Vision Series Network Packet Broker v5.10.0

Security Target

Version 2.0

December 2023

Document prepared by

www.lightshipsec.com

Document History

Version	Date	Author	Description
2.0	04 Dec 2023	Garrett Nickel	Official release for Assurance Maintenance

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the Vision Series Network Packet Broker v5.10.0 Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 Keysight Network Packet Brokers are at the heart of all Keysight Visibility solutions. Their main function is to aggregate, load balance and filter network traffic before it is processed by network security and performance monitoring tools.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	Vision Series Network Packet Broker v5.10.0 Build: 5.10.0
Security Target	Vision Series Network Packet Broker v5.10.0 Security Target, v2.0

1.3 Conformance Claims

3 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	
TD0536	NIT Technical Decision for Update Verification Inconsistency	
TD0537	NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	
TD0538	NIT Technical Decision for Outdated link to allowed-with list	
TD0546	NIT Technical Decision for DTLS - clarification of Application Note 63	NA since DTLS is not claimed

TD #	Name	Rationale if n/a
TD0547	NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	
TD0555	NIT Technical Decision for RFC Reference incorrect in TLSS Test	
TD0556	NIT Technical Decision for RFC 5077 question	
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	
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	
TD0592	NIT Technical Decision for Local Storage of Audit Records	

1.4 Terminology

Table 3: Terminology

Term	Definition
CC	Common Criteria
EAL	Evaluation Assurance Level
IFC	Ixia Fabric Controller (IFC)
Ixia	Ixia Visibility Solutions have been rebranded to Keysight Technologies

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

2 TOE Description

2.1 Type

4 The TOE is a network device.

2.2 Usage

2.2.1 Deployment

5 Figure 1 shows an example deployment of the TOE (Network Packet Broker). Usage is as follows:

a) Capture network traffic by tapping network links.

b) Through non-production network links, traffic flows to the Network Packet Broker where duplicate data is removed and filtered.

c) Performance and monitoring tools then receive the most appropriate data stream, tailored specifically for that tool.

6

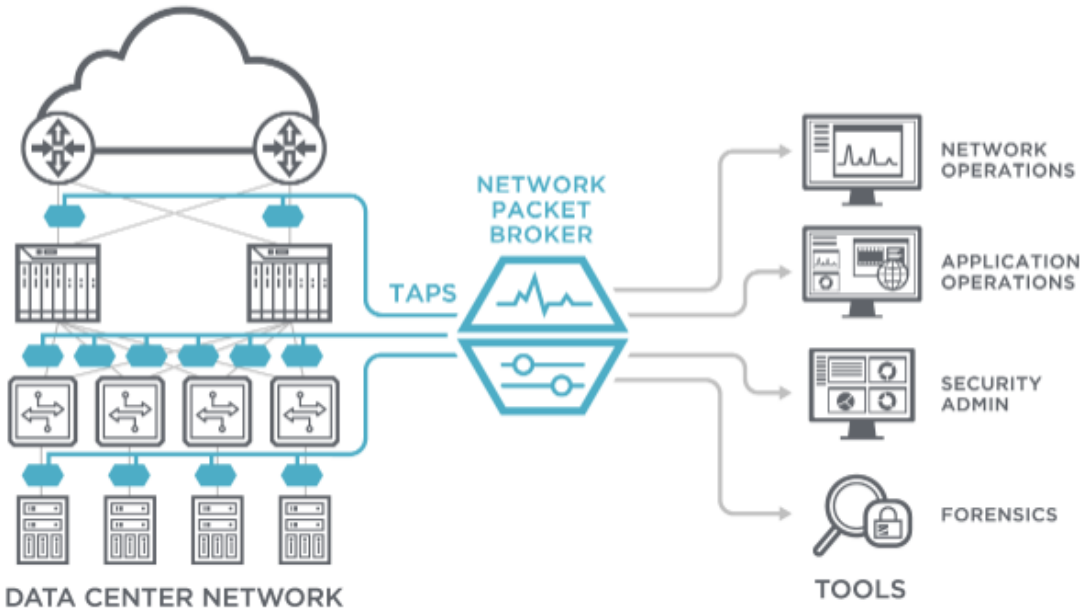

Figure 1: Example TOE deployment

7 **Note:** The TOE may be deployed as a cluster using IFC. This does not impact on any TOE security functions.

