Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms Security Target

Document Version: 1.3

Document Date: 11 March 2024

7035 Ridge Rd,
Hanover, MD 21076

2400 Research Blvd
Suite 395
Rockville, MD 20850

Revision History

Version	Date	Changes
Version 0.1	December 17, 2021	Initial Release
Version 0.2	January 31, 2021	Updated based on vendor responses
Version 0.3	February 14, 2022	Additional comments based on responses
Version 0.4	February 27, 2022	Updated requirements with additional comments
Version 0.5	March 04, 2022	Updated based on vendor responses
Version 0.6	March 16, 2022	Updated TSS based on vendor responses
Version 0.7	April 26, 2022	Confirmed TSS information with vendor.
Version 0.8	N/A	Internal only revision
Version 0.9	February 05, 2023	Removed TLS server and TLS mutual authentication
Version 0.10	April 13, 2023	Reviewed ST, made corrections, added three new appliances.
Version 0.11	April 15, 2023	Removed the new appliances.
Version 0.12	May 11, 2023	Added new appliances.
Version 0.13	May 17, 2023	Vendor mods.
Version 0.14	June 15, 2023	Addressed ECRs
Version 0.15	September 08, 2023	Addressed ECRs
Version 0.16	September 19, 2023	Updated due to new EAR.
Version 0.17	December 1, 2023	Update due to new TDs, removed RADsec, & modified TOE ID.
Version 0.18	December 15, 2023	• Removed secure channels to NTP and OCSP. Affected FTP_ITC.1.1, FTP_ITC.1.3, FTP_ITC.1 TSS, Figure 1, Table 3, and various sections of the document. • Removed RFC 8308 section 3.1 and RFC 8332 from FCS_SSHS_EXT.1.1. • Removed contradiction of CN and SAN accepted values in FCS_TLSC_EXT.1 TSS section. TSS now states FQDN are allowed in CN and SAN. IPv4 address allowed in SAN only. • Wildcard support went from not supported to supported in FCS_TLSC_EXT.1 TSS.
Version 0.19	January 02, 2024	• Removed TD0633
Version 1.0	January 25, 2024	• Modified FMT_SMF.1
Version 1.1	February 23, 2024	• Addressing validators ECR comments
Version 1.2	March 05, 2023	Addressing validators ECR comments
Version 1.3	March 11, 2023	Addressing validators ECR comments

Contents

1 Introduction

This document is a Security Target (ST) which provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms. The ST serves as the basis for the Common Criteria (CC) evaluation and identifies the TOE, the scope of the evaluation, and the assumptions made throughout. This ST also describes the intended operational environment of the TOE and states the security functional and assurance requirements that the TOE meets.

1.1 Security Target and TOE Reference

ST and TOE Identification is given in Table 1.

Table 1 TOE/ST Identification

Identifier	Value
ST Title	Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms Security Target
ST Version	1.3
ST Date	11 March 2024
ST Author	Acumen Security, LLC
TOE Identifier	Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms
TOE Software	Ciena SAOS 10.7.1
TOE Hardware	Ciena 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms
TOE Security Guidance	Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms CC Guidance Supplement, v1.3
TOE Developer	Ciena Corporation
Key Words	Network Device, Ciena, Encryption, SAOS

1.2 TOE Overview

The TOE is the Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms. It is a non-distributed, non-virtual network device which implements routing and switching functionalities for enterprise, mobility, and converged network architectures. In these architectures, the TOE can be deployed in the access, aggregation, or core of the network. The TOE uses a Linux based container architecture for its SAOS Network Operating System and includes the Ciena SAOS 10.7.1 operating system executed on the Ciena 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms. The technical characteristics of the platforms are described in Sect. 1.3.

The TOE implements the general functionality of a router/switch consistent with the collaborative Protection Profile for Network Devices v2.2E. The TOE implements controlled connectivity between two subnetworks and a management interface. All network traffic between the connected subnetworks is controlled by the TOE and the authorized administrators may manage the TOE using the management interface.

The management interface is a Command Line Interface (CLI) which may be accessed locally or remotely. Local access is via a console port which is a Serial EIA-561 (RJ-45) or a USB-C port. It allows management of the TOE from a workstation physically connected to the TOE. Remote management is over Secure Shell (SSH). SSH implements a secure remote login over a network connection and allows protected CLI.

All administrators are identified and authenticated using a username and password or based on SSH public key authentication. Access is only granted, and the user assigned to the role administrator upon successful authentication. Authentication is implemented locally. Authentication of TLS peers is done using X.509 Public Key Certificates. The validity of the X.509 public key certificates is verified using the Online Certificate Status Protocol (OCSP). TLS and Hypertext Transfer Protocol Security (HTTPS) may also be used for secure file transfer to and from the outside of the TOE.

In addition to the management ports for local and remote access by the administrators, the variants of the TOE also implement a different number of network ports for the interconnection of different subnetworks (see Sect. 1.3). The network ports are physically separate from the management ports and administrative access may not take place from the network interconnection ports.

The TOE does not protect the data flowing through itself. The TOE is only to be deployed in a secure data center and to only be physically accessible by trusted administrators. Administrators are trusted to operate the TOE in accordance with the security guidance at all times and not attempt to circumvent or suppress the security functions and mechanisms of the TOE.

1.3 TOE Description

The TOE is the Ciena SAOS 10.7.1 software executed on the Ciena 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms summarized in Table 2. The same software is executed on each platform. The various models of the TOE differ in performance and number of ports, but all run the same OS version 10.7.1 software. The TOE is available in two form factors:

1. a rack-mount appliance with a variable number of replaceable modules or ‘blades’, and
2. Large NFV Compute Server, a field-replaceable unit (FRU) housed in the 3926

Table 2 TOE Hardware Platforms

Models/Platform	1G/10G SFP+	Processors	100G	Power Options
3926	6	4x1.5GHz ARM Cortex A53	--	AC, DC
3928	4	4x1.5 GHz ARM Cortex A53	--	AC, DC
3948	4	4x1.5 GHz ARM Cortex A53	--	AC, DC
5144	8	4x2GHz ARM Cortex A72	--	AC, DC
5164	32x[1G/10G/25G]	4x2GHz ARM Cortex A72	4x [100G/ 200G]	AC, DC
5162	40	Intel XEON D1527, 4CORE	2	AC, DC
5170	4x 25G/10G/1G and 36x 10G/1G	Intel XEON D1527, 4CORE	4xQSFP28	AC, DC

Models/Platform	1G/10G SFP+	Processors	100G	Power Options
8180	--	Intel XEON D1527, 4CORE	32xQSFP28 FRU module options: 1xWLAi FRU and 4x100G CFP2-DCO	AC, DC
5171	4x 25G/10G/1G and 36x 10G/1G	Intel XEON D1539, 8CORE	FRU module options: 2x QSFP28, 1x QSFP28 + 1x 100G CFP2-DCO, 2x 100G CFP2-DCO, 1x200G CFP2-DCO	AC, DC
Large NFV compute server (FRU)	--	Intel XEON D1548, 8CORE	--	--

