**
The TSF shall maintain the roles:

- *Security 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

- *The Security Administrator role shall be able to administer the TOE locally;*
- *The Security Administrator role shall be able to administer the TOE remotely;*

are satisfied.

### 5.2.5 Protection of the TSF (FPT)

#### 5.2.5.1 FTP_APW_EXT.1 Protection of Administrator Passwords

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

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

#### 5.2.5.2 FPT_SKP_EXT.1 Protection of TSF Data (for reading of all pre-shared, symmetric, and private keys)

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

#### 5.2.5.3 FPT_STM_EXT.1 Reliable Time Stamps

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

**FPT_STM_EXT.1.2**
The TSF shall [*allow the Security Administrator to set the time, synchronise time with an NTP server*].

#### 5.2.5.4 FPT_TST_EXT.1 TSF Testing

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

- *File system checks*
- *SHA-256 Software integrity checks*
- *Cryptographic algorithm known answer tests*
- *Cryptographic algorithm pairwise consistency test*
- *Health test of the noise source*].

#### 5.2.5.5 FPT_TUD_EXT.1 Trusted Update

**FPT_TUD_EXT.1.1**
The TSF shall provide *Security Administrators* the ability to query the currently executing version of the TOE firmware/software and [*no other TOE firmware/software version*].

**FPT_TUD_EXT.1.2**
The TSF shall provide *Security Administrators* the ability to manually initiate updates to TOE firmware/software and [*no other update mechanism*].

**FPT_TUD_EXT.1.3**
The TSF shall provide means to authenticate firmware/software updates to the TOE using a [*digital signature*] prior to installing those updates.

### 5.2.6 TOE Access (FTA)

#### 5.2.6.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

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

- *terminate the session*]

after a Security Administrator-specified time period of inactivity

#### 5.2.6.2 FTA_SSL.3 TSF-initiated Termination

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

#### 5.2.6.3 FTA_SSL.4 User-initiated Termination

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

#### 5.2.6.4 FTA_TAB.1 Default TOE Access Banners

**FTA_TAB.1.1**
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.

### 5.2.7 Trusted Path/Channels (FTP)

#### 5.2.7.1 FTP_ITC.1 Inter-TSF Trusted Channel

**FTP_ITC.1.1**
The TSF shall **be capable of using [ *TLS*] to** provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [*authentication 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**
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 *[audit server, authentication server]*.

#### 5.2.7.2 FTP_TRP.1/Admin Trusted Path

**FTP_TRP.1.1/Admin**
The TSF shall **be capable of using [*TLS*] to** provide a communication path between itself and **authorized** 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 provides detection of modification of the channel data**.

**FTP_TRP.1.2/Admin**
The TSF shall permit remote **Administrators** to initiate communication via the trusted path.

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

## 5.3 TOE SFR Dependencies Rationale for SFRs

The PP and any relevant EPs/Modules/Packages contain(s) all the requirements claimed in this ST. As such, the dependencies are not applicable since the PP has been approved.

## 5.4 Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from the PP and any relevant EPs/Modules/Packages, which is/are derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in Table .

**Table 12 – Security Assurance Requirements**

| Assurance Class | Assurance Components | 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 functionality specification |
| Guidance Documents | AGD_OPE.1 | Operational user guidance |
| | AGD_PRE.1 | Preparative Procedures |
| Life Cycle Support | ALC_CMC.1 | Labelling of the TOE |
| | ALC_CMS.1 | TOE CM coverage |
| Tests | ATE_IND.1 | Independent testing – conformance |
| Vulnerability Assessment | AVA_VAN.1 | Vulnerability survey |

## 5.5 Assurance Measures

The TOE satisfied the identified assurance requirements. This section identifies the Assurance Measures applied by Progress Software Corporation to satisfy the assurance requirements. The following table lists the details.

