Dell EMC Networking SmartFabric OS10.5.4

Security Target

Version 2.0

September 2023

Document prepared by

Lightship Security

www.lightshipsec.com

Document History

Version	Date	Author	Description
1.0	19 Jan 2023	M Ibrishimova	Addressed OR06.
1.1	03 April 2023	Khushmit Kaur	Addressed OR09.
1.2	03 May 2023	Khushmit Kaur	ST Updates + OR 17
1.3	11-May-2023	Khushmit Kaur	Addressed OR7 + OR15
1.4	20-June-2023	Khushmit Kaur	Addressed OR7, OR15, OR19, OR20, OR21
1.5	22-June-2023	Khushmit Kaur	Addressed OR7, OR22, OR23
1.6	18-July-2023	Khushmit Kaur	Addressed OR24
1.7	01-Aug-2023	Khushmit Kaur	ST Updates
1.8	28-Aug-2023	M Ibrishimova	Addressed OR25
1.9	05 Sep 2023	M Ibrishimova	Addressed minor comment.
2.0	05 Sep 2023	M Ibrishimova	Addressed CB OR

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the Dell EMC Networking SmartFabric OS10.5.4 Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	Dell EMC Networking SmartFabric OS10.5.4 Version: OS10.5.4.3P1
Security Target	Dell EMC Networking SmartFabric OS10.5.4 Security Target, v2.0

1.3 Conformance Claims

2 This ST supports the following conformance claims:

a) CC version 3.1 revision 5

b) CC Part 2 extended

c) CC Part 3 conformant

d) collaborative Protection Profile for Network Devices, v2.2e

e) NIAP Technical Decisions per Table 2

Table 2: NIAP Technical Decisions

TD #	Name	Rationale if n/a
TD0527	Updates to Certificate Revocation Testing (FIA_X509_EXT.1)	
TD0528	NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4	N/A. The TOE does not claim NTP
TD0536	NIT Technical Decision for Update Verification Inconsistency	
TD0537	NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	
TD0546	NIT Technical Decision for DTLS - clarification of Application Note 63	N/A. The TOE does not claim DTLS
TD0547	NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	
TD0555	NIT Technical Decision for RFC Reference incorrect in TLSS Test	N/A. The TOE does not claim FCS_TLSS_EXT.1

TD #	Name	Rationale if n/a
TD0556	NIT Technical Decision for RFC 5077 question	N/A. The TOE does not claim FCS_TLSS_EXT.1
TD0563	NiT Technical Decision for Clarification of audit date information	
TD0564	NiT Technical Decision for Vulnerability Analysis Search Criteria	
TD0569	NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	N/A. The TOE does not claim DTLSS and TLSS
TD0570	NiT Technical Decision for Clarification about FIA_AFL.1	
TD0571	NiT Technical Decision for Guidance on how to handle FIA_AFL.1	
TD0572	NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	
TD0580	NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e	
TD0581	NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	
TD0591	NIT Technical Decision for Virtual TOEs and hypervisors	N/A. The TOE is not a virtual TOE
TD0592	NIT Technical Decision for Local Storage of Audit Records	
TD0631	NIT Technical Decision for Clarification of public key authentication for SSH Server	
TD0632	NIT Technical Decision for Consistency with Time Data for vNDs	
TD0633	NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance	N/A. The TOE does not claim IPSec
TD0634	NIT Technical Decision for Clarification required for testing IPv6	
TD0635	NIT Technical Decision for TLS Server and Key Agreement Parameters	N/A. The TOE does not claim FCS_TLSS_EXT.1

TD #	Name	Rationale if n/a
TD0636	NIT Technical Decision for Clarification of Public Key User Authentication for SSH	N/A the TOE does not claim FCS_SSHC_EXT.1
TD0638	NIT Technical Decision for Key Pair Generation for Authentication	
TD0639	NIT Technical Decision for Clarification for NTP MAC Keys	N/A. The TOE does not claim NTP
TD0670	NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	
TD0738	NIT Technical Decision for Link to Allowed-With List	

1.4 Terminology

Table 3: Terminology

Term	Definition
CC	Common Criteria
NDcPP	collaborative Protection Profile for Network Devices
PP	Protection Profile
TOE	Target of Evaluation
TSF	TOE Security Functionality

2 TOE Description

2.1 Type

3 The TOE is a network switch.

2.2 Usage

4 The TOE is deployed within a network to provide layer 2 and layer 3 network management and interconnectivity functionality. The TOE interfaces within the scope of evaluation are shown in Figure 1.

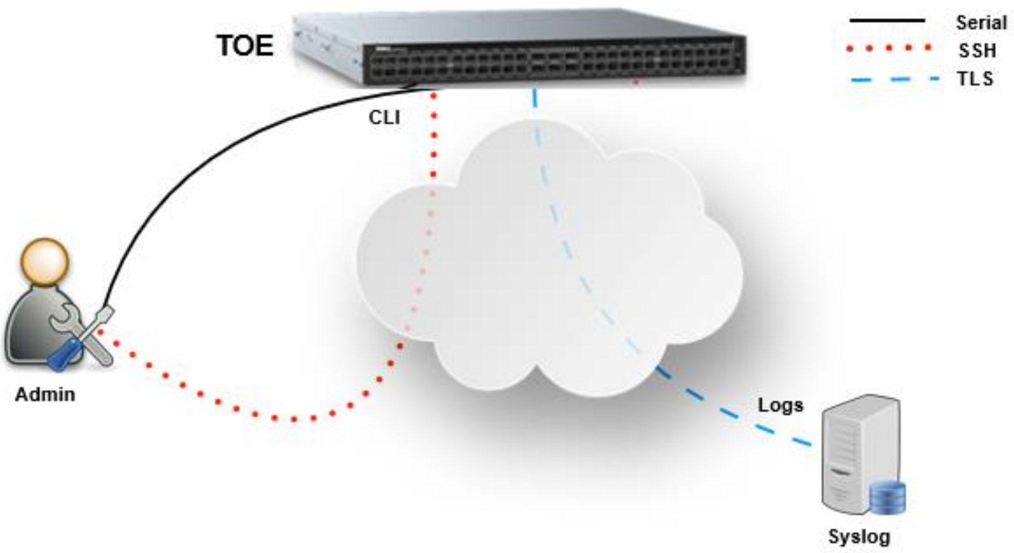

Figure 1: Example TOE deployment

5 The TOE interfaces are as follows:

a) **CLI.** Administrative CLI via direct serial connection or SSH.

b) **Logs.** Syslog via TLS.

