Infinera Corporation Transcend Network Management System Server 18.10.3 Security Target

Version 1.5
12/09/2022

Prepared for:

Infinera Corporation

9005 Junction Drive, Suite C
Annapolis Junction, MD 20701

Prepared By:

www.gossamersec.com

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is Infinera Corporation Transcend Network Management System Server provided by Infinera Corporation. The TOE is being evaluated as a software application.

The Security Target contains the following additional sections:

- Conformance Claims (Section 2)
- Security Objectives (Section 3)
- Extended Components Definition (Section 4)
- Security Requirements (Section 5)
- TOE Summary Specification (Section 6)

Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a parenthetical number placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.1 Security Target Reference

ST Title –Transcend Network Management System Server 18.10.3 Security Target

ST Version – Version 1.5

ST Date – 12/09/2022

1.2 TOE Reference

TOE Identification –Infinera Corporation Transcend Network Management System Server 18.10.3

TOE Developer – Infinera Corporation

Evaluation Sponsor – Infinera Corporation

1.3 TOE Overview

The Target of Evaluation (TOE) is Transcend Network Management System (TNMS) Server version 18.10.3 which consists of server and mediator components.

Note that the full TNMS system consists of client and server components, this evaluation is limited only to the server components since the Protection Profile for Application Software, Version 1.4, 07 October 2021 (ASPP14) does not support the evaluation of distributed application solutions. Please refer to *the Infinera Corporation Transcend Network Management System Client Security Target* where the other TNMS components are addressed.

1.4 TOE Description

The Transcend Network Management System (TNMS) is designed to provide end-to-end network and service management across multiple technologies and equipment vendors. The TNMS system has been developed with the following features:

- Network and service management with a broad feature set, from deep node-level troubleshooting to end-to-end service configuration and monitoring, across multiple technologies and equipment vendors for improved operational efficiency.
- An advanced graphical user interface providing overviews of the most relevant data and guidance through configuration steps.
- Flexible deployment configuration options that fit various needs of different network operators: from small networks to very large infrastructures, including support for virtualization and high availability.
- Clear user interfaces that provide user-friendly navigation and supporting responsive and efficient use.

For purposes of this evaluation, the TNMS Server is a software application that accepts management instructions via secure communication with a TNMS Client and then securely transfers management instructions to configured network entities. This evaluation addresses and is limited to the security functions claimed in Section 5 and further described in Section 6 of this Security Target (ST).

1.4.1 TOE Architecture

Software Requirements:

The TNMS Server is a pair of Java applications designed to run in the following operational environment:

- Red Hat Enterprise Linux (RHEL) 7.9 (64 bit) / CentOS 7.9 (64 bit) on a 64 bit Intel Xeon processor
- Amazon Corretto (OpenJDK) JDK/JRE 11.0.6

The TNMS Server TOE includes the following components that are co-located (and are depicted in Figure 1 below):

- Server component: The server component of the TNMS Server implements a TLS server that accepts TLS connections from a TNMS Client, operates on instructions sent from the TNMS Client and then uses mediator APIs as necessary to communicate with network entities to implement those instructions.
- Mediator component: The mediator component of the TNMS Server offers APIs used by the server component that enable it to securely communicate, using SSH (Java Secure Channel - JSch) as a client, with configured network entities via the mediator.

The TOE components communicate with each other through inter-process communication. The secure communication features all utilize Bouncy Castle (installed with the TNMS Server) for cryptographic operations.

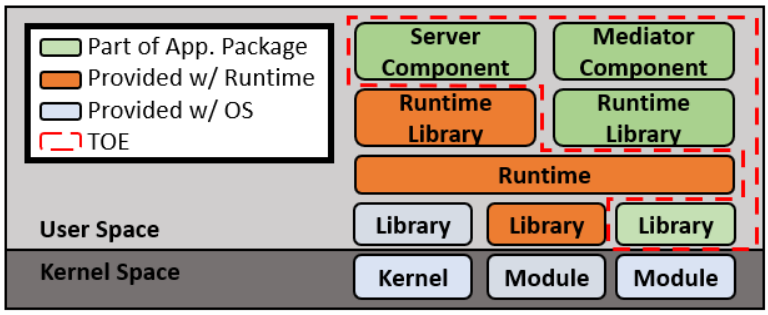

Figure 1. *TOE Architecture*

The TOE was installed and tested on the following platform

CentOS 7.9.2009 with Amazon Corretto 11.0.6 on Intel® Xeon® E5-2670

1.4.1.1 Physical Boundaries

The TNMS Server TOE is a pair of Java applications (server and mediator) running on Amazon Corretto (OpenJDK) JDK/JRE version 11.0.6 operating in a RHEL / CentOS 7.9 (64 bit) environment. The only external services the TOE depends on are a Certificate Authority for X509 certificate validation services, the TNMS Client with which the TNMS Server is configured to work, an Oracle database (that is installed on the same host platform and accessed locally), and network entities that are managed by the TNMS via secure communication from the mediator application.

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by TNMS:

- Cryptographic support
- User data protection
- Security management
- Privacy
- Protection of the TSF (TOE Security Function)
- Trusted path/channels

1.4.1.2.1 Cryptographic support

The TOE uses Automated Cryptographic Validation Test System (ACVTS)-validated cryptographic algorithm implementations, provided by the Bouncy Castle cryptographic module installed with the TOE, to support asymmetric key generation, encryption/decryption, signature generation and verification and establishment of trusted channels to protect data in transit. The TOE implements a TLS server to securely communicate with a TNMS Client, implements a SSH client to securely communicate with managed network entities, and implements functionality to securely store key data related to secure communications. The TOE also relies on the underlying Java platform to generate entropy that is used as input data for the TOE's deterministic random bit generator (DRBG).

1.4.1.2.2 User data protection

The TOE does not access any hardware resources or sensitive information repositories other than network access. No sensitive data outside of secure credentials is stored in non-volatile memory. Inbound and outbound network communications are restricted to those that are TOE-initiated to configured network elements, responding to incoming TNMS Clients TLS connections for remote management, and checking for updates.

1.4.1.2.3 Security management

After installation, an administrator manages the TOE through a TNMS client, and the TOE stores administrator configurations in its database stored in the platform file system.

When configured with default credentials or no credentials, the TOE restricts its functionality and only allows the ability to set new credentials. By default, the TOE is configured with file permissions to protect itself and its data from unauthorized access.

1.4.1.2.4 Privacy

The TOE does not transmit personally identifiable information (PII) over any network interfaces.

1.4.1.2.5 Protection of the TSF

The TOE protects itself against exploitation by implementing address space layout randomization (ASLR) and by not allocating any memory region for both write and execute permission. The TOE uses standard platform APIs and includes a number of third party libraries used to perform its functions.