2.2.2 Trusted Paths and Channels

8 The TOE's trusted paths and channels within the scope of evaluation are shown in Figure 2.

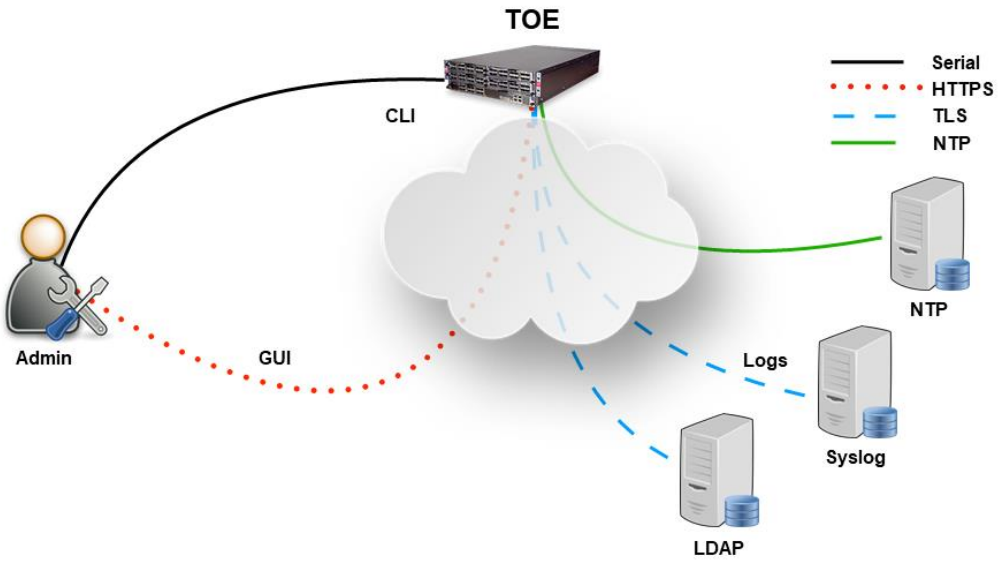

Figure 2: TOE Trusted Paths and Channels

9 The TOE trusted paths and channels are as follows:

a) **Serial Console.** Administrative interface via direct serial connection.

b) **GUI/WebAPI.** Administrative web GUI/WebAPI via HTTPS.

c) **Logs.** Logs sent to syslog via TLS.

d) **NTP.** NTP communications make use of SHA-1 message digests.

e) **LDAP.** The TOE uses an LDAP authentication server via TLS.

2.3 Security Functions / Logical Scope

10 The TOE provides the following security functions:

a) **Protected Communications.** The TOE protects the integrity and confidentiality of communications as noted in section 2.2.2 above.

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 digital signatures.

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.

f) **Cryptographic Operations.** The TOE implements a cryptographic module. Relevant Cryptographic Algorithm Validation Program (CAVP) certificates are shown in Table 4.

Table 4: CAVP Certificates

Module	Services	Algorithms	Certificates
BouncyCastle	TLS/HTTPS X.509v3 Key Encryption	AES-CBC AES-GCM RSA KeyGen (186-4) RSA SigGen (186-4) RSA SigVer (186-4) ECDSA KeyGen (186-4) ECDSA SigGen (186-4) ECDSA SigVer (186-4) SHA-1, SHA-256 HMAC-SHA-1, HMAC-SHA-256 KAS-ECC Hash DRBG	C1551 AES 5940 RSA 3118 ECDSA 1590 Component 2169 SHS 4693 HMAC 3915 KAS 210 DRBG 2493
OpenSSL	NTP	SHA-1	C1550 SHS 4692

2.4 Physical Scope

11 The physical boundary of the TOE includes the Vision Series Network Packet Broker v5.10.0 software on the appliance models shown in Table 5. The TOE is delivered via commercial courier.