1.3.1 Physical Scope of the TOE

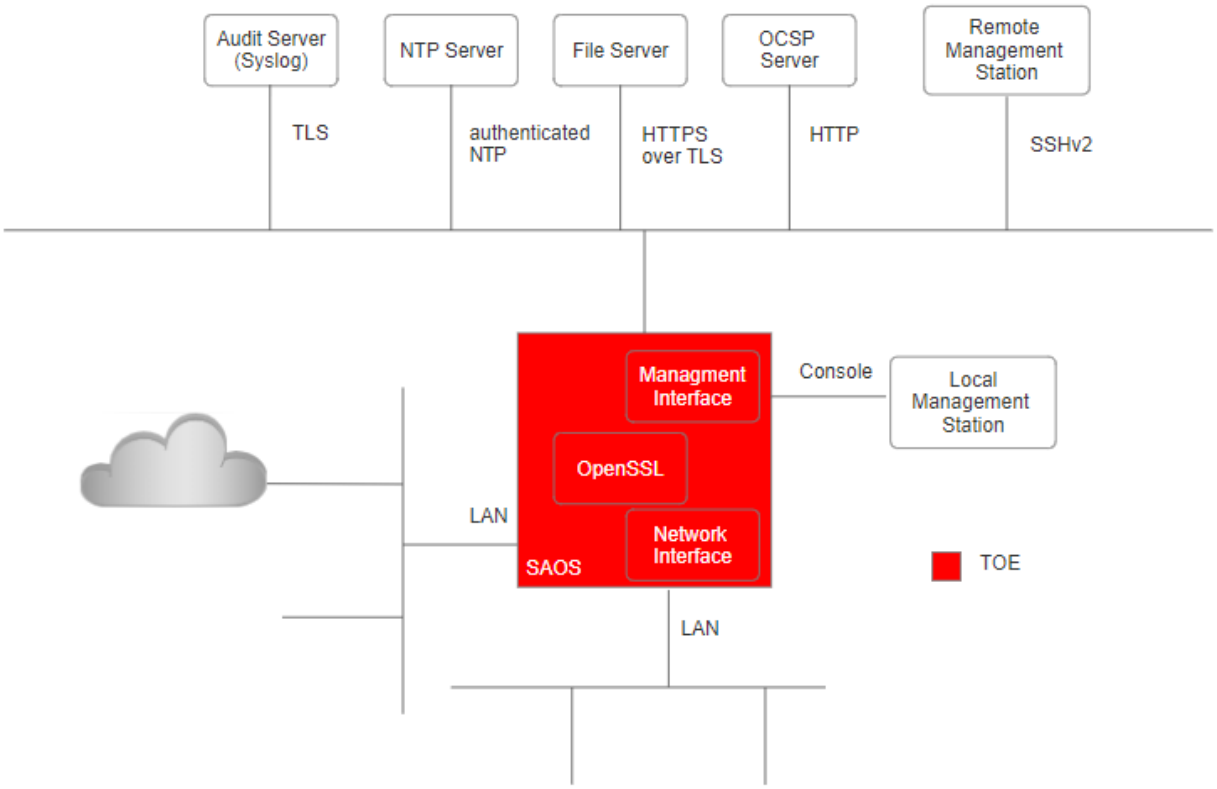
The TOE is the complete network appliance, or a Large NFV Compute Server comprised of TOE hardware, TOE software and TOE security guidance:

- TOE software is Ciena SAOS 10.7.1,
- TOE hardware is Ciena 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms, and
- TOE security guidance is:
  - *Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms CC Guidance Supplement,* v1.3.
  - *3948/513x/5144/516x/5170/811x Routers and Platforms, Security SAOS 10.7.1*, May 2022
  - *5162 Router, Installation*, November 2023
  - *D-NFVI Software, D-NFVI Installation*, D-NFVI 10.7.1, May 2022

The TOE is deployed in an environment that includes the IT components illustrated in the following figure. The TOE itself is delivered as an appliance or an FRU with the software installed. The administrator of the TOE may verify the TOE software and, if necessary, download and install the correct version.

The physical boundary of the TOE is illustrated below. Non-TOE components are summarized in Table 3. The TOE implements a TLS Client and SSH Server for secure connectivity to the components of the environment. Each component of the environment is required to implement the corresponding client and/or server. The remote management workstation is required to implement a SSH Client for accessing the TOE, and the audit server and File Server must include a TLS Server for which the TOE can connect using the TLS Client.

Figure 1: TOE Boundary and Operational Environment



1.3.2 Logical Scope of the TOE

The TOE is a non-distributed, non-virtual network device. It is a complete appliance or FRU which implements the security functions and mechanisms required by the *collaborative Protection Profile for Network Devices,* version 2.2E. The security functions and functions constitute the logical scope of the TOE as summarized in this section.

1.3.2.1 Security Audit

The TOE implements extensive auditing capabilities to allow legitimate administrators to examine the events that have occurred. Audit records are generated for all auditable events, including the starting and stopping of the audit service and each auditable event stated in Table 10. The TOE stores audit records locally and may be configured to export them to an external audit server using syslog over TLS. Each audit record contains the date and time of event, type of event, subject identity, and any other event-related relevant data.

1.3.2.2 Cryptographic Support

The TOE includes the OpenSSL v3.0.8 library which implements cryptographic functions and protocols for trusted paths and trusted channels. Specifically, the TOE implements SSH server and a TLS client for communication with trusted peer entities. Peer entity authentication for TLS is using X.509 public key certificates. Cryptographic algorithms are all Cryptographic Algorithm Validation Program (CAVP) validated. The validation certificate references are given in Table 14.

TLS v1.2 is used for protecting the transfer of syslog messages to an external Syslog server.

HTTPS over TLS is used for secure transfer of files to an external File Server.

SSH is used to protect the remote management of the TOE. Remote management of the TOE is using CLI over SSH.

1.3.2.3 Identification and Authentication

The TOE authenticates all users connecting to the management interfaces of the TOE. Authentication may take place over the console for local access or over SSH for remote access. Only upon successful authentication, given that the user is authorized for the role, is a user assigned to the role administrator and granted access to the management functions of the TOE. Local users authenticate to the TOE using a username and password. Remote users may also use SSH public-key authentication. A customizable warning banner is displayed at each authentication window.

The TOE uses X.509v3 certificates for peer entity authentication of TLS peers. The TSF determines the validity of the certificates by confirming the validity of the certificate chain and verifying that the certificate chain ends in a trusted Certificate Authority (CA). The TOE connects to an Online Certificate Status Protocol (OCSP) server using HTTP (unsecure) to confirm the revocation status of the certificates.

1.3.2.4 Security Management

The TOE allows local and remote management of its security functions. Local management is from a management workstation connected to the console or USB port of the TOE and the remote management is from a workstation connected to the TOE over SSHv2.

All management functions are implemented using the CLI and are only made available to authorized administrators upon successful identification and authentication. There are no other management interfaces than the CLI, i.e., the CLI implements each management function of the TOE.

The management functions the TOE implements include the ability to configure the access banner the TOE displays at each authentication window, the ability to configure the session inactivity timers, the ability to update the TOE software and to verify the authenticity of the updates, the ability to configure the authentication failure parameters, the ability to configure audit behaviour, the ability to modify the behaviour of the transmission of audit data to an external syslog server, the ability to manage the cryptographic keys, the ability to configure thresholds for SSH rekeying, the ability to set the time which is used for time-stamps, the ability to configure Network Time Protocol (NTP), the ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors, and the ability to import X.509v3 certificates to the TOE's trust store.

1.3.2.5 Protection of the TSF

The TOE protects all passwords, pre-shared keys, symmetric keys, and private keys from unauthorized disclosure. Pre-shared keys, symmetric keys, and private keys are stored encrypted. An exception is the SSH host keys which are required by the SSH Daemon when the SSH starts. The SSH Daemon is executed at the root privileges and the SSH host keys are only accessible with root privileges. No user of the TOE is granted root privileges. Passwords are stored as non-reversible hash values computed using SHA-512 using the Linux Pluggable Authentication Module (PAM) functions. The TOE maintains system time via its local hardware clock which is manually set by an administrator. The administrator may also configure the TOE to connect to an NTP server for time synchronization.

The TOE executes self-tests during initial start-up to ensure correct operation and enforcement of its security functions. An administrator can install software updates to the TOE and verify the authenticity of all updates prior to the installation.

Access to the TOE functions is only using the CLI from the management ports. The CLI cannot be invoked from the ports used for connecting the subnetworks across the TOE. Access to the CLI is only granted to authorized administrators upon successful authentication.

1.3.2.6 TOE Access

Prior to establishing an administration session with the TOE, an access banner is displayed to the user. The banner messaging is customizable but is typically used to warn the users of the consequences of attempted unauthorized access. The TOE will terminate an interactive session after a configurable time of session inactivity. A user may terminate his/her local and remote administrative sessions on will. Users may change their own passwords, but the TOE enforces minimum quality criteria for the passwords. The TOE also maintains a counter for consecutive failed authentication attempts for each user. If the counter value reaches an administrator-defined threshold, the TOE triggers protective measures to prevent password guessing attacks.

1.3.2.7 Trusted Path/Channels

The TOE implements trusted paths and trusted channels. The trusted path is a SSH connection between the TOE and the remote management workstation. The SSH client of the remote management workstation connects to the SSH Server implemented by the TOE. Upon successful connection establishment and authentication of the user, the remote administrator uses the CLI over SSH to manage the TOE.

For trusted channels, the TOE implements a TLS client used by the TOE to connect to the peer entities. The peer entities are a remote File server and the syslog server. Both systems are mandatory in the Operational Environment. The TOE also implements HTTPS over TLS for connecting to a remote file server. The TLS Client is only used for TLSv1.2 connections.