**Table 13 – TOE Security Assurance Measures**

| SAR Component | How the SAR will be met |
|---|---|
| ADV_FSP.1 | The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes). |
| AGD_OPE.1 | The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance. |

| SAR Component | How the SAR will be met |
|---|---|
| AGD_PRE.1 | The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration. |
| ALC_CMC.1 | The Configuration Management (CM) documents describe how the consumer identifies the evaluated TOE. The CM documents identify the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked and how potential changes are incorporated. |
| ALC_CMS.1 | |
| ATE_IND.1 | Vendor will provide the TOE for testing. |
| AVA_VAN.1 | Vendor will provide the TOE for testing.<br>Vendor will provide a document identifying the list of software and hardware components. |

# 6 TOE Summary Specification

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

**Table 14 – TOE Summary Specification SFR Description**

| SFR | Rationale |
|---|---|
| FAU_GEN.1<br>FAU_GEN.2 | The TSF generates audit records for the auditable events specified in Table 11 as well as the following:<br>• Startup and shut-down of the audit function<br>• Generation/importing, changing, or deleting certificates and cryptographic keys. The TSF identifies the certificate or key being operated on by including the following in the audit record:<br>○ Generated Keys:<br>▪ CSRs: X.509 Subject associated with the key<br>▪ Self-Signed Cert: hostname (in the CN)<br>○ Uploaded/Imported Keys: uploaded filename or certificate name.<br>○ For changing, and deleting of certificates and associated keys, the TOE logs the certificate name.<br><br>Each of the events is specified in the audit record is in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. |
| FAU_STG_EXT.1 | The TSF transmits generated audit data to an external server using the TLS trusted channel specified in FTP_ITC.1. The TSF sends audit records to the external server as the audit records are generated. The TSF does not retransmit audit logs that were generated while the connection to the audit server was down.<br><br>The TOE is a standalone TOE.<br><br>When local audit storage is exhausted, the TSF will not record new events **locally** until additional space is available. **Records are still transmitted to the remote syslog endpoint, and so the audit trail is preserved. Local audit records** will be temporarily stored in a buffer until they can be stored. The TSF allows all available space to be used to store audit records. For the Virtual Load Master that is up to 7GB. The HW Load Master models have up to 25GB of space available to store audit records.<br><br>The TSF prevents unauthorized users from modifying or deleting audit records. |
| FAU_STG_EXT.3/LocSpace | The TSF generates a log when audit storage reaches 85% of capacity to inform the administrator that audit storage is nearing capacity.<br><br>The **Disk Usage** under **System Configuration > System Administration > System Log Files** provides a visual indication of the percentage used/free of the log partition. Color coding is also used to highlight different usage levels:<br>• 0% to 50%: green<br>• 50% to 90%: orange<br>• 90% to 100%: red |
| FCS_CKM.1 | The TSF generates P-256 ECDSA keys for the administrative UI (HTTPS). |