2.3 Security Functions / Logical Scope

6 The TOE provides the following security functions:

a) **Protected Communications.** The TOE protects the integrity and confidentiality of communications using secure protocols as noted in section 2.2 above, and using cryptographic algorithms as described in Table 4.

b) **Secure Administration.** The TOE enables secure management of its security functions, including:

i) Administrator authentication with passwords

ii) Configurable password policies

iii) Role Based Access Control

iv) Access banners

v) Management of critical security functions and data

vi) Protection of cryptographic keys and passwords

c) **Trusted Update.** The TOE ensures the authenticity and integrity of software updates through GPG digital signatures and published hash. The TOE also implements “show version” CLI command that displays information about firmware version running on the TOE. An authorized user must authenticate to the secure Dell Support website where the software downloads are available. The downloaded image must be transferred to the appliance using a secure method such as Secure Copy or SFTP.

d) **System Monitoring.** The TOE generates logs of security relevant events. The TOE stores logs locally and is capable of sending log events to a remote audit server.

e) **Self-Test.** The TOE performs a suite of self-tests to ensure the correct operation and enforcement of its security functions. The TOE performs diagnostic self-tests and cryptographic module self-tests during start-up and generates audit records to record a failure. Self-tests comply with the FIPS 140-2 requirements for self-testing.

f) **Identification and Authentication.** The TOE ensures that all users must be authenticated before accessing its functions and data. TOE can be accessed directly via serial RJ45 connection or remotely via SSHv2 connection. When a user account has sequentially failed authentication the configured number of times, the account will be locked for a Security Administrator defined time period. The TOE uses X.509v3 certificates to support authentication for TLS. Certificate revocation checking is performed using a CRL.

g) **Security Audit.** The TOE generates audit records of user and administrator actions. The TOE includes the user identity in audit events resulting from actions of identified users. The Security Administrator can configure the TOE to send logs in real-time to a syslog server via TLS.

h) **Cryptographic Operations.** The TOE implements a cryptographic module. The cryptographic module has the ability to generate and destroy cryptographic keys. Relevant Cryptographic Algorithm Validation Program (CAVP) certificates are shown in Table 4.

Table 4: CAVP Certificates

Algorithm Capability	Certificate
AES-CBC	A1949
AES-CTR	
AES-GCM	
RSA KeyGen (186-4) RSA SigGen (186-4) RSA SigVer (186-4)	

Algorithm Capability	Certificate
ECDSA KeyGen (186-4) ECDSA SigGen (186-4) ECDSA SigVer (186-4)	
SHA-1, SHA-256, SHA-384, SHA-512	
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512	
KAS-ECC Component	
Counter DRBG	

2.4 Physical Scope

7 The physical boundary of the TOE includes all software and hardware shown in Table 5. The TOE is delivered via commercial courier.

Table 5: TOE models

Type	Model	CPU	Software	CAVP
Physical	S4112F-ON S4112T-ON S4128F-ON S4128T-ON S4148F-ON S4148T-ON MX5108n	Intel Atom C2338 (Silvermont)	Dell Networking SmartFabric OS 10.5.4	A1949
	MX9116n	Intel Atom C2538 (Silvermont)		
	S5212F-ON N3248TE-ON	Intel Atom C3338 (Goldmont)		
	S5224F-ON S5232F-ON S5248F-ON S5296F-ON Z9264F-ON	Intel Atom C3538 (Goldmont)		
	Z9432F-ON S5448F-ON	Intel Atom C3758 (Goldmont)		

Type	Model	CPU	Software	CAVP
	E3224F-ON	Intel Atom C3558/C3558R (Goldmont)		
	Z9332F-ON	Intel Pentium D1508 (Broadwell)		

2.4.1 Guidance Documents

8 The TOE includes the following guidance documents (PDF):

a) Dell EMC Networking SmartFabric OS10.5.4 Common Criteria Guide, v1.1

b) Dell SmartFabric OS10 User Guide Release 10.5.4, 12 2022 Rev. A05

2.4.2 Non-TOE Components

9 The TOE operates with the following components in the environment:

a) **Audit Server.** The TOE can send audit events to a Syslog server.

2.4.3 Functions not included in the TOE Evaluation

10 The evaluation is limited to those security functions identified in Security Functions / Logical Scope 2.3. Switching and software defined networking functions are outside the scope of TOE security functions.

3 Security Problem Definition

11 The Security Problem Definition is reproduced from section 4 of the NDcPP.

3.1 Threats

Table 6: Threats

Identifier	Description
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, flaw in the product) to compromise the device and

Identifier	Description
	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

Table 7: Assumptions

Identifier	Description
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). In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device functionality.

Identifier	Description
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 NDcPP. 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

Table 8: Organizational Security Policies

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

4 Security Objectives

12 The security objectives are reproduced from section 5 of the NDcPP.

Table 9: Security Objectives for the Operational Environment

Identifier	Description
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.
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_ADMIN	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.

5 Security Requirements

5.1 Conventions

13 This document uses the following font conventions to identify the operations defined by the CC:

a) **Assignment.** Indicated with italicized text.

b) **Refinement.** Indicated with bold text and strikethroughs.

c) **Selection.** Indicated with underlined text.

d) **Assignment within a Selection:** Indicated with italicized and underlined text.

e) **Iteration.** Indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").