1.3.3 TOE Environment

The environmental components described in Table 3 are required to operate the TOE in the evaluated configuration.

Table 3 Environmental Components of the TOE

Component	Purpose/Description
Audit server	The audit server supports syslog messages over TLS to receive the audit files from the TOE. The audit data is stored in the remote audit server for redundancy purposes.
NTP server	An external NTP Server for synchronizing the TOE time with. NTP time stamps are protected from tampering using SHA-1 for authentication.
File Server	Remote file server for storing user files and updating the TOE. Communication with the File Server is with HTTPS over TLS.
OCSP Server	Validity of the certificates the TOE uses for asserting the authenticity of the TLS peers is verified using OCSP. Communication with an OCSP Server is over HTTP.
Management Workstation	A workstation used by an administrator to manage the TOE locally or remotely. The remote management station must include a SSHv2 client.

1.3.4 Product Functionality not Included in the Scope of the Evaluation

The following product functionality is not covered by the evaluation:

- Telnet is not included and must be disabled.
- Telemetry Client must not be used.
- MACsec functionality is not evaluated and must not be used.
- SNMP is not evaluated and must be disabled.
- FTP to upload or download files/configuration is not evaluated and must be disabled.

2 Conformance Claims

This section states the conformance claims and the conformance claims rationale and identifies the applicable Technical Decisions (TD).

2.1 CC Conformance Claims

The TOE is CC 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, 23 March 2020 [NDcPPv2.2e]

with the following optional and selection-based SFRs.

- FAU_STG.1
- FCS_HTTPS_EXT.1
- FCS_NTP_EXT.1
- FCS_SSHS_EXT.1
- FCS_TLSC_EXT.1
- FIA_X509_EXT.1/Rev
- FIA_X509_EXT.2
- FMT_MOF.1/Functions
- FMT_MTD.1/CryptoKeys

2.3 Conformance Claims 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.

2.4 Technical Decisions

All NIAP Technical Decisions issued to date and applicable to NDcPPv2.2e have been considered. Table 4 identifies all relevant TDs and argues their applicability to the TOE.

Table 4 Technical Decisions

Technical Decision	Applicable	Exclusion Rationale and Notes
TD0527: Updated 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	

Technical Decision	Applicable	Exclusion Rationale and Notes
TD0537: NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	Yes	
TD0546: NIT Technical Decision for DTLS – clarification of Application Note 63	No	The TOE does not implement DTLS.
TD0547: NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	Yes	
TD0555: NIT Technical Decision for RFC Reference incorrect in TLSS Test	No	The TOE does not implement a TLS Server.
TD0556: NIT Technical Decisions for RFC 5077 question	No	The TOE does not implement TLS Server.
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	The TOE does not implement DTLS.
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	Yes	
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	Yes	
TD0632: NIT Technical Decision for Consistency with Time Data for vNDs	Yes	
TD0635: NIT Technical Decision for TLS Server and Key Agreement Parameters	No	The TOE does not implement a TLS Server.
TD0636: NIT Technical Decision for Clarification of Public Key User Authentication for SSH	No	The TOE does not implement a SSH Client.
TD0638: NIT Technical Decision for Key Pair Generation for Authentication	Yes	
TD0639: NIT Technical Decision for Clarification for NTP MAC Keys	Yes	

Technical Decision	Applicable	Exclusion Rationale and Notes
TD0670: NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	Yes	
TD0738: NIT Technical Decision for Link to Allowed-With List	Yes	
TD0790: NIT Technical Decision: Clarification Required for testing IPv6	Yes	Archived TD0634
TD0792: NIT Technical Decision: FIA_PMG_EXT.1 – TSS EA not in line with SFR	Yes	
TD0800: Updated NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance	No	The TOE does not implement IPSec. TD0633 is archived.

3 Security Problem Definition

The security problem definition has been taken directly from the claimed PP and any relevant EPs, Modules and Packages identified in Section 2.2. It is reproduced here for the convenience of the reader.

3.1 Threats

The threats applicable to the TOE are stated in in Table 5.

Table 5 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 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,

ID	Threat
	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 6 are drawn directly from the PP and any relevant EPs, Modules and Packages.

Table 6 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).

ID	Assumption
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).
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. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
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.

3.3 Organizational Security Policies

The OSPs included in Table 7 are drawn directly from the PP and any relevant EPs, Modules and Packages.

Table 7 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 and Packages. They are reproduced here for the convenience of the reader.

There are no secure objectives explicitly stated for the TOE in [NDcPPv2.2e].

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 8 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 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. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.
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.

5 Security Requirements

This section states the security requirements for the TOE. The security requirements include the Security Functional Requirements (SFR) and the Security Assurance Requirements (SAR).

5.1 Security Functional Requirements Summary

This section identifies and defines the Security Functional Requirements (SFRs) for the TOE. The SFRs included in this section are derived from the applicable Protection Profiles, EPs, Modules and Packages stated in Sect. 2.2. The Security Functional Requirements for the TOE are summarized in Table 9.

Table 9 SFRs

Requirement	Description
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_STG.1	Protected Audit Trail Storage
FAU_STG_EXT.1	Protected Audit Event Storage
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/ARMA53	Random Bit Generation
FCS_RBG_EXT.1/ARMA72	Random Bit Generation
FCS_RBG_EXT.1/Intel	Random Bit Generation
FCS_SSHS_EXT.1	SSH Server Protocol
FCS_TLSC_EXT.1	TLS Client 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
FMT_MOF.1/Functions	Management of Security Functions Behaviour
FMT_MOF.1/ManualUpdate	Management of Security Functions Behaviour
FMT_MTD.1/CoreData	Management of TSF Data
FMT_MTD.1/CryptoKeys	Management of TSF Data

Requirement	Description
FMT_SMF.1	Specification of Management Functions
FMT_SMR.2	Restrictions on security roles
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
FPT_APW_EXT.1	Protection of Administrator Passwords
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

5.2 Conventions

The CC allows the performance of assignment, selection, refinement, and iteration on the Security Functional Requirements. The following notations and conventions are used to identify and express the operations on the requirements:

- Assignment: Indicated with *italicized* text and surrounded with brackets (‘[‘,’]’),
- Refinement: Removed text is indicated with ~~overstricken~~ text and addition with **bold** text,
- Selection: Indicated with underlined text and surrounded with brackets (‘[‘,’]’), and
- Iteration: Indicated by appending the iteration identifier after a slash, e.g., /SigGen.

Where operations were completed in the PP and relevant EPs, Modules and Packages, the formatting used in the PP, EP, Module or Package is retained. Extended SFRs are identified by the addition of “EXT” after the requirement name.

The SFRs are duplicated exactly as they are in the CPP_ND_V2.2E except for selections and assignments text. For selections and assignments, the font conventions are described above (e.g., if a selection is listed in the PP italicized, the italicized font will not be maintained).

5.3 Security Functional Requirements

This section is used for stating each applicable Security Functional Requirement for the TOE.

5.3.1 Security Audit (FAU)

5.3.1.1 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) All 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 10*.

FAU_GEN.1.2

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

a) Date and time of the event, type of event, subject identity, 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 10*.*

Table 10 Security Functional Requirements and Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG.1	None.	None.
FAU_STG_EXT.1	None.	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/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session	Reason for failure
FCS_NTP_EXT.1	• Configuration of a new time server • Removal of configured time server	• Identity if new/removed time server
FCS_RBG_EXT.1/ARMA53	None.	None.
FCS_RBG_EXT.1/ARMA72	None.	None.
FCS_RBG_EXT.1/Intel	None.	None.
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure

Requirement	Auditable Events	Additional Audit Record Contents
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_UAU_EXT.2	All use of identification and authentication mechanism	Origin of the attempt (e.g., IP address)
FIA_UAU.7	None.	None.
FIA_UIA_EXT.1	All use of identification and authentication mechanism	Origin of the attempt (e.g., IP address)
FIA_X509_EXT.1/Rev	• Unsuccessful attempt to validate a certificate • Any addition, replacement or removal of trust anchors in the TOE's trust store	• Reason for failure of certificate validation • Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
FIA_X509_EXT.2	None.	None.
FMT_MOF.1/Functions	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process (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_TST_EXT.1	None.	None.
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.

Requirement	Auditable Events	Additional Audit Record Contents
FTA_SSL_EXT.1	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 • Termination of the trusted channel • 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 • Termination of the trusted path. • Failure of the trusted path functions.	None.

5.3.1.2 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.