<table>
<tr><th>SFR</th><th>Rationale</th></tr>
<tr><td></td><td>The TSF generates P-256, P-384, and P-521 ECDH for the ECDHE key establishment used in TLS.<br><br>The relevant NIST CAVP certificate is listed in Table 15.</td></tr>
<tr><td>FCS_CKM.2</td><td>The TSF performs SP 800-56Ar2 compliant elliptic curve-based key establishment using curves P-256, P-384, and P-521 as part of the TLS handshake.<br><br>The relevant NIST CAVP certificates are listed in Table 15.</td></tr>
<tr><td>FCS_CKM.4</td><td>The TSF destroys keys in RAM by performing an overwrite with zeroes.<br><br>The TSF destroys keys stored in non-volatile memory by logically addressing the storage location and performing an overwrite with zeros. Once the overwrite is complete, the file storing the key is deleted. Please see Table 16 for an identification of cryptographic keys, storage locations, generation methods, and timing of zeroization.</td></tr>
<tr><td>FCS_COP.1/DataEncryption</td><td>The TSF performs AES encryption and decryption in CBC and GCM modes with 128 and 256-bit keys for TLS.<br><br>The relevant NIST CAVP certificate is listed in Table 15.</td></tr>
<tr><td>FCS_COP.1/SigGen</td><td>The TSF performs RSA 2048 signature verification to verify the integrity and authenticity of updates.<br><br>The TSF performs ECDSA P-256 signature generation and verification as part of TLS.<br><br>The relevant NIST CAVP certificate is listed in Table 15.</td></tr>
<tr><td>FCS_COP.1/Hash</td><td>The TSF performs SHA-1, SHA-256, SHA-384, and SHA-512 hashing.<br><br>Hashing of are used for the following security functions:<ul><li>NTP – SHA-1</li><li>Digital Signature generation and verification – SHA-256</li><li>File Integrity Checking – SHA-256</li><li>Password Hashing – SHA-512</li><li>HMAC primitive – SHA-1, SHA-256, SHA-384</li></ul>The relevant NIST CAVP certificate is listed in Table 15.</td></tr>
<tr><td>FCS_COP.1/KeyedHash</td><td>The TSF uses the following HMAC algorithms in TLS:<table><tr><th>Algorithm</th><th>Hash Function</th><th>Block Size</th><th>Key Size</th><th>Digest Size</th></tr><tr><td>HMAC-SHA-1</td><td>SHA-1</td><td>512 bits</td><td>160 bits</td><td>160 bits</td></tr><tr><td>HMAC-SHA-256</td><td>SHA-256</td><td>512 bits</td><td>256 bits</td><td>256 bits</td></tr><tr><td>HMAC-SHA-384</td><td>SHA-384</td><td>1024 bits</td><td>384 bits</td><td>384 bits</td></tr></table>The relevant NIST CAVP certificate is listed in Table 15.</td></tr>
<tr><td>FCS_RBG_EXT.1</td><td>The TSF implements an SP 800-90A CTR_DRBG using AES-256. The DRBG is seeded with at least 256-bits of entropy from a third-party hardware entropy source.<br><br>The relevant NIST CAVP certificate is listed in Table 15.</td></tr>
</table>

| SFR | Rationale |
|---|---|
| FCS_HTTPS_EXT.1 | The TSF acts as an HTTPS server to secure administrative connections to the WUI. The TSF implements HTTPS as specified in RFC 2818 using TLS as specified in FCS_TLSS_EXT.1 .<br><br>The TOE's HTTPS protocol complies with RFC 2818. The TOE implements all "MUST", "REQUIRED", and "SHOULD" statements from the RFC 2818 that are applicable to a HTTP server. The TOE web GUI operates on an explicit TCP port designed to natively implement TLS. The web server attempts to send closure Alerts prior to closing a connection in accordance with section 2.2.2 of RFC 2818. |
| FCS_NTP_EXT.1 | The TSF supports time updates using NTPv4. The TSF authentications updates using an administrator configured symmetric key and SHA-1. The TOE rejects broadcast and multicast time updates. The TOE allows up to 10 NTP time sources to be configured. |
| FCS_TLSC_EXT.1 | The TSF is a TLS client for securing communications with Syslog and LDAP servers. The TSF supports TLSv1.2 and TLSv1.1 with the following ciphersuites:<br>• TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA<br>• TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA<br>• TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256<br>• TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384<br>• TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256<br>• TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384<br>The TSF supports the following identifier types:<br>• DNS name in the SAN or CN. Wildcards are supported in the left-most position.<br>• IPv4 address in the SAN or CN.<br><br>The TSF only checks the identifier in the CN if the SAN extension is not present. The TSF does not support SRV or URI identifiers.<br><br>The reference identifier for external IT devices are configured by the administrator using the available administrative commands in the CLI. The reference identifiers must be an IPv4 address or a hostname.<br><br>When the reference identifier is a hostname, the TOE compares the hostname against all the DNS Name entries in the Subject Alternative Name (SAN) extension. If the hostname does not match any of the DNS Name entries, then the verification fails. If the certificate does not contain any DNS Name entries in SAN, the TOE will compare the hostname against the Common Name (CN). If the hostname does not match the CN, then the verification fails. For both DNS Name and CN matching, the hostname must be an exact match or wildcard match. In the case of a wildcard match, the wildcard must be the left-most component, wildcard matches a single component, and there are at least two non-wildcard components.<br><br>When the reference identifier is an IP address, the TOE converts the IP address to a binary representation in network byte order. IPv4 addresses are converted directly from decimal to binary with period "." serving as the delineator. The TOE compares the binary IP address against all the IP Address entries in the Subject Alternative Name extension. If there is not an exact binary match, then the verification fails. If the SAN entry is missing, the TOE will compare the IPv4 |