The TOE includes mechanisms to check for updates and to query the current version of the application software. TOE software is digitally signed and distributed using the platform-supported package manager. The TOE does not update its own binary code in any way and when removed, all traces of the TOE application software are deleted.

1.4.1.2.6 Trusted path/channels

The TOE protects communications between itself and managed network entities using SSH and between itself and the TNMS Client using TLS.

1.4.2 TOE Documentation

The following user and administrative guidance is available:

Infinera Transcend Network Management System Server 18.10.3 Administrative Guidance for Common Criteria, Version 1.1, December 6, 2022

2. Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.
    - Part 3 Extended
- Package Claims:
    - Protection Profile for Application Software, Version 1.4, 10/7/2021
    - Functional Package for Transport Layer Security (TLS), Version 1.1, 2/12/2019
    - Functional Package for Secure Shell (SSH), Version 1.0, 5/13/2021 (ASPP14/PKGTLS11/SSH10)

Package	Technical Decision	Applied	Notes
PP_APP_V1.4	TD0669 – FIA_X509_EXT.1 Test 4 Interpretation	No	Not supported
PKG_SSH_EXT.1	TD0666 – Ambiguous intent of FCS_SSHS_EXT.1	No	Not supported
PP_APP_V1.4	TD0664 – Testing activity for FPT_TUD_EXT.2.2	Yes	Applied
PP_APP_V1.4	TD0659 – Change to Required NIST Curves for FCS_CKM.1/AK	Yes	Applied
PP_APP_V1.4	TD0655 – Mutual authentication in FTP_DIT_EXT.1 for SW App	Yes	Applied
PP_APP_V1.4	TD0650- Conformance claim sections updated to allow for MOD_VPNC_V2.3 and 2.4	No	VPNC not claimed
PP_APP_V1.4	TD0628 – Addition of Container Image to Package Format	Yes	Applied
PP_APP_V1.4	TD0626 – FCS_COP.1 Keyed Hash Selections	Yes	Applied
PP_APP_V1.4	TD0624 – Addition of DataStore for Stored and Setting Configuration Options	Yes	Applied
PKG_TLS_V1.1	TD0588 - Session Resumption Support in TLS package	No	Not supported
PKG_TLS_V1.1	TD0513 - CA Certificate loading	No	Not supported
PKG_TLS_V1.1	TD0499 - Testing with pinned certificates	No	Not supported
PKG_TLS_V1.1	TD0469 - Modification of test activity for FCS_TLSS_EXT.1.1 test 4.1	Yes	Applied
PKG_TLS_V1.1	TD0442 - Updated TLS Ciphersuites for TLS Package	Yes	Applied

2.1 Conformance Rationale

The ST conforms to the ASPP14/PKGTLS11/SSH10. As explained previously, the security problem definition, security objectives, and security requirements have been drawn from the PP.

3. Security Objectives

The Security Problem Definition may be found in the ASPP14/PKGTLS11/SSH10 and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The ASPP14/PKGTLS11/SSH10 offers additional information about the identified security objectives, but that has not been reproduced here and the ASPP14/PKGTLS11/SSH10 should be consulted if there is interest in that material.

In general, the ASPP14/PKGTLS11/SSH10 has defined Security Objectives appropriate for software application and as such are applicable to the Infinera Corporation Transcend Network Management System Server TOE.

3.1 Security Objectives for the Operational Environment

OE.PLATFORM The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.

OE.PROPER_ADMIN The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

OE.PROPER_USER The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.

4. Extended Components Definition

All of the extended requirements in this ST have been drawn from the ASPP14/PKGTLS11/SSH10. The ASPP14/PKGTLS11/SSH10 defines the following extended requirements and since they are not redefined in this ST the ASPP14/PKGTLS11/SSH10 should be consulted for more information in regard to those CC extensions.

Extended SFRs:

- ASPP14:FCS_RBG_EXT.1: Random Bit Generation Services
- ASPP14:FCS_RBG_EXT.2: Random Bit Generation from Application
- SSH10:FCS_SSH_EXT.1: SSH Protocol
- SSH10:FCS_SSHC_EXT.1: SSH Protocol - Client
- ASPP14:FCS_STO_EXT.1: Storage of Credentials
- PKGTLS11:FCS_TLS_EXT.1: TLS Protocol
- PKGTLS11:FCS_TLSS_EXT.1: TLS Server Protocol
- ASPP14:FDP_DAR_EXT.1: Encryption Of Sensitive Application Data
- ASPP14:FDP_DEC_EXT.1: Access to Platform Resources
- ASPP14:FDP_NET_EXT.1: Network Communications
- ASPP14:FMT_CFG_EXT.1: Secure by Default Configuration
- ASPP14:FMT_MEC_EXT.1: Supported Configuration Mechanism
- ASPP14:FPR_ANO_EXT.1: User Consent for Transmission of Personally Identifiable
- ASPP14:FPT_AEX_EXT.1: Anti-Exploitation Capabilities
- ASPP14:FPT_API_EXT.1: Use of Supported Services and APIs
- ASPP14:FPT_IDV_EXT.1: Software Identification and Versions
- ASPP14:FPT_LIB_EXT.1: Use of Third Party Libraries
- ASPP14:FPT_TUD_EXT.1: Integrity for Installation and Update
- ASPP14:FPT_TUD_EXT.2: Integrity for Installation and Update
- ASPP14:FTP_DIT_EXT.1: Protection of Data in Transit

Extended SARs:

- ALC_TSU_EXT.1: Timely Security Updates

5. Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the ASPP14/PKGTLS11/SSH10. The refinements and operations already performed in the ASPP14/PKGTLS11/SSH10 are not identified (e.g., highlighted) here, rather the requirements have been copied from the ASPP14/PKGTLS11/SSH10 and any residual operations have been completed herein. Of particular note, the ASPP14/PKGTLS11/SSH10 made a number of refinements and completed some of the SFR operations defined in the Common Criteria (CC) and that PP should be consulted to identify those changes if necessary.

The SARs are also drawn from the ASPP14/PKGTLS11/SSH10. The ASPP14/PKGTLS11/SSH10 should be consulted for the assurance activity definitions.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by Infinera Corporation Transcend Network Management System Server TOE.