5.3.1.3 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1

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

FAU_STG.1.2

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

5.3.1.4 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 [

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

].

FAU_STG_EXT.1.3

The TSF shall [overwrite previous audit records according to the following rule: *[the oldest file is overwritten]*] when the local storage space for audit data is full.

5.3.2 Cryptographic Support (FCS)

5.3.2.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1

The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;
- 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;
- FFC Schemes using 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526].

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

5.3.2.2 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: [

- RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1";
- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";
- FFC Schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [groups listed in RFC 3526].

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

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

5.3.2.3 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]];
- 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.*

5.3.2.4 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, CTR, 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,
- CTR as specified in ISO 10116,
- GCM as specified in ISO 19772

].

5.3.2.5 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*.

5.3.2.6 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,
- HMAC-SHA-512

] and cryptographic key sizes [

- *160 bits,*
- *256 bits,*
- *384 bits,*
- *512 bits*

] **and message digest sizes** [

- 160,
- 256,
- 384,
- 512

] **bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*.

5.3.2.7 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 [

- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [*2048 bits, 4096 bits*],
- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [*256 bits*]

]

that meet the following: [

- 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

].

5.3.2.8 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.

5.3.2.9 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 [

- 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.

5.3.2.10 FCS_RBG_EXT.1/ARMA53 Random Bit Generation

FCS_RBG_EXT.1.1/ARMA53

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/ARMA53

The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [

- *[1]* software-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.

Application Note: /ARMA53 includes 3926, 3928, and 3948 models all running on ARM Cortex A53 processors.

5.3.2.11 FCS_RBG_EXT.1/ARMA72 Random Bit Generation

FCS_RBG_EXT.1.1/ARMA72

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/ARMA72

The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [

- *[1]* software-based noise source,
- *[1]* 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.

Application Note: /ARMA72 includes 5144 and 5164 models both running on ARM Cortex A72 processors.

5.3.2.12 FCS_RBG_EXT.1/Intel Random Bit Generation

FCS_RBG_EXT.1.1/Intel

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/Intel

The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [

- *[1]* software-based noise source,
- *[2]* 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.

Application Note: /Intel iteration includes the 5162, 5170, 5171, 8180 and the Large NVPs all running on Intel processors.

5.3.2.13 FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.1

The TSF shall implement the SSH protocol in accordance with: RFCs *4251, 4252, 4253, 4254*, [4256, 4344, 5656, 6668].

FCS_SSHS_EXT.1.2

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

Application Note: Modified as per TD 0631.

FCS_SSHS_EXT.1.3

The TSF shall ensure that, as described in RFC 4253, packets greater than [*32768*] bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4

The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [

- aes128-ctr,
- aes256-ctr,
- aes128-gcm@openssh.com,
- aes256-gcm@openssh.com

].

FCS_SSHS_EXT.1.5

The TSF shall ensure that the SSH public-key based authentication implementation uses [

- ssh-rsa,
- ecdsa-sha2-nistp256,

] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6

The TSF shall ensure that the SSH transport implementation uses [

- hmac-sha1,
- hmac-sha2-256,
- hmac-sha2-512,
- implicit

] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7

The TSF shall ensure that [

- diffie-hellman-group14-sha1,
- ecdh-sha2-nistp256

] and [

- diffie-hellman-group14-sha256,
- diffie-hellman-group16-sha512,
- ecdh-sha2-nistp384,
- ecdh-sha2-nistp521

] are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHS_EXT.1.8

The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

5.3.2.14 FCS_TLSC_EXT.1 TLS Client Protocol without Mutual Authentication

FCS_TLSC_EXT.1.1

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

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268,
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268,
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492,
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492,
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC5246,
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC5289,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC5289,
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC5289,
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC5289

] 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 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 [

- 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.

5.3.3 Identification and Authentication (FIA)

5.3.3.1 FIA_AFL.1 Authentication Failure Management

FIA_AFL.1.1

The TSF shall detect when an Administrator configurable positive integer within *[1-5]* 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 an Administrator defined time period has elapsed].

5.3.3.2 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: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, *[“+”, “,”, “-”, “.”, “/”, “:”, “;”, “<”, “=”, “>”, “\”, “`”, and “~”]*]

b) Minimum password length shall be configurable to between [*1*] and [*128*] characters.

5.3.3.3 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.

5.3.3.4 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**.

5.3.3.5 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.

5.3.3.6 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 extendedKeyUsagefield.
  - 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.

5.3.3.7 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 [not accept the certificate].

Application Note: Modified as per TD0537.

5.3.4 Security Management (FMT)

5.3.4.1 FMT_MOF.1/Functions Management of Security Functions Behaviour

FMT_MOF.1.1/Functions

The TSF shall restrict the ability to [modify the behaviour of] the functions [

- transmission of audit data to an external IT entity,

] *to Security Administrators*.

5.3.4.2 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.*

5.3.4.3 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*.

5.3.4.4 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*.

5.3.4.5 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 [signature] capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- [
    - Ability to modify the behaviour of the transmission of audit data to an external IT entity;
    - Ability to manage the cryptographic keys;
    - Ability to configure thresholds for SSH rekeying;
    - Ability to set the time which is used for time-stamps;
    - Ability to configure NTP;
    - Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
    - Ability to import X.509v3 certificates to the TOE's trust store;
    - Ability to manage the trusted public keys database

].

Application Note: Modified as per TD0631.

5.3.4.6 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.

5.3.5 Protection of the TSF (FPT)

5.3.5.1 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.

5.3.5.2 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.

5.3.5.3 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

].

Application Note: This SFR has been updated as per TD0632.

5.3.5.4 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: [

- *Check of various FPGA devices access and sanity,*
- *Check of PCI bus and devices response,*
- *Filesystem Integrity,*
- *Crypto KAT/self-test*

].

5.3.5.5 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.

5.3.6 TOE Access (FTA)

5.3.6.1 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.*

5.3.6.2 FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1

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

5.3.6.3 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

5.3.6.4 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.

5.3.7 Trusted Path/Channels (FTP)

5.3.7.1 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1

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

- *[File 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 [

- *transmission of audit data,*
- *installing a TOE upgrade from File Server,*

].

5.3.7.2 FTP_TRP.1/Admin Trusted Path

FTP_TRP.1.1/Admin

The TSF shall **be capable of using** [SSH] **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.*

5.4 Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from the PP and any relevant EPs, Modules and Packages. The assurance requirements are summarized in Table 11.

Table 11 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

Assurance Class	Assurance Components	Component Description
	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 Security Requirements Rationale

All SFRs and SARs are derived from the PP and any relevant EPs, Modules and Packages. There are no additions or removals, other than those allowed by the PP, implemented in the ST. As such, the security requirements rationale of the PP is directly applicable and is not repeated here.

6 TOE Summary Specification

This section is the TOE Summary Specification. It commences with the description of how the Security Functional Requirements applicable to the TOE are fulfilled. That is followed by a description of how the Security Assurance Requirements are fulfilled. The CAVP certificate references to the cryptographic functions the TOE implements are given in Sect. 6.3 and the destruction of cryptographic keys and Critical Security Parameters (CSP) summarized in Sect. 6.4.

6.1 Fulfillment of the Security Functional Requirements

The fulfillment of the Security Functional Requirements by the TOE is given in Table 12.