14 **Note:** Operations performed within the Security Target are denoted within brackets []. Operations shown without brackets are reproduced from the NDcPP.

5.2 Extended Components Definition

15 Refer to Annex A: Extended Components Definition.

5.3 Functional Requirements

Table 10: Summary of SFRs

Requirement	Title
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
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_RBG_EXT.1	Random Bit Generation
FCS_SSHS_EXT.1	SSH Server Protocol

Requirement	Title
FCS_TLSC_EXT.1	TLS Client Protocol Without Mutual Authentication
FCS_TLSC_EXT.2	TLS Client Support for Mutual Authentication
FIA_AFL.1	Authentication Failure Management
FIA_PMG_EXT.1	Password Management
FIA_UIA_EXT.1	User Identification and Authentication
FIA_UAU_EXT.2	Password-based Authentication Mechanism
FIA_UAU.7	Protected Authentication Feedback
FIA_X509_EXT.1/Rev	X.509 Certificate Validation
FIA_X509_EXT.2	X.509 Certificate Authentication
FIA_X509_EXT.3	X.509 Certificate Requests
FMT_MOF.1/ManualUpdate	Management of security functions behaviour
FMT_MOF.1/Functions	Management of security functions behaviour
FMT_MTD.1/CoreData	Management of TSF Data
FMT_MTD.1/CryptoKeys	Management of TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.2	Restrictions on Security Roles
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_TUD_EXT.1	Trusted Update
FPT_STM_EXT.1	Reliable Time Stamps
FTA_SSL_EXT.1	TSF-initiated Session Locking
FTA_SSL.3	TSF-initiated Termination
FTA_SSL.4	User-initiated Termination
FTA_TAB.1	Default TOE Access Banners

Requirement	Title
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1/Admin	Trusted Path

5.3.1 Security Audit (FAU)

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 shutdown 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 2~~** **Table 11**.*

Table 11: Audit Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	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.

Requirement	Auditable Events	Additional Audit Record Contents
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_RBG_EXT.1	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
FCS_TLSC_EXT.2	None.	None
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate 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.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	None.
FMT_MOF.1/Functions	None.	None.
FMT_MTD.1/CoreData	None.	None.
FMT_MTD.1/CryptoKeys	None.	None.

Requirement	Auditable Events	Additional Audit Record Contents
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	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).
FTA_SSL_EXT.1 (if "terminate the session" is selected)	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_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.

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 2~~*** ***Table 11****.*

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.

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: [*log rotation: delete oldest log file*]] when the local storage space for audit data is full.

5.3.2 Cryptographic Support (FCS)

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]~~.

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 was changed by TD0580 and TD0581.

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*.

FCS_COP.1/DataEncryption Cryptographic Operation (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].

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, 3072*],

- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [*256,384 and 521 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, P-384, P-521]; ISO/IEC 14888-3, Section 6.4

].

FCS_COP.1/Hash Cryptographic Operation (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*.

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-512] and cryptographic key sizes *[160, 256, 512]* **and message digest sizes [160, 256, 512] bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”*.

FCS_RBG_EXT.1 Random Bit Generation

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [CTR_DRBG (AES)].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [[*one*] platform-based noise source] with a minimum of [256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.1 The TSF shall implement the SSH protocol that complies with: RFCs 4251, 4252, 4253, 4254, [4344, 5647, 5656, 6668, 8268, 8332].

FCS_SSHS_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following user authentication methods as described in RFC 4252: public key-based, [password based].

Application note: This SFR was changed by TD0631.

FCS_SSHS_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [*256 kilo*]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-cbc, aes256-cbc, 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, rsa-sha2-256, rsa-sha2-512] 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, diffie-hellman-group18-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.

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_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- 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_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246] and no other ciphersuites.

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

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

- Not implement any administrator override mechanism].

FCS_TLSC_EXT.1.4 The TSF shall [not present the Supported Elliptic Curves/Supported Groups Extension] in the Client Hello.

FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication

FCS_TLSC_EXT.2.1 The TSF shall support TLS communication with mutual authentication using X.509v3 certificates.

5.3.3 Identification and Authentication (FIA)

FIA_AFL.1 Authentication Failure Management

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within [*1-16*] 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].

FIA_PMG_EXT.1 Password Management

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

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”];

b) Minimum password length shall be configurable to between [*9*] and [*32*] *characters.*

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.

FIA_UAU_EXT.2 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.

FIA_UAU.7 Protected Authentication Feedback

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

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 [a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3]
- The TSF shall validate the extendedKeyUsage field according to the following rules:
    - *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.*
    - *Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
    - *Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*
    - *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

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

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 [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 [accept the certificate, not accept the certificate].

FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [Common Name].

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

5.3.4 Security Management (FMT)

FMT_MOF.1/ManualUpdate Management of security functions behaviour

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

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*.

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*.

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*.

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 [digital signature, hash comparison] 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 set the time which is used for time-stamps;
  - 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;]

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)

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.

FPT_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.

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: [

- *BIOS tests*
- *Cryptographic module tests*
- *Kernel and system binary integrity tests*].

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 [the most recently installed version of the TOE firmware/software].

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, published hash] prior to installing those updates.

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].

5.3.6 TOE Access (FTA)

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.

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*.

FTA_SSL.4 User-initiated Termination

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

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)

FTP_ITC.1 Inter-TSF trusted channel

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

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

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*audit server*].