Requirement Class	Requirement Component
FCS: Cryptographic support	ASPP14:FCS_CKM.1: Cryptographic Key Generation Services
	ASPP14:FCS_CKM.1/AK: Cryptographic Asymmetric Key Generation
	ASPP14:FCS_CKM.1/PBKDF: Password Conditioning
	ASPP14:FCS_CKM.1/SK: Cryptographic Symmetric Key Generation
	ASPP14:FCS_CKM.2: Cryptographic Key Establishment
	ASPP14:FCS_COP.1/Hash: Cryptographic Operation - Hashing
	ASPP14:FCS_COP.1/KeyedHash: Cryptographic Operation - Keyed-Hash Message Authentication
	ASPP14:FCS_COP.1/Sig: Cryptographic Operation - Signing
	ASPP14:FCS_COP.1/SKC: Cryptographic Operation - Encryption/Decryption
	ASPP14:FCS_RBG_EXT.1: Random Bit Generation Services
	ASPP14:FCS_RBG_EXT.2: Random Bit Generation from Application
	SSH10:FCS_SSH_EXT.1: SSH Protocol
	SSH10:FCS_SSHC_EXT.1: SSH Protocol - Client
	ASPP14:FCS_STO_EXT.1: Storage of Credentials
	PKGTLS11:FCS_TLS_EXT.1: TLS Protocol
	PKGTLS11:FCS_TLSS_EXT.1: TLS Server Protocol
FDP: User data protection	ASPP14:FDP_DAR_EXT.1: Encryption Of Sensitive Application Data
	ASPP14:FDP_DEC_EXT.1: Access to Platform Resources
	ASPP14:FDP_NET_EXT.1: Network Communications
FMT: Security management	ASPP14:FMT_CFG_EXT.1: Secure by Default Configuration
	ASPP14:FMT_MEC_EXT.1: Supported Configuration Mechanism
	ASPP14:FMT_SMF.1: Specification of Management Functions
FPR: Privacy	ASPP14:FPR_ANO_EXT.1: User Consent for Transmission of Personally Identifiable
FPT: Protection of the TSF	ASPP14:FPT_AEX_EXT.1: Anti-Exploitation Capabilities
	ASPP14:FPT_API_EXT.1: Use of Supported Services and APIs
	ASPP14:FPT_IDV_EXT.1: Software Identification and Versions
	ASPP14:FPT_LIB_EXT.1: Use of Third Party Libraries

	ASPP14:FPT_TUD_EXT.1: Integrity for Installation and Update
	ASPP14:FPT_TUD_EXT.2: Integrity for Installation and Update
FTP: Trusted path/channels	ASPP14:FTP_DIT_EXT.1: Protection of Data in Transit

Table 1 TOE Security Functional Components

5.1.1 Cryptographic support (FCS)

5.1.1.1 Cryptographic Key Generation Services (ASPP14:FCS_CKM.1)

ASPP14:FCS_CKM.1.1

The application shall [***implement asymmetric key generation***].

5.1.1.2 Cryptographic Asymmetric Key Generation (ASPP14:FCS_CKM.1/AK)

ASPP14:FCS_CKM.1.1/AK

The application shall [***implement functionality***] to 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-384 and [P-256. P-521] that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.4,***].

5.1.1.3 Password Conditioning (ASPP14:FCS_CKM.1/PBKDF)

ASPP14:FCS_CKM.1.1/PBKDF

A password/passphrase shall perform [**PBKDFv2 (HMAC-SHA2-256)**] in accordance with a specified cryptographic algorithm as specified in FCS_COP.1/KeyedHash, with [**10,000**] iterations, and output cryptographic key sizes [***256***] that meet the following: NIST SP 800-132.

ASPP14:FCS_CKM.1.2/PBKDF

The TSF shall generate all salts using a RBG that meets FCS_RBG_EXT.1 and with entropy corresponding to the security strength selected for PBKDF in FCS_CKM.1.1/PBKDF.

5.1.1.4 Cryptographic Symmetric Key Generation (ASPP14:FCS_CKM.1/SK)

ASPP14:FCS_CKM.1.1/SK

The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes [***128 bit, 256 bit***].

5.1.1.5 Cryptographic Key Establishment (ASPP14:FCS_CKM.2)

ASPP14:FCS_CKM.2.1

The application shall [***implement functionality***] to perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [***Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography'***].

5.1.1.6 Cryptographic Operation - Hashing (ASPP14:FCS_COP.1/Hash)

ASPP14:FCS_COP.1.1/Hash

The application shall perform cryptographic hashing services in accordance with a specified

cryptographic algorithm [***SHA-1, SHA-256, SHA-384, SHA-512***] and message digest sizes [***160, 256, 384, 512***] bits that meet the following: FIPS Pub 180-4.

5.1.1.7 Cryptographic Operation - Keyed-Hash Message Authentication (ASPP14:FCS_COP.1/KeyedHash)

ASPP14:FCS_COP.1.1/KeyedHash

The application shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm [***HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512***] and [***HMAC-SHA-1***] with key sizes [**160, 256, 384, 512**] and message digest sizes [***256, 384, 512***] and [***160***] bits that meet the following: FIPS Pub 198-1, 'The Keyed-Hash Message Authentication Code' and FIPS Pub 180-4, 'Secure Hash Standard'. (TD0626 applied)

5.1.1.8 Cryptographic Operation - Signing (ASPP14:FCS_COP.1/Sig)

ASPP14:FCS_COP.1.1/Sig

The application shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm [***RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 4, ECDSA schemes using 'NIST curves' P-256, P-384 and [P-521] that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 5***].

5.1.1.9 Cryptographic Operation - Encryption/Decryption (ASPP14:FCS_COP.1/SKC)

ASPP14:FCS_COP.1.1/SKC

The application shall perform encryption/decryption in accordance with a specified cryptographic algorithm [***AES-CBC (as defined in NIST SP 800-38A) mode, AES-GCM (as defined in NIST SP 800-38D) mode, AES-CTR (as defined in NIST SP 800-38A) mode***] and cryptographic key sizes [***128-bit, 256-bit***].

5.1.1.10 Random Bit Generation Services (ASPP14:FCS_RBG_EXT.1)

ASPP14:FCS_RBG_EXT.1.1

The application shall [***invoke platform-provided DRBG functionality, implement DRBG functionality***] for its cryptographic operations.

5.1.1.11 Random Bit Generation from Application (ASPP14:FCS_RBG_EXT.2)

ASPP14:FCS_RBG_EXT.2.1

The application shall perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using [***Hash_DRBG (any)***].

ASPP14:FCS_RBG_EXT.2.2

The deterministic RBG shall be seeded by an entropy source that accumulates entropy from a platform-based DRBG and [***no other noise source***] with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.

5.1.1.12 SSH Protocol (SSH10:FCS_SSH_EXT.1)

SSH10:FCS_SSH_EXT.1.1

The TOE shall implement SSH acting as a [***client***] in accordance with that complies with RFCs 4251, 4252, 4253, 4254, [***4344, 5656, 6668***] and no other standard.