Table 12 Fulfillment of the Security Functional Requirements

Requirement	TSS Description
FAU_GEN.1 FAU_GEN.2	The TOE generates an audit record whenever an auditable event occurs. Auditable events include the start-up and shut-down of the audit function, and all administrative actions. The administrative actions include login and logout by administrators, all changes to TOE configuration, all actions (generating, importing, exporting, renaming, moving, and deleting) of cryptographic keys, and all changes in passwords. An audit log uniquely identifies a cryptographic key by its name, the operation performed on the relevant key, and the user identity performing the operation. The TOE also generates an audit record for each event stated in Table 10. Each of the events specified in the audit record is in enough detail to identify the user for which the event is associated (e.g., user identity, IP address), when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. The date and time information for any audit event is recorded by the TOE as part of each audit record to ensure the timing of the event can be unambiguously determined from the data contained in the audit record. The representation of date and time information recorded for each event allows unanimous determination of at day, month and year information for the date and hours, minutes and second information for the time.
FAU_STG.1 FAU_STG_EXT.1	Audit records are stored persistently on the local file system. The TOE is a standalone component that stores audit data locally. The amount of audit data that may be stored locally on the TOE is dependent on the available disk space which varies depending on platform. When the local audit data store capacity is exhausted, the TOE will overwrite audit records starting with the oldest audit record. The Security Administrator can configure the TOE to transfer the audit data to an external audit server. The audit logs are sent to the external syslog server via TLS in real-time. Only authorized administrators may view and clear audit records using the CLI which is the sole interface to the management functions of the TOE.
FCS_CKM.1	The TOE implements generation of asymmetric cryptographic keys using the following asymmetric schemes: • RSA schemes using cryptographic key sizes of 2048 bits and 4096 bits as defined in FIPS PUB 186-4, • ECC schemes using NIST curves P-256, P-384 and P-521 as defined in FIPS PUB 186-4, and

<table>
<tr><th>Requirement</th><th>TSS Description</th></tr>
<tr><td></td><td>
Diffie-Hellman Groups 14 (2048-bit MODP) and 16 (4096-bit MODP)
The asymmetric cryptographic keys generated by the above methods are used by the protocols the TOE implements for trusted path and trusted channels as follows:
<table>
<tr><td></td><td>TLS</td><td>SSH</td></tr>
<tr><td>RSA</td><td>2048 bits, 4096 bits</td><td>2048 bits, 4096 bits</td></tr>
<tr><td>ECC</td><td>secp256r1, secp384r1, secp521r1</td><td>nistp256, nistp384, nistp521</td></tr>
<tr><td>FFC (DH Groups)</td><td>N/A</td><td>Group 14, Group 16</td></tr>
</table>
</td></tr>
<tr><td>FCS_CKM.2</td><td>
The TOE implements RSA, ECC and FFC (DH Groups) for the key establishment.
RSA and ECC are used in TLS. FFC safe Primes (DH Group 14, DH Group 16) and ECC schemes are used in SSH. TLS is used for protecting the communication between the TOE and the audit server. TLS is also used for implementing HTTPS which the TOE uses for communicating with an external file server. SSH is used for protecting the remote management session between the remote management workstation and the TOE.
DH Groups 14 and 16 are used for implementing SSH which protects the remote management session between the remote management workstation and the TOE.
<table>
<tr><td></td><td>TLS
(FCS_TLSC_EXT.1.1, FCS_TLSC_EXT.1.4)</td><td>SSH
(FCS_SSHS_EXT.1.7)</td></tr>
<tr><td>RSA</td><td>2048 bits, 4096 bits</td><td>N/A</td></tr>
<tr><td>ECC</td><td>secp256r1, secp384r1, secp521r1</td><td>nistp256, nistp384, nistp521</td></tr>
<tr><td>FFC (DH Groups)</td><td>N/A</td><td>Group 14, Group 16</td></tr>
</table>
For RSA and FFC key establishment schemes, no CAVP exists. CCTL has performed all assurance/evaluation activities..
</td></tr>
<tr><td>FCS_CKM.4</td><td>
The TOE stores all keys in plaintext form. The TOE stores keys in volatile and non-volatile memory depending upon the type and purpose of the keys.
The TOE destroys plaintext cryptographic keys stored in the volatile storage by a single overwrite with zeroes before freeing the memory.
Plaintext keys stored in the non-volatile storage are maintained by the file system. These plaintext keys are destroyed by SAOS when an administrator makes configuration changes (ssh server config or tls-service-profile config) that result in changing, replacing or deletion of these files. The keys are destroyed by the SAOS by overwriting the storage location of the key with a single overwrite of zeroes. The destruction of each cryptographic key and Critical Security Parameter (CSP) is summarized in Table 15.

The above key destruction methods apply to all configurations and circumstances, except one. The only situation where the key destruction may be prevented would be if the system suffers a crash or loss of power. This situation only impacts the keys that are stored in the filesystem. Since the TOE
</td></tr>
</table>

<table>
<tr><th>Requirement</th><th>TSS Description</th></tr>
<tr><td></td><td>is inaccessible in this situation, administrative zeroization cannot be performed. The keys stored in filesystem are not directly accessible to any user or administrator.</td></tr>
<tr><td>FCS_COP.1/DataEncryption</td><td>The TOE implements symmetric encryption and decryption using AES in CBC, GCM and CTR modes. Key sizes of 128 and 256 bits are implemented. AES encryption and decryption is used by TLS and SSH protocols.</td></tr>
<tr><td>FCS_COP.1/Hash</td><td>The TOE implements cryptographic message digest (hash value) computation using SHA-1, SHA-256, SHA-384, and SHA-512 with message digest sizes of 160 bits, 256 bits, 384 bits, and 512 bits respectively. The hashing algorithms are used in SSH and TLS connections for secure communications.
The TOE uses message digests for the following functions:
<table>
<tr><th>Function</th><th>SHA-1</th><th>SHA-256</th><th>SHA-384</th><th>SHA-512</th></tr>
<tr><td>Digital signature computation</td><td></td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>Digital Signature verification</td><td>X</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>TLS HMAC</td><td>X</td><td>X</td><td>X</td><td></td></tr>
<tr><td>SSH HMAC</td><td>X</td><td>X</td><td></td><td>X</td></tr>
<tr><td>Password storage</td><td></td><td></td><td></td><td>X</td></tr>
<tr><td>NTP Message Authentication</td><td>X</td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>FCS_COP.1/KeyedHash</td><td>The HMAC (keyed Hash) algorithms used by the TOE are summarized in the following. For each HMAC, the table states the Hash algorithm used, the key size, block size and the message digests (output) length.
<table>
<tr><th></th><th>Hash Algorithm</th><th>Key Size</th><th>Block Size / Output Length</th></tr>
<tr><td>HMAC-SHA-1</td><td>SHA-1</td><td>128 bits</td><td>160 bits</td></tr>
<tr><td>HMAC-SHA-256</td><td>SHA-256</td><td>256 bits</td><td>256 bits</td></tr>
<tr><td>HMAC-SHA-384</td><td>SHA-384</td><td>384 bits</td><td>384 bits</td></tr>
<tr><td>HMAC-SHA-512</td><td>SHA-512</td><td>512 bits</td><td>512 bits</td></tr>
</table></td></tr>
<tr><td>FCS_COP.1/SigGen</td><td>The TOE generates and verifies digital signatures with RSA Digital Signature Algorithm and cryptographic key sizes (modulus) 2048 bits and 4096 bits.
The TOE also generates and verifies digital signatures with ECC using key sizes 256 bits for NIST curves P-256.</td></tr>
<tr><td>FCS_HTTPS_EXT.1</td><td>The TOE supports secure communication of the TOE with the File server over an HTTPS connection using TLS v1.2 implementation. In this scenario, the TOE acts as a TLS client communicating with the servers in the Operational Environment. The HTTPS protocol complies with RFC 2818.</td></tr>
<tr><td>FCS_NTP_EXT.1</td><td>The TOE supports the use of the NTP version 4 (NTP v4) to synchronize the clock of the TOE with an NTP server. An NTP server is not required as the clock source and can be set manually over SSH using the <code>clock set</code> command. If NTP is used, the TOE validates the integrity of the time source using SHA1 as the message digest algorithm. The TOE supports at least three and a</td></tr>
</table>