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 Assurance Requirements

16 The TOE security assurance requirements are summarized in Table 12.

Table 12: Assurance Requirements

Assurance Class	Components	Description
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.1	Security Objectives for the operational environment
	ASE_REQ.1	Stated Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
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 Analysis

17 In accordance with section 7.1 of the NDcPP, the following refinement is made to ASE:

a) **ASE_TSS.1.1C Refinement:** The TOE summary specification shall describe how the TOE meets each SFR. **In the case of entropy analysis, the TSS is used in conjunction with required supplementary information on Entropy.**

6 TOE Summary Specification

18 The following describes how the TOE fulfils each SFR included in section 5.3.

6.1 Security Audit

6.1.1 FAU_GEN.1/FAU_GEN.2

19 The TOE generates the audit records specified at Table 11.

20 The following information is logged because of the Security Administrator generating/importing or deleting cryptographic keys:

a) **Generate SSH key-pair**. Action and implicitly identified key because this is the only SSH host key (RSA).

b) **Generate CSR.** Action and key reference (certificate and key files names/path).

c) **Import Certificate.** Action and key reference (certificate common name (CN)).

d) **Import CA Certificate.** Action and unique reference (certificate common name (CN)).

21 The TOE includes the user identity in audit events resulting from actions of identified users.

6.1.2 FAU_STG_EXT.1

22 The TOE is a standalone TOE that stores data locally.

23 The Security Administrator can configure the TOE to send logs to a syslog server. Log events are sent in real-time. Logs are sent via TLS.

24 The TOE implements log rotation – logs are rotated at 1GB and 5 copies/rotations of each type of log is stored. The TOE contains two relevant types of log files:

a) **Audit Log.** For user activity and configuration changes.

b) **Event Log.** For device events.

25 Only authorized administrators may view audit records and no capability to modify the audit records is provided.

6.2 Cryptographic Support

6.2.1 FCS_CKM.1

26 The TOE supports key generation for the following asymmetric schemes:

a) **RSA 2048-bit, 3072-bit.** Used in SSH and TLS RSA cipher suites.

b) **ECC P-256, ECC P-384, ECC P-521.** Used in SSH.

c) **Diffie-Hellman group 14, 16, 18.** Diffie-Hellman safe primes are used in SSH and TLS (TLS only uses group 14).

6.2.2 FCS_CKM.2

27 The TOE supports the following key establishment schemes:

a) **RSA schemes.** Used in TLS cipher suites with RSA key exchange. TOE operates as a sender.

b) **ECC schemes.** Used in SSH.

c) **Diffie-Hellman group 14, 16, 18.** Used in SSH and TLS (TLS only uses group 14). The TOE meets RFC 3526 Section 3 by implementing the 2048-bit Modular Exponential (MODP) Group, the 4096-bit MODP Group, and the 8192-bit MODP Group.

28 Table 13 below identifies the scheme being used by each service.

Table 13: Key Agreement Mapping

Scheme	SFR	Service
RSA	FCS_TLSC_EXT.1	Audit Server
ECC	FCS_SSHS_EXT.1	Administration
FFC Safe Primes	FCS_SSHS_EXT.1 FCS_TLSC_EXT.1	Administration
		Audit Server

6.2.3 FCS_CKM.4

29 Table 15 shows the origin, storage location and destruction details for cryptographic keys. Unless otherwise stated, the keys are generated by the TOE.

6.2.4 FCS_COP.1/DataEncryption

30 The TOE provides symmetric encryption and decryption capabilities using 128- and 256-bit AES in CBC, CTR, and GCM mode. AES is implemented in TLS and SSH.

31 The relevant NIST CAVP certificate numbers are listed Table 4.

6.2.5 FCS_COP.1/SigGen

32 The TOE provides cryptographic signature generation and verification services using:

a) RSA Signature Algorithm with key size of 2048, and 3072-bit.

b) ECDSA Signature Algorithm with key size of 256, 384 and 521 bits.

33 The RSA signature verification is used for the TLS and SSH protocols, and for update verification.

34 The ECDSA signature verification is used in SSH protocols.

35 The relevant NIST CAVP certificate numbers are listed in Table 4.

6.2.6 FCS_COP.1/Hash

36 The TOE provides cryptographic hashing services using SHA-1, SHA-256, SHA-384, and SHA-512.

37 SHA is implemented in the following parts of the TSF:

a) TLS and SSH.

b) Hashing of passwords in non-volatile storage.

c) Kernel image digital signature and file integrity checking.

d) Update verification.

38 The relevant NIST CAVP certificate numbers are listed in Table 4.

6.2.7 FCS_COP.1/KeyedHash

39 The TOE provides keyed-hashing message authentication services using HMAC-SHA1, HMAC-SHA2-256, and HMAC-SHA2-512.

40 HMAC is implemented in TLS and SSH.

41 The characteristics of the HMACs used in the TOE are given in Table 14.

Table 14: HMAC Characteristics

Algorithm	Block Size	Key Size	Digest Size
HMAC-SHA-1	512 bits	160 bits	160 bits
HMAC-SHA-256	512 bits	256 bits	256 bits
HMAC-SHA-512	1024 bits	512 bits	512 bits

42 The relevant NIST CAVP certificate numbers are listed in Table 4.

6.2.8 FCS_RBG_EXT.1

43 The TOE contains a CTR_DRBG that is seeded with 256 bits of full entropy from Intel’s Digital Random Number Generator (DRNG) via the RDRAND instruction. The Intel DRNG (RDRAND) is a third-party entropy source that is assumed to provide 256 bits of full entropy.

44 Additional detail is provided in the proprietary Entropy Description.

6.2.9 FCS_SSHS_EXT.1

45 The TOE implements SSH in compliance with RFCs 4251, 4252, 4253, 4254, 4344, 5647, 5656, 6668, 8268, 8332.

46 The TOE supports password-based or public key authentication for users. (ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521). Users are verified when attempting to authenticate via username and public key through the use of the authorized keys file, or by confirming the validity of the username and password presented.

47 The TOE supports ssh-rsa, rsa-sha2-256, rsa-sha2-512 SSH server’s host public key algorithms.

48 The TOE examines the size of each received SSH packet. If the packet is greater than 256 KB, it is automatically dropped.