SSH10:FCS_SSH_EXT.1.2

The TSF shall ensure that the SSH protocol implementation supports the following authentication methods:
[***'password' (RFC 4252),***
'publickey' (RFC 4252):
[ssh-rsa (RFC 4253),

ecdsa-sha2-nistp256 (RFC 5656),
ecdsa-sha2-nistp384 (RFC 5656)]]
and no other methods.

SSH10:FCS_SSH_EXT.1.3
The TSF shall ensure that, as described in RFC 4253, packets greater than [**262,126**] in an SSH transport connection are dropped.

SSH10:FCS_SSH_EXT.1.4
The TSF shall protect data in transit from unauthorised disclosure using the following mechanisms: [***aes128-ctr (RFC 4344), aes256-ctr (RFC 4344), aes128-cbc (RFC 4253), aes256-cbc (RFC 4253)***] and no other mechanisms.

SSH10:FCS_SSH_EXT.1.5
The TSF shall protect data in transit from modification, deletion, and insertion using: [***hmac-sha2-256 (RFC 6668)***] and no other mechanisms.

SSH10:FCS_SSH_EXT.1.6
The TSF shall establish a shared secret with its peer using:
[***ecdh-sha2-nistp256 (RFC 5656),***
ecdh-sha2-nistp384 (RFC 5656),
ecdh-sha2-nistp521 (RFC 5656)]
and no other mechanisms.

SSH10:FCS_SSH_EXT.1.7
The TSF shall use SSH KDF as defined in [***RFC 5656 (Section 4)***] to derive the following cryptographic keys from a shared secret: session keys.

SSH10:FCS_SSH_EXT.1.8
The TSF shall ensure that [***a rekey of the session keys***] occurs when any of the following thresholds are met:
- one hour connection time
- no more than one gigabyte of transmitted data, or
- no more than one gigabyte of received data.

5.1.1.13 SSH Protocol - Client (SSH10:FCS_SSHC_EXT.1)

SSH10:FCS_SSHC_EXT.1.1
The TSF shall authenticate its peer (SSH server) using: [***using a local database by associating each host name with a public key corresponding to the following list: [ssh-rsa (RFC 4253), ecdsa-sha2-nistp256 (RFC 5656), ecdsa-sha2-nistp384 (RFC 5656)]***] as described in RFC 4251 section 4.1.

5.1.1.14 Storage of Credentials (ASPP14:FCS_STO_EXT.1)

ASPP14:FCS_STO_EXT.1.1
The application shall [***implement functionality to securely store [administrator passwords, TLS server certificates (and private keys), and SSHv2 private keys and passwords] according to [FCS_COP.1/SKC, FCS_CKM.1/PBKDF]***] to non-volatile memory.

5.1.1.15 TLS Protocol (PKGTLS11:FCS_TLS_EXT.1)

PKGTLS11:FCS_TLS_EXT.1.1
The product shall implement [***TLS as a server,***]

5.1.1.16 TLS Server Protocol (PKGTLS11:FCS_TLSS_EXT.1)

PKGTLS11:FCS_TLSS_EXT.1.1
The product shall implement TLS 1.2 (RFC 5246) and [***no earlier TLS versions***] as a server that supports the cipher suites [
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289]

and no other cipher suites, and also supports functionality for [***none***] (TD0442 & TD0588 applied)

PKGTLS11:FCS_TLSS_EXT.1.2

The product shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [**TLS 1.1**]

PKGTLS11:FCS_TLSS_EXT.1.3

The product shall perform key establishment for TLS using [***ECDHE parameters using elliptic curves [secp256r1, secp384r1, secp521r1] and no other curves,***]

5.1.2 User data protection (FDP)

5.1.2.1 Encryption Of Sensitive Application Data (ASPP14:FDP_DAR_EXT.1)

ASPP14:FDP_DAR_EXT.1.1

The application shall [***protect sensitive data in accordance with FCS_STO_EXT.1***] in non-volatile memory.

5.1.2.2 Access to Platform Resources (ASPP14:FDP_DEC_EXT.1)

ASPP14:FDP_DEC_EXT.1.1

The application shall restrict its access to [***network connectivity***].

ASPP14:FDP_DEC_EXT.1.2

The application shall restrict its access to [***no sensitive information repositories***].

5.1.2.3 Network Communications (ASPP14:FDP_NET_EXT.1)

ASPP14:FDP_NET_EXT.1.1

The application shall restrict network communication to [***user-initiated communication for [connecting to managed network entities], respond to [connection attempts from TNMS Clients]***].

5.1.3 Security management (FMT)

5.1.3.1 Secure by Default Configuration (ASPP14:FMT_CFG_EXT.1)

ASPP14:FMT_CFG_EXT.1.1

The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials.

ASPP14:FMT_CFG_EXT.1.2

The application shall be configured by default with file permissions which protect the application's binaries and data files from modification by normal unprivileged user.

5.1.3.2 Supported Configuration Mechanism (ASPP14:FMT_MEC_EXT.1)

ASPP14:FMT_MEC_EXT.1.1

The application shall [***invoke the mechanisms recommended by the platform vendor for storing and setting configuration options***].

5.1.3.3 Specification of Management Functions (ASPP14:FMT_SMF.1)

ASPP14:FMT_SMF.1.1

The TSF shall be capable of performing the following management functions [***[Configure TLS Server credentials, Configure network elements]***].

5.1.4 Privacy (FPR)

5.1.4.1 User Consent for Transmission of Personally Identifiable (ASPP14:FPR_ANO_EXT.1)

ASPP14:FPR_ANO_EXT.1.1
The application shall [***not transmit PII over a network***].

5.1.5 Protection of the TSF (FPT)

5.1.5.1 Anti-Exploitation Capabilities (ASPP14:FPT_AEX_EXT.1)

ASPP14:FPT_AEX_EXT.1.1
The application shall not request to map memory at an explicit address except for [**no exceptions**].
ASPP14:FPT_AEX_EXT.1.2
The application shall [***not allocate any memory region with both write and execute permissions***].
ASPP14:FPT_AEX_EXT.1.3
The application shall be compatible with security features provided by the platform vendor.
ASPP14:FPT_AEX_EXT.1.4
The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.
ASPP14:FPT_AEX_EXT.1.5
The application shall be built with stack-based buffer overflow protection enabled.

5.1.5.2 Use of Supported Services and APIs (ASPP14:FPT_API_EXT.1)

ASPP14:FPT_API_EXT.1.1
The application shall use only documented platform APIs.