| SFR | Rationale |
|---|---|
| | address against the Common Name (CN). If the IPv4 address in CN is not an exact binary match, then the verification fails. For IPv4 address in SAN or CN matching, the IPv4 address must be an exact binary match.<br>The TLS channel is terminated if verification fails.<br><br>SAN is prioritized over CN. The TOE does not enforce canonical format.<br><br>The TLS client will transmit the Supported Elliptic Curves extension in the Client Hello message by default with support for the following NIST curves: secp256r1, secp384r1, and secp521r1. |
| FCS_TLSS_EXT.1 | The TSF is an HTTPS/TLS server for providing the WUI trusted channel to remote administrators. The TSF supports TLSv1.2 and TLSv1.1 with the following ciphersuites:<br>• TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA<br>• TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA<br>• TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256<br>• TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384<br>• TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256<br>• TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384<br>The TSF rejects the connection if the client attempts to establish a connection using an older version of TLS or SSL.<br>The TSF will perform ECDHE key establishment using secp256r1, secp384r1, and secp521r1. If the client did not propose one of these curves, the connection fails.<br>The TSF does not support session resumption or session tickets. |
| FIA_AFL.1 | The TSF blocks remote authentication attempts after a configurable number of failed attempts (both password and cert-based attempts). The security administrator can configure the threshold to be from 1 through 999. Once an account is locked, the account must be unlocked using the “bal” account through the WUI. The administration of the TSF is always possible, because the TSF never locks the local console. |
| FIA_PMG_EXT.1 | The TSF allows administrators passwords to be composed of any printable ASCII character (i.e. 0x20-0x7E inclusive).<br>The TSF allows the security administrator to configure the minimum password length to be 8-16 characters. |
| FIA_UIA_EXT.1 | Prior to authentication, the TSF only allows users to display the warning banner and automatically generate keys on a new system.<br>Authentication is based on username/password for the web interface and local console. The TOE does not expose any interface, through any access method prior to successful login. |
| FIA_UAU_EXT.2 | The TSF uses a username and password to authenticate administrative users at the local console. |
| FIA_UAU.7 | The TSF does not echo any characters back when passwords are typed at the local console. |
| FIA_X509_EXT.1/Rev | The TOE performs X.509 certificate validation at the following points: |