49 The TOE utilises AES-CBC-128, AES-CBC-256, AES-CTR-128, AES-CTR-256, aes128-gcm@openssh.com, aes256-gcm@openssh.com for SSH encryption.

50 The TOE provides data integrity for SSH connections via HMAC-SHA1, HMAC-SHA2-256 and HMAC-SHA2-512.

51 The TOE supports diffie-hellman-group14-sha1, ecdh-sha2-nistp256, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, ecdh-sha2-nistp384 and ecdh-sha2-nistp521 for SSH key exchanges.

52 The TOE will re-key SSH connections after 1 hour or an encryption key has been used to protect 1GB of data (whichever occurs first).

6.2.10 FCS_TLSC_EXT.1 and FCS_TLSC_EXT.2

53 The TOE operates as a TLS client for the trusted channel with an audit server. The TOE client-side certificates for TLS mutual authentication.

54 Only TLS 1.2 is allowed, and cipher suites are not user configurable for the audit server connection. The cipher suites are restricted to the following:

a) TLS_RSA_WITH_AES_128_CBC_SHA

b) TLS_RSA_WITH_AES_128_CBC_SHA256

c) TLS_RSA_WITH_AES_256_CBC_ SHA256

d) TLS_RSA_WITH_AES_256_CBC_SHA

e) TLS_DHE_RSA_WITH_AES_256_CBC_SHA

f) TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

g) TLS_DHE_RSA_WITH_AES_128_CBC_SHA

h) TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

55 Cipher suites are not user configurable.

56 The reference identifier (DNS, or IP Address) for the Audit Server is automatically configured by the TOE. The TOE converts IPv4 address in the CN to binary format and stores them in an array in network byte order. The TOE enforces the RFC 3986 for IPv4 canonical format. Wildcards are not supported.

57 The TSF does not present the Supported Elliptic Curves Extension in the Client Hello.

58 The TOE supports the presentation of a X.509v3 certificate to a TLS server for TLS mutual authentication.

59 X.509v3 certificates are configured on a certification authority (CA) and installed on the TOE. After installing a certificate on the TOE, an administrator configures an X.509v3 Security Profile and adds the previously installed certificate to the Certificate field of the Security Profile.

60 The TOE chooses which certificate to use during mutual authentication with a TLS server based on the Security Profile. The TOE adheres to RFC 5246 for implementing client certificates in the TLS protocol to present to non-TOE IT entities.

6.3 Identification and Authentication

6.3.1 FIA_PMG_EXT.1

61 The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper- and lower-case letters, numbers, and special characters “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”.

62 The minimum password length is settable by the Administrator. Minimum password length shall be configurable to between [9] and [32] characters.

6.3.2 FIA_UIA_EXT.1

63 The TOE requires all users to be successfully identified and authenticated. The TOE warning banner may be viewed prior to authentication.

64 No administrative actions are allowed before user identification and authentication.

65 Access to the TOE is facilitated through the following interfaces:

a) Directly connecting to the TOE appliance (serial over RJ45) using a password based authentication.

b) Remotely connecting to each appliance via SSHv2 using a password or public key based authentication.

6.3.3 FIA_UAU_EXT.2

66 Regardless of the interface at which the administrator interacts, the TOE prompts the user for a credential. Only after the administrative user presents the correct authentication credentials will they be granted access to the TOE administrative functionality. No TOE administrative access is permitted until an administrator is successfully identified and authenticated.

67 All user authentication is password-based or public key-based.

68 The TOE provides a local password-based authentication mechanism.

69 The process for authentication is the same for administrative access whether administration is occurring via direct connection or remotely. At initial login, the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative credential associated with the user account (e.g., password or SSH public/private key response). The TOE then either grants administrative access (if the combination of username and credential is correct) or indicates that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.

6.3.4 FIA_UAU.7

70 For all authentication at the local CLI the TOE provides no feedback when the administrative password is entered so that the password is obscured.

6.3.5 FIA_AFL.1

71 The TOE is capable of tracking authentication failures of remote administrators (those using SSH) by using a counter for each remote user.

72 When a user account has sequentially failed authentication the configured number of times, the account will be locked for a Security Administrator defined time period.

73 After the Security Administrator defined time period passes, account access is restored.

74 The administrator can configure the maximum number of failed attempts using the CLI.

75 The local console does not enforce the lockout mechanism when the TOE is configured and used according to the Dell EMC Networking SmartFabric OS10 Common Criteria Guide.

6.3.6 FIA_X509_EXT.1/Rev

76 The TOE performs X.509 certificate validation at the following points:

a) TOE TLS client validation of server X.509 certificates.

b) When certificates are loaded into the TOE.

77 In all scenarios, certificates are checked for several validation characteristics:

a) If the certificate ‘notAfter’ date is in the past or ‘notBefore’ is in the future, then this is an expired certificate which is considered invalid.

b) The certificate chain must terminate with a trusted CA certificate.

c) Server certificates consumed by the TOE TLS client must have a ‘serverAuthentication’ extendedKeyUsage purpose.

78 A trusted CA certificate is defined as any certificate loaded into the TOE trust store that has, at a minimum, a basicConstraints extension with the CA flag set to TRUE. The TOE also supports a ‘trusted host’ certificate which is a self-signed certificate that can be stored in the trust store.

79 The TOE chooses which TLS client certificate to use during mutual authentication with a TLS server based on the Security Profile. The TOE adheres to RFC 5246 for implementing client certificates in the TLS protocol to present to non-TOE IT entities.

80 The TOE chooses and validates the server certificate received in response to a TLS client hello message sent by the TOE.

81 Certificate revocation checking for the above scenarios is performed using a CRL.

82 As X.509 certificates are not used for trusted updates, firmware integrity self-tests or client authentication, the code-signing and clientAuthentication purpose is not checked in the extendedKeyUsage for related certificates. OCSP signing purpose in the extendedKeyUsage is not supported.