5.1.5.3 Software Identification and Versions (ASPP14:FPT_IDV_EXT.1)

ASPP14:FPT_IDV_EXT.1.1
The application shall be versioned with [***/major and minor version and build number/***]

5.1.5.4 Use of Third Party Libraries (ASPP14:FPT_LIB_EXT.1)

ASPP14:FPT_LIB_EXT.1.1
The application shall be packaged with only [**the following third-party components**].

Component name	Component version
ASM	4.2 5.1
AXL Software Radius client	4.0
Angular	1.4.8
Animal Sniffer Annotations	1.17
Apache ActiveMQ	5.16.3
Apache Common Annotations 1.3 API	1.0.0.Final
Apache Commons CLI	1.2 1.4
Apache Commons Codec	1.11
Apache Commons Collection	3.2.2 4.2
Apache Commons DBCP	1.7

Apache Commons DbUtils	1.7
Apache Commons Exec	1.3
Apache Commons IO	2.6 2.7
Apache Commons JCS :: Core	2.2.1
Apache Commons Lang	2.6 3 3.1 3.7 3.8 3.8.1
Apache Commons Logging	1.1.1 1.2
Apache Commons Net	2.0 3.6
Apache Commons Pool	1.6
Apache Commons Text	1.4 1.6 1.8
Apache Commons Validator	1.6
Apache Commons jexl	2.1.1
Apache Groovy	2.4.17
Apache HttpClient	3.1 4.5.6 4.5.13
Apache HttpComponents Core	4.4.10
Apache Kafka	1.1.0
Apache Log4j	1.2.17 1.2.15 2.7 2.10.0 2.11.2 2.13.3
Apache Tomcat	3.2.3 9.0.54 9.0.68
Apache XML Commons	1.4.01 2.6.0
Apache XML Graphics Commons	2.3 2.6
Apache Xalan (Java)	2.7.2
Apache Xerces2 J	2.9.1 2.12.0.SP03
AspectJ	1.9.5
AsyncHttpClient	1.9.40
AutoValue Annotations	1.6.5
Avalon Framework API	4.1.4
BCTLS FIPS	1.0.9
Batik XML utility library	1.10 1.16

Bootstrap (Twitter)	3.4.1
Bouncy Castle	1.45 1.61 1.64
Bouncy Castle Provider - FIPS	1.0.2 1.0.2.1
Bouncy Castle TLS (FIPS)	1.0.2.1
CDI APIs	2.0
Castor	0.9.5
Checker Qual	2.5.2
Common Annotations	1.0.2.Final
Dagger 2 dagger	2.21
Db4o	7.12.132
Disruptor Framework	3.4.2
Elsa Serialization	3.0.0.M7001
Expression Language	3.0.0
Expression Language API	1.0.7.Final
Extended StAX API	1.8.1
FindBugs jsr305	1.3.9 3.0.2
GeoServer	2.17.0
Goldman Sachs Collections	5.1.0
Google Gson	2.8.5 2.8.9
Google Guice	3.0 4.0
Guava	26.0
Guava: Google Core Libraries for Java	18.0-rc 26.0 27.0
H2 Database Engine	1.4.196
Hamcrest	1.3
HawtJNI Runtime	1.11
Hibernate JPA 2 Metamodel Generator	5.3.7.FFinal
Hibernate Validator	6.0.18.Final
HyperSQL Database Engine	1.8.0.10
Install Anywhere	2018
J2EE Connector Architecture	1.5
J2EE Management	1.0.1
J2ObjC Annotations	1.3
JAVAX RMI API	1.0.6.Final
JAXB Implementation	2.3.2
JAXB Runtime	2.3.2
JBoss EJB client	4.0.12.Final
JBoss Logging	3.2.1.Final 3.3.1.Final

JBoss Marshalling API	2.0.9.Final
JBoss Remoting	5.0.0.Final 5.0.8.Final
JBoss classfilewriter	1.2.3.Final
JCL 1.2 Implemented Over SLF4J	1.7.26
JDOM	1.1 1.1.3 2.0.6
JFreeChart	1.0.13
JFreeReport Extensions	0.8.7
JFtp - FTP Client	1.2.3
JGraphT - Core	1.2.0
JSON Web Token Support	0.7.0 0.9.1
JSch	0.1.55 0.1.55a
JUL to SLF4J bridge	1.7.26
JUnit	3.8.1
JZlib	1.1.3
JacORB	3.4
Jackson	2.7.4 2.9.8 2.10.2 2.10.3 2.12.5
Jakarta Annotations API	21.3.4
Jakarta JCS	1.3
Jakarta XML	2.3.2
Jansi	1.18
Java Architecture for XML Binding	2.3.2
Java Communications API	1.0
Java DMK	5.1
Java Mail	1.4
Java Servlet API	3.1.0
Java Servlet Technology	2.2b
Java gRPC	1.26.0 1.26.1
Java inject from the JSR-330 Expert Group	1.0
Java(TM) EE Interceptors 1.2 API	1.0.0.Final
JavaBeans Activation Framework API jar	1.2.1
JavaBeans(TM) Activation Framework Specification	1.1
JavaHelp	2.0_01
JavaServer Pages (TM) TagLib Implementation	1.2
JavaTM Authentication and Authorization Service (JAAS)	1.0
Javassist	3.21.0-GA

Jcommander	1.48.0
Jetbrains annotations	13.0
Jline	3.14.1
Jscape	8.5.0
Koloboke Collections API	1.0.0
Kotlin Stdlib	1.3.10
MapStruct Core JDK 8	1.2.0.Final
Metrics Core	4.0.3
Metrics Integration with JMX	4.0.3
ModeShape	5.4.1.Final
Monfox TL1	3.10.32
Netty Project	3.10.6.Final 4.1.48.Final
OW2 Utilities :: Base64	2.0.0
OpenCensus	0.23.0 0.25.0
OpenFusion CORBA Services	4.2.5
Openmap	5.1.15
Oracle Database JDBC Drivers	18.3.0.0
Oracle Fast Infoset	1.2.16
Oracle iStack	3.0.8
Picocli - a might tiny Command Line Interface	4.3.2
Protocol Buffer Java API	3.11.0
Quartz	1.8.6
Querydsl	3.7.4 4.2.1
Reactor Components	2.0.8.RELEASE
Remoting-jmx	3.0.1.Final 3.0.4.Final
SLF4J API Module	1.7.25
SLF4J Binding	2.11.1 2.13.3 2.7
SNMP4J	2.5.0 2.5.6
Simple Logging Façade for Java (SLF4J)	1.7.2 1.7.13 1.7.21 1.7.30
SmoothieMap	1.3
SnakeYAML	1.17
Spring	5.0.16
Spring Boot	1.5.22.RELEASE
Spring Boot Log4J2 Starter	1.5.22.RELEASE
Spring Boot Undertow Starter	1.5.20.RELEASE
Spring Framework	5.0.16.RELEASE