Table 5: TOE models

Model	CPU	Notes on differences
Vision ONE	Intel Core i7-3555LE	1RU - All-in-one tool that provides high-performance, lossless visibility

Model	CPU	Notes on differences
Vision 7300/7303	Intel Core i7-3555LE	7RU - High-density, modular platform for high performance, intelligent visibility
Vision E40	Atom C2538	1RU - Cost-effective rack-level visibility for ANY size data center
Vision E100	Xeon D-1518	1RU - Cost-effective rack-level visibility for ANY size data center
Vision E10S	Celeron 3965U	1RU - Cost-effective rack-level visibility designed for branch and remote offices
Vision X	Xeon D-1527	3RU - Scalable visibility for data centres today and tomorrow
TradeVision	Intel Core i7-3555LE	1RU - Market feed management and tap aggregation for monitoring capital markets

2.4.1 Guidance Documents

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

a) Vision Series Network Packet Broker v5.10.0 Common Criteria Guide, v2.0

b) Vision ONE Network Packet Broker Installation Guide 913-2419-01 Rev-G

c) TradeVision Network Packet Broker Installation Guide 913-2421-01 Rev-C

d) Vision Edge 40/100 Network Packet Broker Installation Guide 913-2450-01 Rev-D

e) Vision Edge 10S Network Packet Broker Installation Guide 913-2529-01 Rev-E

f) Vision 7300/7303 Network Packet Broker Installation Guide 913-2530-01 Rev-D

g) Vision X Network Packet Broker Installation Guide 913-2542-01 Rev-G

h) Ixia Vision 7300/7303 Startup Guide 913-2413-01 Rev-B

i) Vision Edge 10S Startup Guide 913-2414-01 Rev C

j) Ixia Vision Edge E40/E100 Startup Guide 913-2415-01 Rev-C

k) Vision ONE Startup Guide 913-2416-01 Rev-D

l) Vision X Quick Start Guide Digital 913-2499-01 Rev-F

m) TradeVision Quick Start Guide v5.9.0 913-2885-01 Rev-A

n) TradeVision Network Packet Broker User Guide Release 5.10.0 202110211901-05:00 913-2929-01 Rev A

o) Vision 7300/7303 Network Packet Broker User Guide Release 5.10.0 202110211900-05:00 913-2921-01 Rev A

p) Vision Edge 10S Network Packet Broker User Guide Release 5.10.0 202110211540-05:00 913-2926-01 Rev A

q) Vision Edge 40 Network Packet Broker User Guide Release 5.10.0 202110211543-05:00 913-2927-01 Rev A

r) Vision Edge 100 Network Packet Broker User Guide Release 5.10.0 202110211543-05:00 913-2928-01 Rev A

s) Vision ONE Network Packet Broker User Guide Release 5.10.0 202110211257-05:00 913-2920-01 Rev A

t) Vision X Network Packet Broker User Guide Release 5.10.0 202110211539-05:00 913-2925-01 Rev A

u) Keysight TradeVision Series Web API User Guide 5.10.0, October 2021, 913-2940-01 Rev A

v) Keysight 7300 Series Web API User Guide Release 5.7.1 913-2799-01 Rev A

w) Keysight Vision E10S Web API User Guide Release 5.10.0, October 2021, 913-2936-01 Rev A

x) Keysight E40 Series Web API User Guide Release 5.10.0, October 2021, 913-2933-01 Rev A

y) Keysight E100 Series Web API User Guide Release 5.10.0, October 2021, 913-2934-01 Rev A

z) Keysight Vision ONE Series Web API User Guide Release 5.10.0, October 2021, 913-2931-01 Rev A

aa) Keysight Vision X Series Web API User Guide Release 5.10.0, October 2021, 913-2935-01 Rev A

2.4.2 Non-TOE Components

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

a) **Audit Server.** The TOE is capable of sending audit events to a Syslog server.

b) **NTP Server.** The TOE synchronizes time with an NTP server.

c) **LDAP Server.** The TOE uses LDAP for authenticating users.

2.4.3 Functions not included in the TOE Evaluation

14 Evaluated functionality is limited to those security functions identified at section 2.3.

3 Security Problem Definition

15 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

16 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

17 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").