83 The TOE has a trust store where root CA and intermediate CA certificates can be stored. The trust store is not cached: if a certificate is deleted, it is immediately untrusted. If a certificate is added to the trust store, it is immediately trusted for its given scope.

84 The X.509 certificates for each of the given scenarios are validated using the certificate path validation algorithm defined in RFC 5280, which can be summarized as follows:

a) The public key algorithm and parameters are checked

b) The current date/time is checked against the validity period revocation status is checked

c) Issuer name of X matches the subject name of X+1

d) Name constraints are checked

e) Policy OIDs are checked

f) Policy constraints are checked; issuers are ensured to have CA signing bits

g) Path length is checked

h) Critical extensions are processed

6.3.7 FIA_X509_EXT.2

85 The TOE has a trust store where root CA and intermediate CA certificates can be stored. The trust store is not cached: if a certificate is deleted, it is immediately untrusted. If a certificate is added to the trust store, it is immediately trusted for its given scope.

86 Instructions for configuring the trusted IT entities to supply appropriate X.509 certificates are captured in the guidance documents. If a connection cannot be established during a validity check of a certificate, then the certificate is rejected by the TOE.

87 As part of the verification process, a CRL is used to determine whether the certificate is revoked or not. If the CRL cannot be obtained, then the TOE will use the last cached information available about certificate to reject the certificate. If the CRL cannot be obtained and the information is not available in the cache about the certificate, the TOE will accept the certificate.

6.3.8 FIA_X509_EXT.3

88 For the Certificate Signing Request, a CN is required and may be an IP address or DNS name. SANs are optional and may be IP address, URI, DNS name or directory name.

6.4 Security Management

6.4.1 FMT_MOF.1/ManualUpdate

89 The TOE restricts the ability to perform software updates to Security Administrators.

6.4.2 FMT_MOF.1/Functions

90 The TOE restricts the ability to modify (enable/disable) transmission of audit records to an external audit server to Security Administrators. The administrator can then configure the TOE to send audit records to an external server.

6.4.3 FMT_MTD.1/CoreData

91 Users are required to login before being provided with access to any administrative functions. Management of the trust store is an administrative function, which is restricted to authenticated administrators.

6.4.4 FMT_SMR.2

92 The TOE implements role-based access control based on pre-defined profiles that are assigned when creating a user.

93 The TOE supports the following pre-defined administrative user profiles (collectively these can be considered the Security Administrator role):

94 Network Operator (netoperator). This user role has no privilege to modify any configuration on the switch but can access Exec mode (monitoring) to view the current configuration and status information.

95 Network Administrator (netadmin). This user role can configure, display, and debug the network operations on the switch. Netadmin can access all of the commands that are available from the network operator role. This role does not have access to the commands that are available to the system security administrator for cryptography operations, AAA, or the commands reserved solely for the system administrator.

96 Security Administrator (secadmin). This user role can control the security policy across the systems that are within a domain or network topology. The security administrator commands include FIPS mode enablement, password policies, inactivity timeouts, banner establishment, and cryptographic key operations for secure access paths.

97 System Administrator (sysadmin). This role has full access to all the commands in the system, exclusive access to commands that manipulate the file system formatting, and access to the system shell. This role can also create user IDs and define other user roles.

98 Management of TSF data via the CLI is restricted to System Administrators and Security Administrators.

6.4.5 FMT_MTD.1/CryptoKeys

99 The TOE administrator can generate and delete SSH, TLS, and X.509 keys. The TOE restricts the ability to manage SSH, TLS and any configured X.509 private keys to Security Administrators.

6.4.6 FMT_SMF.1

100 The TOE may be managed via the CLI (console & SSH). The specific management capabilities include:

a) Ability to administer the TOE locally and remotely

b) Ability to configure the access banner

c) Ability to modify the behaviour of the transmission of audit data to an external IT entity

d) Ability to configure the session inactivity time before session termination or locking

e) Ability to manage the cryptographic keys;

f) Ability to update the TOE and to verify the update using digital signature or hash comparison.

g) Ability to configure the authentication failure parameters

h) Ability to manage the trusted public keys database

i) Ability to set the time which is used for timestamps

j) Ability to:

   i) Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors.

   ii) Ability to import X.509v3 certificates to the TOE's trust store.

6.5 Protection of the TSF

6.5.1 FPT_SKP_EXT.1

101 Keys are protected as described in Table 15. In all cases, plaintext keys cannot be viewed through an interface designed specifically for that purpose.

Table 15: Keys

Key	Algorithm	Storage	Zeroization
TLS Private Key	RSA	NVRAM – plaintext	Overwritten with zeroes by Security Administrator CLI command which invokes a proprietary API.

Key	Algorithm	Storage	Zeroization
TLS Session Keys	TLS KDF	RAM – plaintext	Overwritten with zeroes upon termination of the session or reboot of the appliance
SSH Private Key	RSA	NVRAM – plaintext	Overwritten with zeroes by Security Administrator CLI command which invokes a proprietary API.
SSH Session Keys	SSH KDF	RAM – plaintext	The keys (including re-keyed keys) are overwritten with zeroes when no longer required or reboot of the appliance

6.5.2 FPT_APW_EXT.1

102 Passwords are protected as describe in Table 16. In all cases plaintext passwords cannot be viewed through an interface designed specifically for that purpose.

Table 16: Passwords

Key/Password	Generation/ Algorithm	Storage	Zeroization
Locally stored administrator passwords	User generated	NVRAM - SHA-256 hash	Overwritten with new data.

6.5.3 FPT_TST_EXT.1

103 The TOE performs diagnostic self-tests during start-up and generates audit records to record a failure. Some low-level critical failure modes can prevent TOE start-up and as a result will not generate audit records. In such cases, the TOE appliance will enter failure mode displaying error codes, typically displayed on the console. The TOE can be configured to reboot or to stop with errors displayed when non-critical errors are encountered.