	4.3.25.RELEASE
Spring Security	4.2.13 4.2.14
Stax2 API	4.2
Stormpot	2.4.1
Super CSV	2.4.0
TXW Runtime	2.3.2
Thymeleaf	2.1.6.RELEASE
Trove for Java	3.0.3
Tyrex	1.0.1
Undertow Core	2.0.15.Final
VT Crypt Library	2.1.4
VT Dictionary Libraries	3.0
VT Password	3.1.2
Weld Core	3.0.5.Final
Wildfly	15.0
Woodstox	6.0.3
XML Commons External Components XML API Extensions	1.3.04
Xerces	3.1
XmlSchema Core	2.2.3
atmosphere-cdi	2.5.2
atmosphere-runtime	2.5.3
atmosphere-socketio	2.5.2
cglib	3.2.8
codegen	0.6.8
concurrent	1.0
config - com.typesafe:config	1.3.3
dom4j: flexible XML framework for Java	2.1.1
edtFTPj	2.0.3
error-prone annotations	2.2.0 2.3.2
exp4j	0.3.11
fast-serialization	2.57
google-gson	2.1 2.8.6
image4j	0.7
io.grpc:grpc-context	1.25
istack common utility code runtime	3.0.8
istack commons tools	3.0.7
jQuery	2.1.4
jacorb	2.3.2.redhat-6
javax.ejb API	3.2
javax.transaction API	1.2

jgraph	5.13.0.0
jgraphx	1.5.1.3
jmxremote_optional repackaged as module	5.0
jmxtrans	Build 172
jt-classbreaks	1.1.14
kotlin-argparser	2.0.7
mysema-commons-lang	0.2.4
level db	0.12
logkit	20020529
net.sourceforge.streamsupport:java9-concurrent-backport	1.1.1
objenesis	2.5.1
ognl	3.2.13
ojdbc	11.2.0.3.0
ojdbc8	18.3.0.0.0
perfmark:perfmark-api	0.19.0
reflections	0.9.11
river	2.0.9.Final
spring-boot-actuator	1.5.22.RELEASE
swingx	1.6.4
syslog4j	0.9.46
thymeleaf-extras-springsecurity4	2.1.2.RELEASE
thymeleaf-layout-dialect	1.4.0
thymeleaf-spring4	2.1.6.RELEASE
ucp	1.4.0
unbescape	2.1.6.RELEASE
wasync	2.1.7
webdavlib	2.0
wildfly-common	1.4.0.Final
xenocom	0.0.7
xnio-api	3.5.1.Final 3.6.5.Final

].

5.1.5.5 Integrity for Installation and Update (ASPP14:FPT_TUD_EXT.1)

ASPP14:FPT_TUD_EXT.1.1
The application shall [***provide the ability***] to check for updates and patches to the application software.

ASPP14:FPT_TUD_EXT.1.2
The application shall [***provide the ability***] to query the current version of the application software.

ASPP14:FPT_TUD_EXT.1.3
The application shall not download, modify, replace or update its own binary code.

ASPP14:FPT_TUD_EXT.1.4
Application updates shall be digitally signed such that the application platform can cryptographically verify them prior to installation.
ASPP14:FPT_TUD_EXT.1.5
The application is distributed [***as an additional software package to the platform OS***].

5.1.5.6 Integrity for Installation and Update (ASPP14:FPT_TUD_EXT.2)

ASPP14:FPT_TUD_EXT.2.1
The application shall be distributed using ***[the format of the platform-supported package manager].*** (TD0628 applied)
ASPP14:FPT_TUD_EXT.2.2
The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events
ASPP14:FPT_TUD_EXT.2.3
The application installation package shall be digitally signed such that its platform can cryptographically verify them prior to installation.

5.1.6 Trusted path/channels (FTP)

5.1.6.1 Protection of Data in Transit (ASPP14:FTP_DIT_EXT.1)

ASPP14:FTP_DIT_EXT.1.1
The application shall [***encrypt all transmitted [data] with [TLS as a server as defined in the Functional Package for TLS and also supports functionality for [none], SSH as defined in the Functional Package for Secure Shell]***]
between itself and another trusted IT product.

5.2 TOE Security Assurance Requirements

The SARs for the TOE are the components as specified in Part 3 of the Common Criteria. Note that the SARs have effectively been refined with the assurance activities explicitly defined in association with both the SFRs and SARs.

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1: Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance
	AGD_PRE.1: Preparative Procedures
ALC: Life-cycle support	ALC_CMC.1: Labelling of the TOE
	ALC_CMS.1: TOE CM Coverage
	ALC_TSU_EXT.1: Timely Security Updates
ATE: Tests	ATE_IND.1: Independent Testing - Conformance
AVA: Vulnerability assessment	AVA_VAN.1: Vulnerability Survey

Table 2 Assurance Components

5.2.1 Development (ADV)

5.2.1.1 Basic Functional Specification (ADV_FSP.1)

ADV_FSP.1.1d
The developer shall provide a functional specification.

ADV_FSP.1.2d

The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.1.1c

The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2c

The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3c

The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4c

The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.2 Guidance documents (AGD)

5.2.2.1 Operational User Guidance (AGD_OPE.1)

AGD_OPE.1.1d

The developer shall provide operational user guidance.

AGD_OPE.1.1c

The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2c

The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3c

The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4c

The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5c

The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences, and implications for maintaining secure operation.

AGD_OPE.1.6c

The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7c

The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 Preparative Procedures (AGD_PRE.1)

AGD_PRE.1.1d
The developer shall provide the TOE, including its preparative procedures.

AGD_PRE.1.1c
The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2c
The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2e
The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle support (ALC)

5.2.3.1 Labelling of the TOE (ALC_CMC.1)

ALC_CMC.1.1d
The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.1.1c
The application shall be labelled with a unique reference.

ALC_CMC.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 TOE CM Coverage (ALC_CMS.1)

ALC_CMS.1.1d
The developer shall provide a description in the TSS of how timely security updates are made to the TOE. Application developers must support updates to their products for purposes of fixing security vulnerabilities.

ALC_CMS.1.1c
The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2c
The configuration list shall uniquely identify the configuration items.

ALC_CMS.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.3 Timely Security Updates (ALC_TSU_EXT.1)

ALC_TSU_EXT.1.1d
The developer shall provide a description in the TSS of how timely security updates are made to the TOE. Note: Application developers must support updates to their products for purposes of fixing security vulnerabilities.

ALC_TSU_EXT.1.2d
The developer shall provide a description in the TSS of how users are notified when updates change security properties or the configuration of the product.