Requirement	TSS Description
	maximum of ten NTP servers, however in the evaluated configuration up to 3 are claimed. The TSF shall not update NTP timestamp from broadcast and/or multicast addresses. Both parameters are configured by default to not allow an update.
FCS_RBG_EXT.1/ARMA53, FCS_RBG_EXT.1/ARMA72, FCS_RBG_EXT.1/Intel	The TOE implements one random bit generator: 1. CTR_DRBG (AES-256) implemented by OpenSSL and seeded by 256 bits of entropy. The entropy sources used by the TOE depend on the exact variation of the TOE: • TOE variations 3926, 3928, and 3948 are implemented using ARM Cortex A53 with no readily available hardware sources of entropy. They harvest entropy from the Linux kernel v5.4.154 functions which accumulate and make available to other processes entropy from CPU jitter and CPU interrupts. • TOE variations 5144 and 5164 use the ARM Cortex A72 which implements the IP-76 hardware source of entropy. They also harvest entropy from the Linux kernel v5.4.154 functions which accumulate and make available to other processes entropy from CPU jitter and CPU interrupts. • TOE variations 5162, 5170, 5171, 8180, and the Large NFV Compute Servers are implemented on Intel platforms which implement the RDRAND command that is used for reading entropy from a dedicated CPU circuitry, and also include Infineon SLM9670 or Infineon SLB9665 TPMv2.0 chip which implements a source of entropy which can be read by external processes. They also harvest entropy from the Linux kernel v5.4.154 functions which accumulate and make available to other processes entropy from CPU jitter and CPU interrupts.
FCS_SSHS_EXT.1	The TOE implements a SSH Server for remote administrators to connect securely to the TOE and use the CLI from a remote management station. The TOE implementation of SSHv2 is in compliance with RFCs 4251, 4252, 4253, 4254, 4256, 4344, 5656, and 6668. The TOE implements both public key authentication and password-based authentication. Public key authentication methods supported are ssh-rsa and ecdsa-sha2-nistp256. Any other authentication algorithm requests are rejected. For Public key authentication, the TOE stores a user's (or SSH client's) public key in its local filesystem and associates that key with the user's identity. When a user or client presents its public key, the TOE matches it against the stored value to verify the user's identity. The password-based authentication acts as a fallback option in case the public key authentication fails. The TOE examines all packets for size and drops any packets greater than 32768 bytes and drop in accordance with RFC 4253. For symmetric encryption, the TOE allows aes128-ctr, aes256-ctr, aes128-gcm@openssh.com, and aes256-gcm@openssh.com. Requests for any other algorithms are rejected. For message authentication, the TOE allows hmac-sha1, hmac-sha2-256, hmac-sha2-512 and implicit. Requests for any other algorithms is rejected.

Requirement	TSS Description
	Message authentication algorithm implicit is used for the @openssh.com symmetric encryption algorithms. The SSHv2 implementation of the TOE enforces to only allow the diffie-hellman-group14-sha1, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521 key exchange methods. The TOE is capable of rekeying the SSH connection. The rekeying occurs if a session is longer than one hour or more than one gigabytes of data has been transmitted with one key. The TOE continuously checks both conditions. When either of the conditions are met, the TOE will initiate a rekey.
FCS_TLSC_EXT.1	The TOE implements a TLS Client which supports TLS 1.2 (RFC 5246) and rejects all other TLS and SSL versions. The following ciphersuites are implemented: • TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 • TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 • TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 • TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 The TOE uses TLS for all trusted channels and also to implement HTTPS. Peer entities are authenticated with the X.509 certificates. Mutual authentication is not supported. The trusted channel is established when the peer certificate is valid. The TOE verifies that the presented identifier matches the reference identifier in order to establish the connection. The TOE supports SAN extension and checks SAN extension over CN when present. The TOE ignores CN when SAN is present. When SAN is not present, the TOE falls back to CN check. FQDN is supported in both SAN and CN while IP address is only supported in SAN. The TOE supports wildcards in certificates. The wildcard must be in the left-most label of the presented identifier and can only cover one level of subdomains. For the reference identifier without a left-most label as in the certificate, the connection will fail, i.e., awesome.com doesn't match *.awesome.com. The TLS client does not support certificate pinning. The TLS client will transmit the Supported Elliptic Curves extension in the Client Hello message by default with support for the NIST curves secp256r1, secp384r1 and secp521r1. The non-TOE server can choose to negotiate the elliptic curve from this set for any of the mutually negotiable elliptic curve

Requirement	TSS Description
	cipher suites. The TOE will validate the server's certificate according to FIA_X509_EXT.1/Rev. If the server certificate is invalid, the connection will not be established.
FIA_AFL.1	The TOE maintains a counter of consecutive failed authentication attempts for each user. The counter tracks the number of failed authentication attempts for all remote authentication attempts. Local authentication attempts from the console are not tracked by the counter. When an authentication fails, the counter value is incremented. When an authentication succeeds, the counter value is reset. The maximum number of allowed consecutive authentication attempts may be set by the administrator of the TOE. When the maximum number is reached, the TOE shall lock the account and start a session lockout timer for the account. Once the lockout timer expires, the TOE shall unlock the account. The duration of the lockout may be set by the administrator of the TOE. Accounting locking only applies to remote authentication attempts. Even if an account is locked, the same account may still be used from console if the user is successfully authenticated. This ensures that at no time shall the TOE be in a state where each administrator is locked out and no administrator access to the TOE is possible.
FIA_PMG_EXT.1	Each user of the TOE may choose his/her password. To ensure high quality passwords, the TOE implements quality criteria which each password must meet. The criteria are implemented using the alphabet used for the password selection and the minimum length of the passwords. The passwords must be expressed using the standard Linux alphabet allowed for passwords. The alphabet includes upper and lower case letters, numbers, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", ["+", ",", "-", ".", "/", ":", ";", "<", "=", ">", "\", "`", and "~"]. Each password must also be of the minimum length allowed by the TOE. The minimum length of a password may be configured by the administrator and can be any integer value between 1 and 128 (inclusive).
FIA_UIA_EXT.1	The TOE requires all users to be successfully identified and authenticated prior to assigning them to the role administrator and granting them access to the TOE. The TOE displays an access banner to each user prior at the identification and authentication window. Successful identification and authentication are required for each subsequent administrative access to the TOE. Administrators may access the TOE locally from a console connected to the serial port of a USB-C port of the TOE, or remotely over a SSH connection. For local access, the TOE prompts the user to enter a username and password. The TOE then compares the entered password to the reference password stored for the user. If the verification succeeds and the user is configured as the role administrator, the TOE assigns the user to the role administrator and grants access to the CLI. If the username does not exist or the password is incorrect, the TOE denies access and returns to the authentication window to request a username and password. For remote access, the TOE may be configured to require RSA public key authentication or password-based authentication. The remote access is implemented using SSH. Successful authentication occurs when either the

Requirement	TSS Description
	cryptographic authentication protocol is successfully completed between the TOE and the remote management workstation, or the password verification succeeds in a manner identical to the authentication for local access. If the authentication is successful and the user is granted access to the role administrator, the TOE establishes a SSH connection between the remote management workstation and the TOE and grants the user administrator rights to the TOE (i.e., makes available the CLI). If the authentication fails, the TOE denies access and returns to the authentication windows. The TOE may also take protective measures if the number of consecutive authentication attempts for remote access reaches the maximum number of allowed attempts (see FIA_AFL.1).
FIA_UAU_EXT.2	The TOE implements a password-based authentication method which is used for authenticating the local users.
FIA_UAU.7	Local authentication is echoless, i.e., the TOE does not display on the console any characters when a password is entered.
FIA_X509_EXT.1/Rev FIA_X509_EXT.2	The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication of external TLS peers. Certificates are used to authenticate and establish secure communication channel for the File Server and syslog servers. The TOE supports RSA based certificates in PKCS#12. The TOE allows each TLS service to be configured with its own certificate in a TLS profile. Once a certificate is configured for a Syslog Server using a TLS profile, that certificate will be used for all Syslog Server connection authentication. Likewise, once a certificate is configured for TLS File Server, that certificate will be used for all TLS File Server connection authentication. The TOE will check the validity of the TLS Server certificate prior to establishing a TLS connection with the TLS server. The certificate validation is determined based on reference ID verification, certificate path, extendedKeyUsage field, certificate expiry date and the certificate revocation status. Both trusted channels are treated the same. The TOE also validates 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 TOE validates 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 TOE validates the revocation status of the certificate using Online Certificate Status Protocol (OCSP) as specified in RFC 6960. • The TOE validates the extendedKeyUsage field according to the following rules: o Server certificates presented for TLS must have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field. o Client certificates presented for TLS must have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.

Requirement	TSS Description
	○ 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. ○ The TOE will only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE. The TOE does not use X.509 certificates for trusted updates, hence the requirement for Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field is trivially satisfied. Certificate validity and revocation checking is performed to support authentication of external TLS peers such as audit server and file server. The certificate validity and revocation checking is performed on each certificate when it is uploaded into the TOE as well as part of the authentication step. The TOE used OCSP for revocation checking. If the validation of the certificate fails because the OCSP Server cannot be connected to, the certificate shall not be accepted, and the connection is terminated. The TOE stores all imported certificates for its TLS peers as part of its pkix structure of tls-service-profile. The CA certificates and device (end entity) certificates are stored separately and used accordingly during connection time to validate the TLS peer. The TOE only supports RSA based certificates.