18 **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

19 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_HTTPS_EXT.1	HTTPS Protocol
FCS_NTP_EXT.1	NTP Protocol

Requirement	Title
FCS_RBG_EXT.1	Random Bit Generation
FCS_TLSC_EXT.1	TLS Client Protocol without Mutual Authentication
FCS_TLSC_EXT.2	TLS Client Support for Mutual Authentication
FCS_TLSS_EXT.1	TLS Server Protocol Without Mutual Authentication
FIA_AFL.1	Authentication Failure Management
FIA_PMG_EXT.1	Password Management
FIA_UIA_EXT.1	User Identification and Authentication
FIA_UAU_EXT.2	Password-based Authentication Mechanism
FIA_UAU.7	Protected Authentication Feedback
FIA_X509_EXT.1/Rev	X.509 Certificate Validation
FIA_X509_EXT.2	X.509 Certificate Authentication
FIA_X509_EXT.3	X.509 Certificate Requests
FMT_MOF.1/ManualUpdate	Management of Security Functions Behaviour
FMT_MOF.1/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

Requirement	Title
FTA_SSL.4	User-initiated Termination
FTA_TAB.1	Default TOE Access Banners
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;

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.

Requirement	Auditable Events	Additional Audit Record Contents
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure
FCS_NTP_EXT.1	Configuration of a new time server Removal of configured time server	Identity of new/removed time server
FCS_RBG_EXT.1	None.	None.
FCS_TLSC_EXT.1	Failure to establish a TLS session	Reason for failure
FCS_TLSC_EXT.2	None.	None.
FCS_TLSS_EXT.1	Failure to establish a TLS session	Reason for failure
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Provided user identity, 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	Reason for failure
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.

Requirement	Auditable Events	Additional Audit Record Contents
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MOF.1/Functions	Modification of the behaviour of the transmission of audit data to an external IT entity, the handling of audit data, the audit functionality when Local Audit Storage Space is full.	None.
FMT_MTD.1/CoreData	None.	None.
FMT_MTD.1/CryptoKeys	None.	None.
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.

Requirement	Auditable Events	Additional Audit Record Contents
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. [

- <u>The TOE shall consist of a single standalone component that stores audit data locally</u>]

FAU_STG_EXT.1.3 The TSF shall [<u>overwrite previous audit records according to the following rule: [*delete the oldest 1 MB of local audit data*</u>] 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;

]~~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: [

- 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”;

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

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

] that meets the following: *No Standard*.

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, GCM] mode* and cryptographic key sizes *[128 bits, 256 bits]* that meet the following: *AES as specified in ISO 18033-3, [CBC as specified in ISO 10116, GCM as specified in ISO 19772*].

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

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

- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [*2048 bits or greater*],

] 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,]

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

FCS_HTTPS_EXT.1 HTTPS Protocol

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

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS.

FCS_HTTPS_EXT.1.3 If a peer certificate is presented, the TSF shall [not require client authentication] if the peer certificate is deemed invalid.

FCS_NTP_EXT.1 NTP Protocol

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

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

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

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

FCS_NTP_EXT.1.4 The TSF shall support configuration of at least three (3) NTP time sources.

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 [Hash_DRBG (any)]

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_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_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492].

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches [the reference identifier per RFC 6125 section 6].

FCS_TLSC_EXT.1.3 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [Not implement any administrator override mechanism].

FCS_TLSC_EXT.1.4 The TSF shall [present the Supported Elliptic Curves Extension with the following NIST curves: [secp256r1, secp384r1, secp521r1] and no other curves] 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.

FCS_TLSS_EXT.1 TLS Server Protocol Without Mutual Authentication

FCS_TLSS_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_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492].

FCS_TLSS_EXT.1.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [TLS 1.1].

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

FCS_TLSS_EXT.1.4 The TSF shall support [session resumption based on session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2)].

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 *[3]* 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 *[unlock the user]* is taken by an Administrator;]

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: [[“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [“`”, ”~”, ”_”, ”+”, ”-“, ”=”, ”{“, ”}”, “|”, “\”, “:”, “””, ”;”, ””’, “<”, “>”, “?”, “,”, “.”, “/”, *“[”, ”]”];*

a) Minimum password length shall be configurable to between [*15*] and [*100] 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;
- [[*access to help files (PDF and html format)*
- *view alarm notifications*
- *view software version number*]]

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 presence of the basicConstraints extension and that the CA flag is 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 [HTTPS, TLS], and [no additional uses].