ALC_TSU_EXT.1.1c
The description shall include the process for creating and deploying security updates for the TOE software.

ALC_TSU_EXT.1.2c
The description shall express the time window as the length of time, in days, between public disclosure of a vulnerability and the public availability of security updates to the TOE.

ALC_TSU_EXT.1.3c
The description shall include the mechanisms publicly available for reporting security issues pertaining to the TOE.

Note: The reporting mechanism could include web sites, email addresses, as well as a means to protect the sensitive nature of the report (e.g., public keys that could be used to encrypt the details of a proof-of-concept exploit).

ALC_TSU_EXT.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Tests (ATE)

5.2.4.1 Independent Testing - Conformance (ATE_IND.1)

ATE_IND.1.1d
The developer shall provide the TOE for testing.

ATE_IND.1.1c
The TOE shall be suitable for testing.

ATE_IND.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2e
The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.5 Vulnerability assessment (AVA)

5.2.5.1 Vulnerability Survey (AVA_VAN.1)

AVA_VAN.1.1d
The developer shall provide the TOE for testing.

AVA_VAN.1.1c
The TOE shall be suitable for testing.

AVA_VAN.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence..

AVA_VAN.1.2e
The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3e
The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This chapter describes the security functions:

- Cryptographic support
- User data protection
- Security management
- Privacy
- Protection of the TSF
- Trusted path/channels

6.1 Cryptographic support

ASPP14:FCS_CKM.1:

The TOE generates asymmetric ECDH keys during TLS and SSHv2 connections.

ASPP14:FCS_CKM.1/AK:

The TOE generates P-256 and P-384 EDCHE keys as part of TLS secured connections from incoming TNMS Clients (administrative traffic). The TOE also supports SSHv2 session establishment using ECDH (ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp512). The TOE secures configuration connections to network devices under its administrative management control.

ASPP14:FCS_CKM.1/PBKDF

Within TLS protected Client connections, the TOE receives a SHA-1 hash value derived from the administrator's password. The TOE then uses that binary value, appends a random 16 byte salt, and then subjects the concatenation to PBKDFv2 (HMAC-SHA-256) conditioning to generate a 128-bit output. The TOE generates the per-user 16-byte salt using its Bouncy Castle DRBG.

ASPP14:FCS_CKM.1/SK:

The TOE generates 128 and 256-bit AES keys during the TLS handshake and during SSHv2 session establishment and the TOE uses its Bouncy Castle cryptographic library to generate the random values used during these connections. As required by ASPP14, the TOE's Bouncy Castle library calls the java.security.SecureRandom class [specifically calling SecureRandom.generateSeed()] to obtain a 256-bit seed, which is assumed to contain 256-bits of entropy.

ASPP14:FCS_CKM.2:

The TOE uses ECDHE as part of its TLS connection from TNMS Clients, and the TOE additionally uses ECDH in SSHv2 key exchange for to TOE connections to network devices that the TOE manages.

ASPP14:FCS_COP.1:

The TOE's Bouncy Castle cryptographic library (version 1.0.2.1) provides the following algorithm implementations and has algorithms certificates for each.

SFR	Algorithm	NIST Standard	Cert#
FCS_CKM.1/AK (Key Gen)	RSA IFC key generation 2048 bits	FIPS 186-4, RSA	A2313
	ECDSA ECC key gen P-256, 384, 521	FIPS 186-4, ECDSA	A2313
FCS_CKM.1/PDKDF (Password Conditioning)	PBKDFv2 (HMAC-SHA2-256)	SP 800-108	A2313
FCS_CKM.2 (Key Establishment)	ECC-based key exchange	SP 800-56A, KAS ECC	A2313
FCS_COP.1/SKC	AES Encryption/Decryption	FIPS 197, SP 800-38	A2313

SFR	Algorithm	NIST Standard	Cert#
	CBC, GCM, CTR 128, 256 bits		
FCS_COP.1/Hash	SHA Hashing SHA-1, 256, 384, 512	FIPS 180-4	A2313
FCS_COP.1/Sig	RSA Sign/Verify 2048 bits	FIPS 186-4, RSA	A2313
	ECDSA Sign/Verify P-256, 384, 521	FIPS 186-4, ECDSA	A2313
FCS_COP.1/KeyedHash	HMAC-SHA HMAC-SHA 1, 256, 384, 512	FIPS 198-1 & 180-4	A2313
FCS_RBG_EXT.2 (Random)	DRBG Bit Generation Hash DRBG 256 bits	SP 800-90A	A2313

Table 6-1 Bouncy Castle CAVP Certificates

ASPP14:FCS_COP.1/Hash:

The TOE uses SHA-1, SHA-256, SHA-384, and SHA-512 hashing when generating TLS server authentication signatures and while verifying SSHv2 pubkey signatures received from managed network devices. The TOE also uses SHA-256 during PBKDFv2 transformation of administrator passwords.

ASPP14:FCS_COP.1/KeyedHash:

The TOE uses HMAC as part of TLS and SSHv2 (for encrypted data integrity) and PBKDFv2 (as the one-way function).

ASPP14:FCS_COP.1/Sig:

The TOE generates a digital signature while acting as a TLS server, as part of the TLS certificate message. The TOE also verifies the signatures returned by managed devices while establishing SSHv2 connections.

ASPP14:FCS_COP.1/SKC:

The TOE can negotiate both AES-CBC and AES-CTR ciphers as part of an SSHv2 connections and negotiate AES-GCM as part of a TLS connection. When generating a starting counter value, the TOE generates a random number using its Bouncy Castle random number generator.

ASPP14:FCS_RBG_EXT.1:

The TOE implements a DRBG in its Bouncy Castle library and uses that DRBG when generating per-user salts as well as when generating random values used in TLS handshakes, PKBDF credential transformation, and SSHv2 sessions. The TOE also invokes the platforms-provided DRBG functionality in order to obtain seeding material for its DRBG.

ASPP14:FCS_RBG_EXT.2:

The TOE obtains entropy to seed its DRBG from the platform through the /dev/urandom character device.

SSH10:FCS_SSH_EXT.1.1:

The TOE acts as an SSH Client and complies with RFC 5656 (“Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer”) in addition to the other RFCs mandated by the module.

SSH10:FCS_SSH_EXT.1.2:

The TOE supports ‘password’ and ‘publickey’ authentication methods. For public key, the TOE supports both RSA (ssh_rsa) and ECDSA (ecdsa-sha2-nistp256 and ecdsa-sha2-nistp384) methods. The TOE uses the password option when establishing connections with managed elements supporting or requiring password authentication. The TOE uses the administrator specified password when establishing an SSH connection.