FMT_MOF.1/Functions	The TOE restricts the ability to enable and disable the transmission of audit records to an external audit server to Security Administrators. The Security Administrator can modify the behavior of transmitting audit data to an external audit server with the following configuration from the CLI:
	`config`
	`syslog log-actions remote-syslog-tls destination <ip address or DNS>`
	`syslog log-actions remote-syslog-tls admin-state <enable/disable>`
	
	The TOE's login users (Security Administrators and Read-Only Users) can view the current configuration from the CLI:
	`show syslog tls`
	`show syslog tls statistics`

FMT_MOF.1/ManualUpdate	The Vendor does occasionally publish software updates for the TOE to address security flaws or other bugs in the software. The TOE implements a function which allows administrators to install the software upgrades on the TOE. The CLI of the TOE also implements a command `show software` which allows the administrator to query the currently executing version of the TOE software to determine whether it requires upgrading. The Security Administrator may obtain the software image from the Ciena website and place it on a trusted file server. The TOE may then connect to the file server using HTTPS over TLS for the installation of the software upgrade. The installation of the upgrade is by the CLI command `software install`: *`software install 'url information' tls-service-profile <tls-service-profile Name>`*

Requirement	TSS Description
FMT_MTD.1/CoreData	The TOE requires successful identification and authentication of each administrator prior to granting them access to the TOE. Access to the TOE is by making available to the user a shell in which the user can execute CLI commands. Without access to the shell, the CLI is not accessible to the user and, consequently, administrator accesses are not possible. There are no management functions other than those accessible through the CLI. The only access the TOE allows prior to the successful identification and authentication of the user is the access banner displayed at each login prompt. The TOE restricts the ability to manage the TOE to Security Administrators. This is achieved via role-based access control and privileges assigned to each role.
FMT_MTD.1/CryptoKeys	Only the Security Administrator has the ability to configure the authentication keys TLS functionality and can modify, import, and delete the key for SSH. The TOE restricts the ability to manage SSH (public keys), TLS (public keys), and any configured X.509 certificates (public key) to the security administrators. This is achieved via role-based access control and privileges assigned to each role. The Security Administrator manages the SSH public key by configuring the public-key-based authentication keys for users: system ssh-server user-pubkey install user-name <user> filename <filename> [server-type <server-type>] address <address> [login <login-id> password <password>] OR system ssh-server user-pubkey install user-name <user> url <url> The Security Administrator manages the X.509 certificates used in TLS communication with the peers by configuring the TLS profile, associating the peer authentication profile and importing TLS certificate to the profile: 1. Identify the TLS Profile tls-service-profiles <tls-service-profile-name> tls-profile-name <tls-profile> 2. Identify the peer authentication profile. tls-service-profiles <tls-service-profile-name> tls-peer-auth-profile-name <peer-auth-profile> 3. Identify the TLS certificate. tls-service-profiles <tls-service-profile-name> tls-certificate-name <certificate>
FMT_SMF.1	The TOE implements a management interface for the Security Administrators to configure the TOE. The management interface is a Command Line Interface (CLI) which may be accessed locally from a management workstation connected to the TOE on the console or USB-C interface, or from a remote management workstation connected to the TOE network management port over SSH.

Requirement	TSS Description
	The Security Administrator may use the CLI to manage the TOE locally and remotely. The CLI implements the following management functions: • 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 authenticity of the updates using prior to installation, • Ability to configure the authentication failure handling, • Ability to modify the behaviour of the transmission of audit data to an external IT entity; • Ability to manage cryptographic keys, • Ability to configure thresholds for SSH rekeying, • Ability to set the time locally and configure NTP, • 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, and • Ability to manage the trusted public keys database.
FMT_SMR.2	The TOE only implements a single administrative role: Security Administrator. Users that belong to “Super” or “admin” groups have administrative privileges and assume the role of Security Administrator. Users may, upon successful authentication, based on their privileges (i.e. “Super” or “admin” groups), enter the role of Security Administrators locally and remotely and be granted access to the CLI which allows Security Administrators to manage the TOE locally and remotely. The TOE also supports a single non-administrative role: Read-Only User. Users that belong to “Limited” group have read-only privileges. Read-Only User cannot make any changes to the TOE configuration.
FPT_APW_EXT.1	All passwords are stored by the TOE hashed and salted using SHA-512. The storage and management of the passwords is implemented using the standard Linux Pluggable Authentication Mechanism (PAM) functions. The passwords are stored in a way such that they cannot be viewed by any user.
FPT_SKP_EXT.1	Pre-shared keys, symmetric keys, and private keys are stored encrypted. An exception is the SSH host keys which are required by the SSH Daemon when the SSH starts. The SSH Daemon is executed at the root privileges and the SSH host keys are only accessible with root privileges. During the setup and configuration of the TOE when cryptographic keys are generated, the TOE stores all private keys in a secure directory that is not readily accessible to administrators. Storage and destruction of each CSP and cryptographic key is summarized in Table 15. The TOE can only be accessed through the CLI which implements the complete management interface of the TOE. The CLI does not implement any functions for displaying the symmetric keys, asymmetric private keys, passwords, or any other secret parameters.
FPT_STM_EXT.1	The TOE implements a hardware clock for local date and time. The clock may also be configured to update the time from an external NTP server. The time is maintained by the TOE either via internal hardware clock or connecting to an external NTP server. The hardware clock is a real-time clock (RTC) with battery to maintain time across reboots and power loss. If an NTP server is configured, the TOE synchronizes the time with the external NTP server

Requirement	TSS Description
	periodically. The time is used for producing time stamps which are attached to audit records and to check the X.509 certificate expiration. The TOE also uses the clock to implement the session time out timers for each interactive session and to terminate each interactive session which exceeds the maximum allowed inactivity time.
FPT_TST_EXT.1	The TOE executes self-tests during initial start-up to ensure correct operation and enforcement of its security functions. The TSF runs the following self-tests during initial start-up (on power on) • Check of various FPGA devices access and sanity, • Check of PCI bus and devices response, • Filesystem Integrity, • Crypto KAT/self-test. The “Check of various FPGA devices access and sanity” self-test verifies the health, integrity and accessibility of all hardware FPGAs within the TOE by comparing the value in FPGA’s scratchpad. The “Check of PCI bus and devices response” self-test verifies the status of PCI bus and its connectivity to various PCIe devices connected including its backplane by sending a signal to the connected PCI device and receiving a response back. The “Filesystem Integrity” self-test verifies the firmware integrity by computing a hash and verifying with its stored value. The “Crypto KAT/self-test” self-test verifies the FIPS know answer tests for various algorithms implemented by the TOE’s cryptographic library such as AES, SHA, RSA, ECDSA, DRBG, and HMAC.
FPT_TUD_EXT.1	The TOE implements a CLI command `show software` for querying the currently executing version of the TOE firmware. From time to time, the vendor makes available software upgrades at the product web site. The TOE allows the Security Administrators to manually upgrade the TOE software to the version available at the vendor's web site. Upgrades are digitally signed using RSA with SHA-256. The signature will be verified by the TOE during an upgrade. Upon successful verification of the signature, the image will be loaded onto the TOE. The Security Administrator can obtain the software upgrade from the Ciena website and place it on a trusted filer server. The TOE may then be instructed to connect to the file server using HTTPS over TLS and install the software image. The CLI command for downloading and installing the software upgrade is *`software install 'url information' tls-service-profile <tls-service-profile Name>`* If the images cannot be verified, the image will not be loaded onto the TOE. The TOE does not support partial upgrades, the TOE software shall at each upgrade be upgraded in its entirety. The TOE does not support delayed activation.
FTA_SSL.3	The TOE will terminate a remote interactive session after a configurable time interval of session inactivity. The maximum allowed inactivity may be configured by the administrator of the TOE.

Requirement	TSS Description
	If a remote administrative session is inactive for a configured maximum period of inactivity, the session will be terminated. Fresh identification and authentication shall be required for the creation of a new session. The session inactivity timer will be restored for the new session.
FTA_SSL.4	The TOE allows Administrators to terminate their own interactive sessions with the TOE using the `exit` command.
FTA_SSL_EXT.1	The TOE will terminate a local interactive session after a configurable time interval of session inactivity. If a local user session is inactive for a configured maximum period of inactivity, the TOE will terminate the session.
FTA_TAB.1	The TOE implements an administrator-configurable access banner which is displayed at each login window. Both methods of accessing the TOE (locally form console and remotely over SSH) require user authentication. The access banner displaying an advisory notice and a consent warning message for each administrative method of access is displayed at each login prompt.
FTP_ITC.1	The TOE implements a TLS Client for a trusted channel between itself and authorized IT entities. The remote entity may be an audit server or a File Server. The TOE implements TLS between itself and a remote audit server and implements HTTPS over TLS for between itself and a remote file server. The file server is used in TOE software upgrades and storing user files. The audit server is used in exporting the audit logs securely. Each TLS and HTTPS/TLS connection is logically distinct from other communication channels and protects the channel data from disclosure and allows detection of the modification of the channel data. Peer entity authentication is performed using X.509 certificates for assured identification of the end points used in the trusted channels.
FTP_TRP.1/Admin	The TOE implements a SSH server which allows SSHv2 connection between a remote management station and the TOE. A CLI which implements the management interface of the TOE is available to a remote administration over an encrypted SSHv2 channel. The remote administrator must initiate connection to the TOE using the SSH Client of the remote management station.