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [not accept the certificate].

FIA_X509_EXT.3 X.509 Certificate Requests

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

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

5.3.4 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] capability prior to installing those updates;*
- *Ability to configure the authentication failure parameters for FIA_AFL.1;*
- [
    - Ability to configure audit behaviour;

- Ability to manage the cryptographic keys;
- Ability to configure NTP;
- Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
- Ability to import X.509v3 certificates to the TOE's trust store;]

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: [

- *Firmware integrity tests*
- *Configuration integrity tests*
- *Cryptographic algorithm tests*
- *DRGB tests*
- *Boot loader image verification*].

FPT_TUD_EXT.1 Trusted update

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

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

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

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 [synchronize time with an NTP server].

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, [authentication server] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.
FTP_ITC.1.2	The TSF shall permit **the TSF or the authorized IT entities** to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [*audit server*].

FTP_TRP.1 /Admin Trusted Path

FTP_TRP.1.1/Admin	The TSF shall **be capable of using [HTTPS] 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

20 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

21 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

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

6.1 Security Audit

6.1.1 FAU_GEN.1

23 The TOE generates the audit records specified at FAU_GEN.1 containing the following fields:

a) Date and Time Generated

b) Severity Level

c) Tag

d) Message

e) Source IP Address (external Syslog server only)

f) Source Name (external Syslog server only)

g) Date and Time Received (external Syslog server only)

h) Origin (external Syslog server only)

i) Facility (external Syslog server only)

24 The following information is logged as a result of the Security Administrator generating/importing or deleting cryptographic keys:

a) **Generate CSR**. Action and key reference.

b) **Import Certificate.** Action and key reference.

c) **Import CA Certificate.** Action and key reference.

6.1.2 FAU_GEN.2

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

6.1.3 FAU_STG_EXT.1

26 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 as described by FCS_TLSC_EXT.1.

27 The TOE stores local audit data in 5 1MB rotating log files. When the local audit data store is full, the TOE will delete the oldest log file.

28 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

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

a) **RSA 2048-bit.** Used when generating CSRs.

b) **ECC P-256/P-384/P-521.** Used in TLS.

6.2.2 FCS_CKM.2

30 The TOE cryptographic key mapping is listed in Table 13. The TOE supports the following key establishment schemes:

a) **ECC schemes.** Used in TLS. TOE is sender and receiver. The TOE operates as a TLS server for the web GUI/WebAPI providing administration and as a TLS client for the trusted channel with a syslog server.

Note: RSA is not included in the list of key establishment schemes as it is only used for authentication in TLS, and not key exchange, per the TLS ciphersuites.

Table 13: Cryptographic Key Mapping

Scheme	SFR	Service
ECC	FCS_TLSS_EXT.1	GUI / Administration
	FCS_TLSC_EXT.1/2	LDAP Server
	FCS_TLSC_EXT.1/2	Syslog Server

6.2.3 FCS_CKM.4

31 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

32 The TOE provides symmetric encryption and decryption capabilities using 128 and 256 bit AES in CBC and GCM mode. AES is implemented in TLS and is used in BouncyCastle key encryption.

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

6.2.5 FCS_COP.1/SigGen

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

a) RSA Signature Algorithm with key size of 2048,

35 RSA verification services are used in the TLS. Additionally, RSA signature verification is used for TOE firmware integrity checks.

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

6.2.6 FCS_COP.1/Hash

37 The TOE provides cryptographic hashing services using SHA-1 and SHA-256.

38 SHS is implemented in the following parts of the TSF:

a) TLS;

b) Digital signature verification as part of trusted update validation;

c) Hashing of passwords in non-volatile storage; and

d) Authentication of NTP server.

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

6.2.7 FCS_COP.1/KeyedHash

40 The TOE provides keyed-hashing message authentication services using HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512.