| SFR | Rationale |
|---|---|
| | • TOE TLS client authentication of server X.509 certificates;<br>• When certificates are loaded into the TOE, such as when importing Cas and certificate responses.<br>In all scenarios, certificates are checked for several validation characteristics:<br>• If the certificate 'notAfter' date is in the past, then this is an expired certificate which is considered invalid;<br>• The certificate chain must terminate with a certificate designated as a trust anchor on the TOE;<br>• All certificates not designated as trust anchors must not be revoked, as indicated by an OCSP status check;<br>• All trust anchor and intermediate certificates must contain the basicConstraints extension and have the CA flag set to TRUE.<br>• Server certificates consumed by the TOE TLS client must have a 'serverAuthentication' extendedKeyUsage purpose;<br>• Client certificates consumed by the TOE TLS server must have a 'clientAuthentication' extendedKeyUsage purpose;<br>• Certificates used to sign OCSP responses must have the OCSP signing purpose in the extendedKeyUsage extension. |
| FIA_X509_EXT.2 | As a TLS Client, the TOE uses OCSP to determine whether the certificate is revoked or not.<br>When the TSF does not receive a response from an OCSP server, by default, the TSF rejects the certificate. The administrator can configure the TSF to accept certificates when an OCSP response is not received. |
| FIA_X509_EXT.3 | The TSF is capable of generating certificate signing request that contain the public key, device specific information (e.g. email address, requested SAN name), Common Name, Organization, Organizational Unit, Country |
| FMT_MOF.1/ManualUpdate | The TSF allows the security administrator to initiate manual updates to the TOE software. |
| FMT_MTD.1/CoreData | The TSF displays a warning banner prior to user authentication. There are no administrative functions available for unauthorized users. All administrators must be authenticated and authorized to perform any activity that can alter TSF data.<br>The TSF restricts the ability to manage TSF data to security administrators. |
| FMT_MTD.1/CryptoKeys | The TSF allows the security administrator to generate cryptographic keys associated with the TSF's self-signed web server certificate or Certificate Signing Requests. |
| FMT_SMF.1 | The TSF supports local (Console) and remote (WUI) administrative interfaces.<br>The following management functions are available at the Console:<br>• Manage cryptographic keys<br>The following management functions are available via the WUI:<br>• Configure the access banner<br>• Configure the session inactivity timer<br>• Initiate manual updates |

| SFR | Rationale |
|---|---|
| | • Managed cryptographic keys<br>• Configure TLS versions and ciphersuites<br>• Set the time<br>• Configure NTP<br>• Configure the reference identifier for the Syslog and LDAP servers<br>• Manage the X.509 certificate trust store<br>• Import X.509 certificates into the trust store. |
| FMT_SMR.2 | The TSF supports a bal account (superuser) and administrator accounts. Both account types belong to the Security Administrator role. |
| FPT_SKP_EXT.1 | The TSF prevents reading symmetric and private keys. The private TLS certificate keys are protected through UI restrictions that prevent the security administrators from reading the keys. All other symmetric and private keys are only held in RAM and can only be accessed by the processes performing TLS. The TSF does not utilize pre-shared keys. |
| FPT_APW_EXT.1 | The TSF stores administrative passwords protected by a SHA-512 hash. |
| FPT_TST_EXT.1 | The TSF performs the following tests at power-up:<br>• File systems checks<br>During boot up the TSF checks file system by verifying the metadata and that it is mounted correctly<br>• SHA-256 Software integrity checks<br>The TSF generates a SHA-256 has of the firmware image and compares it with the stored value<br>• Cryptographic algorithm known answer tests<br>For each cryptographic algorithm, the TSF performs a sample cryptographic operation using know values and compares the output with the expected value<br>• Cryptographic algorithm pairwise constancy test<br>For each cryptographic algorithm with a key-pair, the TSF performs a sample operation using know value and compares the output with the corresponding key-pair<br>• Health test of the noise source<br>This is a continuous health-test that checks the number of occurrences of 6 different bit patterns in each 256-bit output from the noise source. It checks if any of the pattern counts are outside of predetermined thresholds. If more than 128 of the most recent 256 256-bit samples fails, the Entropy Source cease to output data<br><br>If any of the tests fail, the TSF disables the affected functionality or halts. The TSF will boot with cryptographic service disabled if the known answer tests, pairwise consistency test, or noise source health test fail. |
| FPT_TUD_EXT.1 | The TSF allows the Security Administrator to query the currently running version of software. The TSF also allows the Security Administrator to initiate software updates. Prior to installing an update, the TSF verifies an RSA 2048 signature on the update to ensure the update is authentic. |