6.2 Fulfillment of the Security Assurance Requirements

The TOE, the development environment and the operational environment satisfy the applicable security assurance requirements. The fulfillment of the security assurance requirement is by the security assurance measures stated in Table 13.

Table 13 Security Assurance Measures

SAR Component	How the SAR will be met
ASE_CLL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.1, ASE_REQ.1, ASE_SPD.1, ASE_TSS.1	The vendor authors a Security Target which meets all requirements stated in the assurance class ASE. The Security Target is evaluated by an independent Information Technology Security Evaluation Facility (ITSEF) licensed under the selected Information Technology Security Evaluation Scheme. The specific Information Technology Security Evaluation Scheme used is the CCEVS operated by NIST. The evaluation ensures that the Security Target meets all the assurance requirements stated in assurance class ASE and is an accurate and complete representation of the security problem the TOE addresses. Potential users of the TOE may examine the

SAR Component	How the SAR will be met
	Security Target to assess and assert the suitability of the TOE for their use case, and to understand the environmental conditions which must be fulfilled when deploying and operating the TOE.
ADV_FSP.1	The vendor authors a functional specification which 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.
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 ALC_CMS.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.
ATE_IND.1	Vendor will provide the TOE for functional testing by the ITSEF.
AVA_VAN.1	Vendor will provide the TOE for penetration testing by the ITSEF. The vendor will provide a document identifying the list of software and hardware components to facilitate the penetration testing by the ITSEF.

6.3 CAVP Certificate Details

The CAVP Certificate details for the cryptographic algorithms the TOE implements are given in Table 14. The TOE includes five different processors (refer to Table 2).

- CAVP A3495 cert includes the certification of the cryptographic algorithms running on four of the processors: ARM Cortex A53, ARM Cortex A72, Intel XEON D1527, and Intel XEON D1539.
- The algorithms running on the fifth processor, the Intel XEON D1548, are claimed included in CAVP A3495 based on the microarchitecture of the processor. Equivalency details are included in the ancillary Equivalency Analysis document.

Table 14 CAVP Algorithm Certificate References

Functions	Standards	Certificates
Asymmetric key generation (FCS_CKM.1)		
RSA Schemes (2048 bit, 4096 bit)	FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3	A3495

Functions	Standards	Certificates
ECC Schemes (ECDSA P-256, P-384, P-521 curves)	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4"	A3495
FFC Schemes ('safe-prime' groups)	NIST SP 800-56A Revision 3 , "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and RFC 3526	A3495
Key Establishment (FCS_CKM.2)		
RSA- based scheme	RSAES-PKCS1-v1_5, Section 7.2 of RFC 3447, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1"	No NIST CAVP, CCTL has performed all assurance/evaluation activities.
Elliptic curve-based scheme	NIST SP 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"	A3495
Finite field-based scheme	NIST Special Publication 800-56A, Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and RFC 3526.	No NIST CAVP, CCTL has performed all assurance/evaluation activities.
Encryption/Decryption (FCS_COP.1/DataEncryption)		
AES in CBC mode (128, 256 bits)	AES as specified in ISO 18033-3. CBC as specified in ISO 10116.	A3495
AES in CTR mode (128, 256 bits)	AES as specified in ISO 18033-3. CTR as specified in ISO 10116.	A3495
AES in GCM mode (128, 256 bits)	AES as specified in ISO 18033-3. GCM as specified in ISO 19772.	A3495
Cryptographic signature services (Signature Generation and Verification) (FCS_COP.1/SigGen)		
RSA Digital Signature Algorithm (rDSA) (2048 and 4096-bit modulus)	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,	A3495
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	A3495
Cryptographic hashing (FCS_COP.1/Hash)		
SHA-1 (digest size 160 bits)	ISO/IEC 10118-3:2004	A3495

Functions	Standards	Certificates
SHA-256 (digest size 256 bits) SHA-384 (digest size 384 bits) SHA-512 (digest size 512 bits)		
Keyed-hash message authentication (FCS_COP.1/KeyedHash)		
HMAC-SHA-1 (key size 160, digest size 160); HMAC-SHA-256 (key size 256 bits, digest size 256 bits); HMAC-SHA-384 (key size 384 bits, digest size 384 bits); HMAC-SHA-512 (key size 512 bits, digest size 512 bits)	ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"	A3495
Random bit generation (FCS_RBG_EXT.1/ARMA53, FCS_RBG_EXT.1/ARMA72, FCS_RBG_EXT.1/Intel)		
CTR-DRBG (AES-256) – 256 bits entropy;	ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions"	A3495

6.4 Cryptographic Key and CSP Destruction

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

Table 15 Destruction of Keys and CSPs

Keys/CSPs	Purpose	Storage Location	Method of Zeroization
SSH Server Host Keys	The SSH server host keys to identify ssh server	Non-volatile storage/file system	Overwrite with zeros to clear cache and read verify, then erase file
SSH session keys	Keys exchanged for protecting the confidentiality of the remote administration session	Volatile storage	Openssh package is used but all keys are overwritten with zeros before freeing memory
SSH PKA	Public key authentication for remote administration over SSH	Non-volatile storage/file system	Overwrite with zeros to clear cache and read verify, then erase file
x509 certificate with keys	For TLS connections	Non-volatile storage/file system	Overwrite with zeros to clear cache and read verify, then erase file
Local user password	User login	Non-volatile storage/file system (shadow file)	Erase file. Password is hashed with sha512 and the password file is only readable by root

Keys/CSPs	Purpose	Storage Location	Method of Zeroization
TLS session HMAC keys	For TLS connections with Audit server,	Volatile Storage	OpenSSL package is used as infrastructure but all keys are overwritten with zeros before freeing memory

7 Acronyms and Abbreviations

The acronyms and abbreviations used in this document are defined in Table 16.

Table 16 Acronyms and abbreviations

Acronym	Definition
AES	Advanced Encryption Standard
CA	Certification Authority
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CLI	Command Line Interface
CM	Configuration Management
CN	Common Name
cPP	Collaborative Protection Profile
CPU	Central Processing Unit
CRC	Cyclic redundancy Checksum
CSP	Critical Security Parameter
CTR	Counter-Mode
DC	Direct Current
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security
ECC	Elliptic Curve Cryptography
EP	Extended Package
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
FQDN	Fully Qualified Domain Name
FRU	Field-Replaceable Unit
GCM	Galois Counter Mode
HMAC	Hashed Message Authentication Code
HTTP	Hyper-Text Transfer Protocol
HTTPS	Hyper-Text Transfer Protocol Security
IEC	International Electrotechnical Committee
IP	Internet Protocol
ISO	International Standards Organization
ITSEF	Information Technology Security Evaluation Facility

Acronym	Definition
KAT	Known Answer Test
MAC	Message Authentication Code
ND	Network Device
NDcPP	Network Device Collaborative Protection Profile
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PAM	Pluggable Authentication Module
PCI	Peripheral Component Interconnect
PIN	Personal Identification Number
PKA	Public Key Authentication
PP	Protection Profile
QFSP	Quad Small Form-Factor Pluggable
RFC	Request For Comments
RJ-45	Registered Jack 45
RSA	Rivest, Shamir & Adleman
SAN	Subject Alternate Name
SAOS	Service Aggregation Operating System
SAR	Security Assurance Requirement
SFP+	Small Form-Factor Pluggable - Enhanced
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SSH	Secure Shell
ST	Security Target
TD	Technical Decision
TLS	Transport Layer Security
TOE	Target of Evaluation
TPM	Trusted Platform module
USB	Universal Serial Bus
USB-C	Universal Serial Bus - C
VM	Virtual Machine
vND	Virtual Network Device
VS	Virtual Server
WLAi	Wave Logic Adaptive interface