SSH10:FCS_SSH_EXT.1.3:

The TOE's Jsch implementation tracks the size of incoming SSHv2 packets (at the transport layer) and aborts processing and discards any packet exceeding a size of 262,126 bytes

SSH10:FCS_SSH_EXT.1.4:

The TOE supports both 128 and 256 AES keys and both the CBC and CTR modes of feedback.

SSH10:FCS_SSH_EXT.1.5:

The TOE supports using HMAC-SHA2-256 to protect SSH packet integrity.

SSH10:FCS_SSH_EXT.1.6:

The TOE supports ECP groups across NIST P-256/384/521 curves (i.e., ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521) for key exchange.

SSH10:FCS_SSH_EXT.1.7:

The TOE supports the KDF defined RFC 5656 for ECDH.

SSH10:FCS_SSH_EXT.1.8:

The TOE enforces a rekeying of the SSH session at the thresholds defined by the SFR.

SSH10:FCS_SSHC_EXT.1:

ASPP14:FCS_STO_EXT.1:

The TNMS server stores administrative passwords, TNMS's TLS server certificates (and private keys), and SSHv2 private keys and passwords. The administrative password is used to access the TOE from the external TNMS Client. The TLS certificates are used to authenticate the TLS channel the TOE and the TNMS client use to communicate. The SSH authentication keys are used to authenticate the TOE to any configured network element.

The TOE does not store administrative passwords directly, but instead, derives a value from the received from the TNMS client using PBKDF, and stores that derived value in its configuration database. The TOE compares these stored values to those newly derived from the administrator's password received from the TNMS Client to decide whether to grant access to the Client.

The TOE protects private keys (TLS server and SSH client) by storing them in its Bouncy Castle keystore in the OS provided filesystem.

PKGTLS11:FCS_TLS_EXT.1:

The TOE's TLS server (which accepts incoming administrative connections from TNMS Clients) supports only TLS version 1.2 and rejects connection attempts from all prior TLS versions.

The TOE supports the ciphersuites listed in section 5.1.1.16 (ECDHE with AES GCM cipher suites) and the TOE selects the elliptic curve (NIST P-256, 834, or 521) depending upon the supported curves specified in the client hello message.

6.2 User data protection

ASPP14:FDP_DAR_EXT.1:

The TOE stores sensitive data including the server login password and SSH client credentials within its configuration database. The TOE also has a TLS Server Certificate and private key used for incoming TLS connections stored in a Bouncy Castle-encrypted Keystore stored in the TOE's installation directory. The TOE does not process any sensitive data outside of the credentials claimed as a part of FCS_STO_EXT.1

ASPP14:FDP_DEC_EXT.1:

The TOE requires an active network connection.

ASPP14:FDP_NET_EXT.1:

The TOE accepts incoming, administrative TLS connections from TNMS Clients and allows administrators to initiate SSH secured network connection to managed network devices

6.3 Security management

ASPP14:FMT_CFG_EXT.1:

The TOE requires that administrators (when they connected through a TNMS Client) authenticate themselves. The TOE comes with a default administrative user and password, and during the initial configuration of the TOE, the initial administrator must set a new password, after which the TOE no longer accepts the default password.

ASPP14:FMT_MEC_EXT.1:

The TOE makes use of its application storage area within its Linux operating system to store its configuration database containing all persistent information.

ASPP14:FMT_SMF.1:

The TOE allows administrators to configure TLS Server credentials as used by TLS connections from external management clients and configure network elements which the TOE connects to via SSH.

6.4 Privacy

ASPP14:FPR_ANO_EXT.1:

The TOE does not transmit any PII. The TOE only accepts the administrator's username and PBKDFv2 transformed password and conveys administrative commands to the configured network element/device.

6.5 Protection of the TSF

ASPP14:FPT_AEX_EXT.1:

The TOE does not specify any compilation flags when compiling its Java code; however, unlike native code, Java does not suffer from buffer overflow vulnerabilities. For any native executables bundled with the TOE, the corresponding compilation flags are used including /DYNAMICBASE, /GS, and /NXCOMPAT for PE and -pie (position independent executable) and -fstack-protector-all for ELF executables.

ASPP14:FPT_API_EXT.1:

The TOE uses the following list of APIs:

java.security.AccessControlContext

java.security.AccessControlException

java.security.AccessController

java.security.cert.CertificateException

java.security.cert.CertificateFactory

java.security.cert.CRLException

java.security.cert.X509Certificate

java.security.cert.X509CRL

java.security.CodeSource

java.security.GeneralSecurityException

java.security.InvalidAlgorithmParameterException

java.security.InvalidKeyException

java.security.InvalidParameterException

java.security.Key

java.security.KeyFactory

java.security.KeyManagementException

java.security.KeyStore

java.security.KeyStoreException

java.security.MessageDigest

java.security.NoSuchAlgorithmException

java.security.NoSuchProviderException

java.security.PrivateKey

java.security.PrivilegedAction

java.security.PrivilegedActionException

java.security.PrivilegedExceptionAction

java.security.ProtectionDomain

java.security.ProviderException

java.security.PublicKey

java.security.SecureRandom

java.security.Security

java.security.spec.InvalidKeySpecException

java.security.spec.PKCS8EncodedKeySpec

java.security.UnrecoverableKeyException

javax.security.auth.kerberos.KerberosTicket

javax.security.auth.login.LoginException

javax.security.auth.Subject

ASPP14:FPT_IDV_EXT.1:

The TOE is versioned with a major and minor version number, as well as a build number that is incremented with every update to the TOE.

ASPP14:FPT_LIB_EXT.1:

ASPP14:FPT_TUD_EXT.1 / ASPP14:ALC_TSU_EXT.1:

The vendor packages updates to the TOE in an RPM format and relies upon the Red Hat Enterprise Linux or CentOS operating system to verify the installation package's signature before installing. Updates are signed by Infinera's GPG key which is provided by the vendor to be installed on the platform. Updates are obtained through Infinera's Customer Service Portal (https://support.infinera.com/). Updates are in the same format as initial initializations and are installed using the same process as the initial installations.

The vendor provides timely security updates for the TOE in case vulnerabilities have been discovered. Reported vulnerabilities and defects are investigated and rated based on the threat and result of the impact analysis and then scheduled for an upcoming bug fix release based on the severity. The vendor aims for security updates as soon as possible with a maximum of 30 days. Third party library updates are also included as a part of the TOE's update. The vendor actively monitors both internal and third-party components and accepts vulnerability reports through the Infinera's Customer portal (https://www.support.infinera.com/).

6.6 Trusted path/channels

ASPP14:FTP_DIT_EXT.1:

The TOE encrypts all data transmitted to and from TNMS Clients using TLS and encrypts all data transmitted to and from network elements/devices using SSHv2