| SFR | Rationale |
|---|---|
| FPT_STM_EXT.1 | The TSF maintains the date and time using the clock provided by the underlying hardware. This date and time is used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions. The time can be manually updated by a Security Administrator or automatically updated using NTP synchronization. |
| FTA_SSL_EXT.1 | The TSF terminates local sessions after 1-1440 minutes of inactivity. |
| FTA_SSL.3 | The TSF terminates remote sessions after 60-86400 seconds of inactivity. |
| FTA_SSL.4 | The TSF allows the administrator to terminate the administrator's own local and remote interactive sessions. |
| FTA_TAB.1 | The TSF displays a configurable message before establishing a local or remote administrative session. |
| FTP_ITC.1 | The TSF provides a trusted channel with the Syslog server and LDAP server as described in FCS_TLSC_EXT.1. |
| FTP_TRP.1/Admin | The TSF provides a trusted path with remote administrators using TLS/HTTPS as described in FCS_TLSS_EXT.1, and FCS_HTTPS_EXT.1. |

## 6.1 CAVP Algorithm Certificate Details

Each of these cryptographic algorithms have been validated as identified in the table below.

**Table 15 – CAVP Algorithm Certificate References**

| Algorithm | CAVP Cert. | Standard | Operation/Use | SFR |
|---|---|---|---|---|
| RSA | C2076 | FIPS 186-4 | RSA 2048 SigVer | FCS_CKM.1 |
| ECDSA | C2076 | FIPS 186-4 | ECDSA P-256 SigGen, SigVer<br>ECDSA P-256, P-384, P-521 KeyGen, PKV | FCS_CKM.1<br>FCS_COP.1/SigGen |
| ECDHE | C2076 | SP 800-56Ar2 | ECDHE P-256, P-384, P-521 | FCS_CKM.2 |
| DRBG | C2076 | SP 800-90Ar1 | CTR_DRBG(AES-256) | FCS_RBG_EXT.1 |
| AES | C2076 | FIPS 197<br>SP 800-38A<br>SP 800-38D | AES in CBC and GCM modes with 128-bit and 256-bit keys | FCS_COP.1/Data Encryption |
| SHA | C2076 | FIPS 180-4 | SHA-1, SHA-256, SHA-384, SHA-512 | FCS_COP.1/Hash |
| HMAC | C2076 | FIPS 198-1 | HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 | FCS_COP.1/KeyedHash |

## 6.2 Cryptographic Key Destruction

The table below describes the key zeroization provided by the TOE and as referenced in FCS_CKM.4.

**Table 16 – Cryptographic Key Destruction**

| Key | Type | Origin | Storage/Protection | Zeroization |
|---|---|---|---|---|
| EC Diffie-Hellman Key | Private ECDH P-256, P-384, or P-521 | TOE generated | RAM | Keys are overwritten with zeros when session closes |
| TLS Private Key | Private ECDSA P-256 | TOE generated | Restricted Filesystem access | Zeroize command |
| TLS Encryption Key | 128-bit or 256-bit AES | TOE generated | RAM | Keys are overwritten with zeros when session closes |
| TLS Integrity Key | HMAC-SHA-1, HMAC-SHA-256, or HMAC-SHA-384 | TOE generated | RAM | Keys are overwritten with zeros when session closes |

# 7 Acronym Table

**Table 17 – Acronyms**

| Acronym | Definition |
|---|---|
| **AES** | Advanced Encryption Standard |
| **CC** | Common Criteria |
| **CRL** | Certificate Revocation List |
| **DTLS** | Datagram Transport Layer Security |
| **EP** | Extended Package |
| **GUI** | Graphical User Interface |
| **IP** | Internet Protocol |
| **NDcPP** | Network Device Collaborative Protection Profile |
| **NIAP** | Nation Information Assurance Partnership |
| **NTP** | Network Time Protocol |
| **OCSP** | Online Certificate Status Protocol |
| **OSP** | Organizational Security Policy |
| **PP** | Protection Profile |
| **RSA** | Rivest, Shamir & Adleman |
| **SFR** | Security Functional Requirement |
| **SSH** | Secure Shell |
| **ST** | Security Target |
| **TOE** | Target of Evaluation |
| **TLS** | Transport Layer Security |
| **TSS** | TOE Summary Specification |
| **WUI** | Web User Interface |