41 HMAC is implemented in TLS and the configuration integrity test.

42 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

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

6.2.8 FCS_HTTPS_EXT.1

44 The TOE web GUI/WebAPI is accessed via an HTTPS connection using the TLS implementation described by FCS_TLSS_EXT.1. The TOE does not use HTTPS in a client capacity. The TOE's HTTPS protocol complies with RFC 2818.

45 RFC 2818 specifies HTTP over TLS. The majority of RFC 2818 is spent on discussing practices for validating endpoint identities and how connections must be setup and torn down. The TOE web GUI/WebAPI operates on an explicit port designed to natively speak TLS: it does not attempt STARTTLS or similar multi-protocol negotiation which is described in section 2.3 of RFC 2818. The web server attempts to send closure Alerts prior to closing a connection in accordance with section 2.2.2 of RFC 2818.

6.2.9 FCS_NTP_EXT.1

46 The TOE makes use of an NTP v4 client that implements the symmetric key authentication scheme defined in RFC5905, performing authentication using SHA-1.

47 The TOE does not update NTP time from broadcast or multicast addresses and supports configuration of at least 3 NTP time sources.

6.2.10 FCS_RBG_EXT.1

48 The TOE contains a Hash_DRBG (any) that is seeded from a hardware entropy source that provides a minimum of 256 bits of entropy. Additional detail is provided the proprietary Entropy Description.

6.2.11 FCS_TLSC_EXT.1 & FCS_TLSC_EXT.2

49 The TOE operates as a TLS client for the trusted channels with syslog and LDAP servers.

50 TLS 1.2 is allowed and ciphersuites are restricted to the following:

a) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289

b) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492

51 Ciphersuites are not user-configurable.

52 The TOE supports 2-way certificate authentication with X.509v3 certificates for Syslog communication. Only DNS names are supported as acceptable reference identifiers. For server certificate verification, the TOE compares the reference identifiers to the identifier in the presented server's TLS certificate.

53 When the TLS client receives an X.509 certificate from the server, the client will compare the reference identifier with the established Subject Alternative Names (SANs) in the certificate. If a SAN is available and does not match the reference identifier, then the verification fails and the channel is terminated. If there are no SANs of the correct type (DNS name) in the certificate, then the TOE will compare the reference identifier to the Common Name (CN) in the certificate Subject. If there is no CN, then the verification fails and the channel is terminated. If the CN exists and does not match, then the verification fails and the channel is terminated. Otherwise, the reference identifier verification passes and additional verification actions can proceed.

54 The TLS client does not support certificate pinning. Only Syslog Communication supports wildcards.

55 The TLS client will transmit the Supported Elliptic Curves extension in the Client Hello message by default with support for the following NIST curves: P256, P384, P521. The non-TOE server can choose to negotiate the elliptic curve from this set for any of the mutually negotiable elliptic curve ciphersuites.

6.2.12 FCS_TLSS_EXT.1

56 The TOE operates as a TLS server for the web GUI/WebAPI trusted path.

57 The server only allows TLS protocol version1.2 (rejecting any other protocol version, including SSL 2.0, SSL 3.0, TLS 1.0 and TLS 1.1 and any other unknown TLS version string supplied) and is restricted to the following ciphersuites by default:

a) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289

b) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492

58 Ciphersuites are not user-configurable.

59 The TLS server is capable of negotiating ciphersuites that include ECDHE key agreement schemes. The TLS server supports NIST curves P256, P384, P521.

60 The TOE supports session resumption based on session IDs according to RFC 5246. When a connection is established by resuming a session, new ClientHello.random and ServerHello.random values are hashed with the session's master_secret. Sessions cannot be resumed unless both the client and server agree.

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 and can range from 15 to 100 characters.

6.3.2 FIA_UIA_EXT.1

63 The TOE requires all users to be successfully identified and authenticated. The following actions may occur prior to authentication:

a) Display the warning banner

b) Access to help files (PDF and html format)

c) View alarm notifications (i.e. system health alarms)

d) View software version number

64 Administrative access to the TOE is facilitated through:

a) **Local.** Directly connecting to the TOE via the Serial Console

b) **Web GUI.** Remotely connecting to the TOE web GUI/WebAPI via HTTPS

6.3.3 FIA_UAU_EXT.2

65 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.