104 The TOE performs diagnostic power-up and conditional self-tests. Self-tests comply with the FIPS 140-2 requirements, as outlined below.

105 Power-up self-tests are executed automatically when the module is loaded into memory. The power-up self-tests include the FIPS140-2 required Software Integrity Test and a set of Cryptographic Algorithms tests. The following Cryptographic Algorithm tests are implemented in the module:

- AES in CBC, CTR, ECB, GCM, mode, encrypt and decrypt KATs
- CTR DRBG KAT and SP800-90A health tests
- HMAC SHA-1, and HMAC SHA-2 (256, and 512) KATs
- RSA encrypt and decrypt KATs
- RSA sign and verify KATs
- SHA-1 KATs
- SHA-2 (256, 384, 512, 512-224, 512-256) KATs

- Software integrity test using HMAC verification.
- ECDSA Pairwise Consistency Test

106 The module performs the following conditional self-tests:

- A Continuous Random Number Generation (CRNG) test each time the toolkit produces random data, as per the FIPS 140-2 standard. The CRNG test is performed for the CTR DRBG and NDRNG (Entropy).
- A repetition count test and adaptive proportion test for the NDRNG (Entropy), as defined in SP 800-90B.
- A pair-wise consistency test each time the module generates an RSA public/private key pair.

107 The TOE generates audit records to record a failure; the messages are displayed on the console and audit records generated for both successful and failed tests. Some low-level critical failure modes can prevent TOE start-up and as a result will not generate audit records. In such cases, the TOE appliance will enter failure mode displaying error codes, typically displayed on the console. The TOE can be configured to reboot or to stop with errors displayed when non-critical errors are encountered. Failure of any of the FIPS mode tests during boot process will stop start-up process and prompt the user to reload.

108 The TOE implements a secure boot process which performs verification of the kernel image digital signature (RSA2048/SHA256) prior to booting the kernel (a failure results in the TOE halting at the boot loader). The kernel and TOE OS are subsequently booted, and a further hash file integrity test is performed on OS10 system binaries (a failure of file integrity results in Exec mode access only and upgrade to a valid image is required to proceed further). Secure boot must be enabled during configuration.

109 By verifying the correct operation of the platform hardware components and ensuring the integrity of software components, the TOE self-tests are sufficient to demonstrate that the security functions are operating correctly.

6.5.4 FPT_TUD_EXT.1

110 Upgrading the TOE is a multi-step process performed by a Security Administrator. An authorized user must authenticate to the secure Dell Support website where the software downloads are available. The downloaded image must be transferred to the appliance using a secure method such as Secure Copy or SFTP.

111 To validate the software image before installing the image, use the "`image secure-install`" command. It verifies the signature of the image files using hash-based authentication. Upgraded image files are installed after they are successfully validated. This validation procedure prevents the installation of corrupted or modified images.

112 GPG digital signatures can also be used to verify the updates using "`image secure-install`" command. If the command reports a bad signature, the image should not be used. Instead, download the file again and start over.

113 The TOE also implements "show version" CLI command that displays information about firmware version running on the TOE. The TOE also has 'show boot detail' which shows versions of both active image and standby image. The "show boot detail" command will immediately recognize and display the new version after it was downloaded, installed, and verified by the administrator.

114 The activation process involves the following:

a) The user to issue the ‘boot system standby’ command.

b) The user issues the ‘reload’ command.

115 After the reboot, what used to be the standby version is now the active image, and what used to be the active image is now the standby. The user can activate the standby version in the same manner as outlined above.

116 Note: After rebooting, the update becomes active only if the ‘boot system standby’ was issued before rebooting. If the ‘reload’ command is issued without the ‘boot system standby’, the system will reload the same image it was just running.

6.5.5 FPT_STM_EXT.1

117 The TOE incorporates an internal clock. The TOE uses an internal battery-backed hardware clock for reliability. The Security Administrator configures date and time settings during initial TOE configuration.

118 The TOE makes used of time for the following:

a) Audit record timestamps

b) Session timeouts (lockout enforcement)

c) Certificate validation

6.6 TOE Access

6.6.1 FTA_SSL_EXT.1

119 The Security Administrator may configure the TOE to terminate an inactive local interactive session (CLI) following a specified period. An administrator may terminate local and remote sessions by enabling re-authentication, which is disabled by default. The settings can be configured in INTERFACE mode, from 1 to 65535 seconds, default 30 seconds.

6.6.2 FTA_SSL.3

120 The Security Administrator may configure the TOE to terminate an inactive remote interactive session following a specified period. The settings can be configured in INTERFACE mode, from 1 to 65535 seconds, default 30 seconds.

6.6.3 FTA_SSL.4

121 Administrative users may terminate their own sessions at any time. The session can be terminated using ‘exit’ command.

6.6.4 FTA_TAB.1

122 The TOE displays an administrator configurable message to users prior to login at the CLI and when logging in remotely.

123 Administrative access to the TOE is facilitated through the following interfaces:

a) Directly connecting to the TOE appliance (serial over RJ45) using a password.

b) Remotely connecting to each appliance via SSHv2 using a password or public key

6.7 Trusted Path/Channels

6.7.1 FTP_ITC.1

124 The TOE supports secure communication with the following IT entities:

a) Audit server via TLS. The TOE acts as a client.

6.7.2 FTP_TRP.1/Admin

125 The TOE provides the following trusted paths for remote administration:

a) **CLI over SSH.**

7 Rationale

7.1 Conformance Claim Rationale

126 The following rationale is presented with regard to the PP conformance claims:

a) **TOE type.** As identified in section 2.1, the TOE is network device, consistent with the NDcPP.

b) **Security problem definition.** As shown in section 3, the threats, OSPs and assumptions are reproduced directly from the NDcPP.

c) **Security objectives.** As shown in section 4, the security objectives are reproduced directly from the NDcPP.

d) **Security requirements.** As shown in section 5, the security requirements are reproduced directly from the NDcPP. No additional requirements have been specified.