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

67 The TOE supports local authentication for each management interface. Authentication is successful when the submitted username and password are verified against stored values.

6.3.4 FIA_UAU.7

68 For all authentication at the local Serial Console the TOE displays only bullets when the administrative password is entered so that the password is obscured.

6.3.5 FIA_AFL.1

69 The TOE is capable of tracking authentication failures of remote administrators.

70 When a user account has sequentially failed authentication the configured number of times (default 3), the account will be locked until a System Administrator performs unlocks the account.

71 The administrator can configure the maximum number of failed attempts for users authenticating to either web GUI/WebAPI or Serial Console. The default administrative account cannot be locked and is limited to the serial console in the evaluated configuration.

6.3.6 FIA_X509_EXT.1/Rev

72 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, such as when importing CAs, certificate responses and other device-level certificates

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

a) If the certificate ‘notAfter’ date is in the past, 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;

d) The TOE validates a certificate path and treats a certificate as a CA certificate when certificates include the basicConstraints extensions and that the CA flag is set to “TRUE” for all CA certificates.

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

75 The TOE does not provide X.509 Certificate Validation on trusted updates, firmware integrity self-tests or client authentication, the code-signing and clientAuthentication purpose is not checked in the extendedKeyUsage for related certificates.

76 The TOE ensures that the X.509 certificates adhere to RFC 5280 Section 6.3 (certificate validation and certificate path validation), 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

77 If, during the entire trust chain verification activity, any certificate under review fails a verification check, then the entire trust chain is deemed untrusted.

6.3.7 FIA_X509_EXT.2

78 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.

79 Instructions for configuring the trusted IT entities to supply appropriate X.509 certificates are captured in the guidance documents.

80 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, the validation will fail.

6.3.8 FIA_X509_EXT.3

81 The TOE supports the generation of Certificate Request Messages as specified by RFC 2986 and validates the chain of certificates from the root CA upon receiving the CA Certificate Response. Certificate Request Messages provided by the TOE include the following information in the request:

a) Public key

b) Common Name (CN)

c) Organization (O)

d) Organizational Unit (OU)

e) Country (C)

6.4 Security Management

6.4.1 FMT_MOF.1/ManualUpdate

82 The TOE restricts the ability to perform software updates to Security Administrators. When attempting to update the TOE as a non-administrator user, the user is not presented with the update option.

6.4.2 FMT_MOF.1/Functions

83 The TOE restricts the ability to modify (enable/disable) transmission of audit records to an external audit server to Security Administrators.

6.4.3 FMT_MTD.1/CoreData

84 Users are required to login, no TOE functionality is available before identification and authentication occurs.

6.4.4 FMT_MTD.1/CryptoKeys

85 The TOE restricts generation, importation, or deletion of cryptographic keys. to Security Administrators.

6.4.5 FMT_SMF.1

86 The TOE may be managed via the Serial Console or GUI/WebAPI (HTTPS). The specific management capabilities include:

a) Ability to administer the TOE locally via Serial Console and remotely via web GUI/WebAPI

b) Ability to configure the access banner via web GUI/WebAPI

c) Ability to configure the session inactivity time before session termination or locking via web GUI/WebAPI

d) Ability to update the TOE and to verify the updates via web GUI/WebAPI

e) Ability to configure the authentication failure parameters via web GUI/WebAPI

f) Ability to configure audit behavior (enable/disable remote logging) via web GUI/WebAPI

g) Ability to configure NTP time sources through web GUI/WebAPI

h) Ability to manage the cryptographic keys, including import and management of X.509v3 certificates via web GUI/WebAPI

6.4.6 FMT_SMR.2

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

88 Management of TSF data via the Serial Console or Web GUI/WebAPI is restricted to Security Administrators.

6.5 Protection of the TSF

6.5.1 FPT_SKP_EXT.1

89 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 Server Private Key	BouncyCastle RSA (2048 bits)	Flash – plaintext	Overwritten with zeroes via a shell script called by Java. The shell script uses the Linux 'dd' command-line utility to zeroize the non-volatile memory via a single direct overwrite (consisting of zeroes) followed by a read-verify.
		RAM - plaintext	JVM garbage collection on deallocation.
TLS Client Private Key	BouncyCastle RSA (2048 bits)	Flash – plaintext	Overwritten with zeroes via a shell script called by Java. The shell script uses the Linux 'dd' command-line utility to zeroize the non-volatile memory via a single direct overwrite (consisting of zeroes) followed by a read-verify.
		RAM - plaintext	JVM garbage collection on deallocation.
TLS Session Keys	BouncyCastle AES (128)	RAM - plaintext	JVM garbage collection on deallocation.
NTP Key	User generated	Flash – plaintext	Overwritten with new value of key via Linux file overwritten.

6.5.2 FPT_APW_EXT.1

90 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
Locally stored administrator passwords	User generated	Flash - SHA-1

6.5.3 FPT_TST_EXT.1

91 At startup, the TOE performs the following tests:

a) Firmware integrity test using CRC32

b) Configuration integrity test using HMAC SHA-256

c) Algorithm Known Answer Tests

d) DRBG health checks: instantiate, un-instantiate, generate, and reseed

e) Boot loader image verification – the boot loader verifies the SHA256 hash of file “mss-upgrade-components.bin” before the software is installed. Before the “mss-upgrade-components.bin” file is decrypted, the SHA256 hash value will be verified

92 The TOE performs this suite of FIPS power-up and conditional self-tests to verify its correct operation. If any of the self-tests fail, the TOE enters into a critical error state and the appliance must be rebooted by an administrator to run the tests again.

93 The cryptographic module executes the following conditional tests when the related service is invoked:

a) Continuous NDRNG test

b) Continuous DRBG test

c) RSA pairwise consistency test

d) Configuration integrity test using HMAC SHA-256

e) Firmware load test with 2048-bit RSA key

6.5.4 FPT_TUD_EXT.1

94 The current firmware version may be queried using GUI/WebAPI.

95 Digitally signed (RSA 2048) upgrade tar files are acquired by contacting Keysight Technical Support or downloaded via a Customer Portal. Only authorized administrators can perform manual software upgrades.

96 When the administrator performs the software upgrade, the TOE verifies the digital signature of the upgrade files using a hardcoded RSA 2048-bit public key.

97 If the digital signature verification fails, the update is aborted, and a log is generated.

98 Upon successful verification, the TOE software extracts the upgrade components from the tar file and performs the software upgrade. After the software is installed, the TOE is automatically restarted and requires the administrator to log in again for the upgrade process to be complete. If the newly installed software fails for any reason, the TOE software reverts to the previous version without loss of functionality.

6.5.5 FPT_STM_EXT.1

99 The TOE uses external NTP servers to synchronize the clock and provide reliable timestamps for syslog messages.

100 The TOE provides reliable time stamps for the following:

a) Security Audit functionality

b) Track the inactivity of administrative sessions

c) Cryptographic functions

6.6 TOE Access

6.6.1 FTA_SSL_EXT.1

101 The TOE is configured to terminate local inactive sessions (Serial Console) based on a specified time period of inactivity configured by a Security Administrator.

6.6.2 FTA_SSL.3

102 The Security Administrator may configure the TOE to terminate an inactive remote interactive session following a specified period of time.

6.6.3 FTA_SSL.4

103 Administrative users are allowed to terminate their own interactive sessions by logging out.

6.6.4 FTA_TAB.1

104 The TOE displays an administrator configurable message to users prior to login at the Serial Console and Web GUI.

105 **Note:** The Web API is not interactive and does not display a banner.

6.7 Trusted Path/Channels

6.7.1 FTP_ITC.1

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

a) TLS v1.2 for connections to the Syslog server

b) TLS v1.2 for connections to the LDAP Authentication Server

6.7.2 FTP_TRP.1/Admin

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

a) Web GUI/WebAPI over HTTPS per FCS_HTTPS_EXT.1.1

7 Rationale

7.1 Conformance Claim Rationale

108 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

109 All security objectives are drawn directly from the NDcPP.

7.3 Security Requirements Rationale

110 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

111 See appended PDF extract of NDcPP extended components definition.