7.2 Security Objectives Rationale

127 All security objectives are drawn directly from the NDcPP.

7.3 Security Requirements Rationale

128 All security requirements are drawn directly from the NDcPP. Table 17 presents a mapping between threats and SFRs as presented in the NDcPP.

Table 17: NDcPP SFR Rationale

Identifier	SFR Rationale
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	• The Administrator role is defined in FMT_SMR.2 and the relevant administration capabilities are defined in FMT_SMF.1 and FMT_MTD.1/CoreData, with optional additional capabilities in FMT_MOF.1/Services and FMT_MOF.1/Functions • The actions allowed before authentication of an Administrator are constrained by FIA_UIA_EXT.1, and include the advisory notice and consent warning message displayed according to FTA_TAB.1 • The requirement for the Administrator authentication process is described in FIA_UAU_EXT.2 • Locking of Administrator sessions is ensured by FTA_SSL_EXT.1 (for local sessions), FTA_SSL.3 (for remote sessions), and FTA_SSL.4 (for all interactive sessions) • The secure channel used for remote Administrator connections is specified in FTP_TRP.1/Admin • (Malicious actions carried out from an Administrator session are separately addressed by T.UNDETECTED_ACTIVITY)

Identifier	SFR Rationale
	• (Protection of the Administrator credentials is separately addressed by T.PASSWORD_CRACKING).
T.WEAK_CRYPTOGRAPHY	• Requirements for key generation and key distribution are set in FCS_CKM.1 and FCS_CKM.2 respectively • Requirements for use of cryptographic schemes are set in FCS_COP.1/DataEncryption, FCS_COP.1/SigGen, FCS_COP.1/Hash, and FCS_COP.1/KeyedHash • Requirements for random bit generation to support key generation and secure protocols (see SFRs resulting from T.UNTRUSTED_COMMUNICATION_CHANNELS) are set in FCS_RBG_EXT.1 • Management of cryptographic functions is specified in FMT_SMF.1
T.UNTRUSTED_COMMUNICATION_CHANNELS	• The general use of secure protocols for identified communication channels is described at the top level in FTP_ITC.1 and FTP_TRP.1/Admin; for distributed TOEs the requirements for inter-component communications are addressed by the requirements in FPT_ITT.1 • Requirements for the use of secure communication protocols are set for all the allowed protocols in FCS_DTLSC_EXT.1, FCS_DTLSC_EXT.2, FCS_DTLSS_EXT.1, FCS_DTLSS_EXT.2, FCS_HTTPS_EXT.1, FCS_IPSEC_EXT.1, FCS_SSHC_EXT.1, FCS_SSHS_EXT.1, FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2 • Optional and selection-based requirements for use of public key certificates to support secure protocols are defined in FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3
T.WEAK_AUTHENTICATION_ENDPOINTS	• The use of appropriate secure protocols to provide authentication of endpoints (as in the SFRs addressing T.UNTRUSTED_COMMUNICATION_CHANNELS) are ensured by the requirements in FTP_ITC.1 and FTP_TRP.1/Admin; for distributed TOEs the authentication requirements for endpoints in inter-component communications are addressed by the requirements in FPT_ITT.1 • Additional possible special cases of secure authentication during registration of distributed TOE components are addressed by FCO_CPC_EXT.1 and FTP_TRP.1/Join.
T.UPDATE_COMPROMISE	• Requirements for protection of updates are set in FPT_TUD_EXT.1 • Additional optional use of certificate-based protection of signatures can be specified using FPT_TUD_EXT.2, supported by the X.509 certificate processing requirements in FIA_X509_EXT.1, FIA_X509_EXT.2 and FIA_X509_EXT.3

Identifier	SFR Rationale
	- Requirements for management of updates are defined in FMT_SMF.1 and (for manual updates) in FMT_MOF.1/ManualUpdate, with optional requirements for automatic updates in FMT_MOF.1/AutoUpdate
T.UNDETECTED_ACTIVITY	- Requirements for basic auditing capabilities are specified in FAU_GEN.1 and FAU_GEN.2, with timestamps provided according to FPT_STM_EXT.1 and if applicable, protection of NTP channels in FCS_NTP_EXT.1 - Requirements for protecting audit records stored on the TOE are specified in FAU_STG.1 - Requirements for secure transmission of local audit records to an external IT entity via a secure channel are specified in FAU_STG_EXT.1 - Optional additional requirements for dealing with potential loss of locally stored audit records are specified in FAU_STG_EXT.2/LocSpace, and FAU_STG_EXT.3/LocSpace - If (optionally) configuration of the audit functionality is provided by the TOE then this is specified in FMT_SMF.1, and confining this functionality to Security Administrators is required by FMT_MOF.1/Functions.
T.SECURITY_FUNCTIONALITY_COMPROMISE	- Protection of secret/private keys against compromise is specified in FPT_SKP_EXT.1 - Secure destruction of keys is specified in FCS_CKM.4 - If (optionally) management of keys is provided by the TOE then this is specified in FMT_SMF.1, and confining this functionality to Security Administrators is required by FMT_MTD.1/CryptoKeys - (Protection of passwords is separately covered under T.PASSWORD_CRACKING)
T.PASSWORD_CRACKING	- Requirements for password lengths and available characters are set in FIA_PMG_EXT.1 - Protection of password entry by providing only obscured feedback is specified in FIA_UAU.7 - Actions on reaching a threshold number of consecutive password failures are specified in FIA_AFL.1 - Requirements for secure storage of passwords are set in FPT_APW_EXT.1.
T.SECURITY_FUNCTIONALITY_FAILURE	- Requirements for running self-test(s) are defined in FPT_TST_EXT.1
P.ACCESS_BANNER	- An advisory notice and consent warning message is required to be displayed by FTA_TAB.1

Annex A: Extended Components Definition

129 Refer to the Extended Components Definition of the Protection Profile.